IAEA 60 Years
Atoms for Peace and Development

International Conference on Physical Protection of Nuclear Material and Nuclear Facilities

13–17 November 2017, Vienna, Austria

Book of Synopses

Organized by the

IAEA 60 Years
Atoms for Peace and Development

in cooperation with the

WORLD INSTITUTE FOR NUCLEAR SECURITY

World Institute for Nuclear Security (WINS)

WNTI

World Nuclear Transport Institute (WNTI)

INTERPOL

International Criminal Police Organization (INTERPOL)

International Conference on Physical Protection of Nuclear Material and Nuclear Facilities

Monday 13 November 2017 - Friday 17 November 2017

IAEA HQ

List of Contributed Synopses

Technical Session 2B-1: **Physical Protection Regime I**

Technical Session 2E-1: **Legal & Regulatory Requirements: Approaches to Development**

Interactive Content Presentations (cont.)

Posters

Posters (cont.)

Posters (cont.)

Posters (cont.)

Synopsis ID: [23]

Strengthening the National Physical Protection Regime: Actions Needed to Move Forward

Elabd, A.[1]; Elhefnawy, O. [1]

[1] Egyptian Nuclear and Radiological Regulatory Authority (ENRRA), Egypt

Corresponding Speaker: A. Elabd

An effective physical protection regime can be a vital barrier to prevent the illicit movement of nuclear material from a controlled environment to an uncontrolled environment. States have taken numerous actions to protect the material within their jurisdictions. These actions have varied widely, depending on the nuclear capabilities, perception of threat, capacity building, technical support, cultural needs and the financial resources available. This study is focused on needs of nuclear newcomers in development of physical protection systems, based on national nuclear security infrastructure. The structure of the paper is divided into three parts. First part introduced the basic physical protection requirements for establishing a regulatory basis of nuclear newcomer States. Second part introduced the complementary recommended requirements that should be implemented by States during establishment its physical protection regime. Third part introduced the proposed actions which States need to move forward for strengthening its physical protection regime by defining five levels of organizational successes, each with its own set of characteristics. By identifying where your organization falls, you will know what you need to do to move to the next stage and improve your ability to secure/protect nuclear material and facilities against unauthorized removal and sabotage. First part: it's established a regulatory basis to build and implement national physical protection regime. Application of the regulations is obligatory for all juridical persons engaged in nuclear activities and for executive bodies responsible for coordinating and controlling nuclear activities. Egypt takes into account the requirements of the Convention on the Physical Protection of Nuclear Material (CPPNM) and its amendment and the IAEA recommendations of INFCIRC/225/Rev.5. Also, during preparation of the regulations the experiences of other countries in this sphere examined and taken into consideration. The Regulations elements: the physical protection objectives; the functions of executive bodies and organizations responsible for ensuring physical protection; the categorization of nuclear material; the physical protection system requirements for nuclear facilities and nuclear material for both storage and transportation; and the response procedures for unauthorized removal and sabotage or other malicious acts. Second part: it's recommended to learn from more efficient international nuclear security systems; taking steps to build international understanding of the threat; establishing effective performance objectives; assure performance; training and certify needed personnel; building nuclear security culture and exchange best practices; and reducing the number of sites that need to be protected. Third part: It deals with evaluation the national physical protection regime according to the proposed five levels. The

proposed levels are highly effective, effective, good, developing and ineffective. Highly effective level has a set of characteristics, for example, State is ratified CPPNM and its amendment, State should have an effective nuclear security (regime/ law and regulations) for (organized/control) the nuclear and radioactive activities, integrated nuclear security support plan (INSSP) and human resources development plan. Good communication between regulatory body, operator and response force team. Individuals are well trained and competence certified. Responsibilities should be documented in Memoranda of Understanding or comparable documents. Effective level has a set of characteristics, for example: State is signed CPPNM and its amendment, State is established the legal and regulatory frameworks. The organization participates is communicated regularly with other stakeholders. The organization is involved in the design of INSSP and participates in table- top exercises to identify any logistical issues. The organization follows developments in physical protection regulations and technology with interest. Good level has a set of characteristics, for example, State is established the legal and regulatory frameworks. The organization participates in a few meetings with other stakeholders when invited. Individuals engaged in physical protection system have been trained but cannot demonstrate their competence for security. Developing level has a set of characteristics, for example, State is starting for establish a regulatory basis. The organization only participates in meetings with other stakeholders when required by the regulator. Individuals engaged in physical protection system have limited understanding, skills and competences for security. An ineffective level has a set of characteristics, for example, State doesn't have a regulatory basis for nuclear activities. The organization does not participate in meetings with other stakeholders related to nuclear activities. The organization is concerned with nuclear safety elements than nuclear security elements. They are important topics that are laid out in more detail in the paper. Egypt announced its intention to take the necessary measures to become a party to CPPNM and its amendment and it adopted the measures stipulated in the law and its executive regulations. Egypt's concern is to enhance and improve the physical protection systems in their nuclear facilities. Egypt are taken several steps in the field of nuclear security in its various aspects such as the legal and regulatory frameworks, physical protection of nuclear material and facilities, nuclear material accounting, security of radioactive sources, IPPAS missions, and human resources development plan.

Synopsis ID: [112]

Specialized Command for Nuclear Security: Coordinate the State's Response to Nuclear Security Threats and Breaches

Haouchine, F. [1] ; Basille, S. [1] ; Cormier, P. [1]

[1] Specialized Command for Nuclear Security, France

Corresponding Speaker: Basille, S

In 2009, in order to counter the terrorist threat to nuclear power plants, the Ministry of Interior created a new type of specialized intervention unit. The IAEA's IPPAS mission carried out in France in 2011 confirmed the relevance of this model: it develops interfaces between safety and security, highlights the defense-in-depth principle, and adapts the state's response to constraints and requirements emerging from new types of threat and the industrial nuclear environment. The Gendarmerie's specialized intervention unit (PSPG) acts as the operator's (EDF) last response in the physical protection system and the state's first response regarding nuclear counter-terrorism. In 2012 and 2013, environmentalist movements opposing nuclear energy have become more and more active, highlighting the need to enhance protection of nuclear materials, activities and facilities, particularly in the areas of anticipation, protection and intervention.

The Ministry of Interior implemented the Specialized Command for Nuclear Security (CoSSeN) to address this necessity. The term "specialized" refers to the concept elaborated in 2007-2009 as well as to all the progress made since then. It symbolizes the state's ambition to strengthen its response regarding facility protection, on an ongoing basis and in cooperation with all the public and industry stakeholders.

The CoSSeN is a government agency with national jurisdiction, which carries out its operational mission under the supervision of the Interior and Energy ministries. It enables public authorities to better coordinate actions as well as their results regarding protection of nuclear materials, activities and facilities. It also emphasizes the defense-in-depth principle in all its aspects (anticipation, protection, intervention). Lastly, it contributes to reinforcing the nuclear security culture.

In order to improve coordination of actions, the CoSSeN:

Contributes to better information sharing between different departments;

Reinforces harmonization of security force practices;

Conducts administrative control and monitoring of individuals requesting access to nuclear facilities;

Develops the expertise of national security forces;

Advises and supports public authorities.

Regarding defense-in-depth, the CoSSeN works particularly on:

Anticipation: It reinforces awareness of internal threats and the external environment; it gathers, analyzes and synthetizes intelligence information; it advises national and local authorities as they elaborate their security and defense plans; it makes recommendations about the development of operational concepts.

Protection: It helps ensure protection of sensitive data by verifying the suitability of the premises in which they are used; regarding transport, it advises authorities as they elaborate their security and defense plans and it provides expertise on security forces operations.

In order to reinforce the security culture, the CoSSeN:

Makes recommendations about the development of operational concepts;

Regarding transport, it advises the security and defense representatives of operators, subcontractors and service providers.

Synopsis ID: [125]

Implementation of a Nuclear Security System in the Kingdom of Morocco

Mrabit, K. [1], **Boustani, B.** [1]

[1] Moroccan Agency for Nuclear and Radiological Safety and Security, Morocco

Corresponding Speaker: B. Boustani

Several legal instruments exist for a global and more universal nuclear security framework, which, once ratified or adopted by a country, become legally binding and must therefore be integrated into the national legislative and regulatory regime. Among the most relevant nuclear security related instruments that were ratified or adopted by the Kingdom of Morocco are:

• The Convention on the Physical Protection of Nuclear Materials and its 2005 amendment, ratified respectively in 2002 and 2015;

• The International Convention for the Suppression of Acts of Nuclear Terrorism, ratified in 2010;

• The Resolution 1373 adopted by the UN Security Council in 2001 following the 11 September terrorists attacks, which requires that member countries take necessary measures to prevent and suppress terrorism;

• The Resolution 1540 adopted by the UN Security Council in 2004 which requires that all States shall refrain from providing any form of support to non-State actors that attempt to develop, acquire, manufacture, possess, transport, transfer or use nuclear, chemical or biological weapons and their means of delivery, in particular for terrorist purposes. . . .

With a view to meeting its international obligations and improving its nuclear security regime, the Kingdom of Morocco has promulgated the law 142-12 related to nuclear and radiological safety and security as well as the creation of the Moroccan Agency for Nuclear and Radiological Safety and Security(AMSSNuR), as the unique Regulatory Body regulating safety, security and safeguards. The provisions of this law, in terms of nuclear security, cover the establishment of a Physical Protection System (PPS) of nuclear materials and associated installations, including measures to protect sensitive information and to ensure their confidentiality. This PPS, which is based on the evaluation of the threat, foresees levels of protection of nuclear materials and of associated installations in accordance with the levels that are prescribed in the Convention for Physical Protection of Nuclear Materials and its amendment. The provisions of the law 142-12 as well as the law 03-03 related to terrorism, criminalize deliberate acts that pose a threat to nuclear materials and foresee penal sanctions that are proportionate to the seriousness of those acts. Responsibilities in terms of nuclear security are shared, but the primary responsibility for the physical protection of nuclear materials, other radioactive

materials as well as associated installations, falls primarily on the licenses or holder of the authorization. With regard to the responsibility of the State, it consists of intervening in the case of a malicious act once it goes beyond the capacities of the holder of the authorization, in order to regain control over these materials, and, as required, minimize the consequences of such an event. Although the former legislative system, prior to the 142-12, did not foresee specific provisions for nuclear security issues, regulatory bodies which were in place made considerable efforts to secure certain installations with nuclear materials or other radioactive materials potentially having the highest risks. Finally, AMSSNuR has established a committee consisting of several all relevant Moroccan ministerial Departments and Institutions having responsibilities in the nuclear security field. This committee, driven by AMSSNuR, will be in charge, inter alia, of establishing the System of Physical Protection of nuclear materials and associated installations through the setting up of a specific nuclear security regulation. The latter will integrate the requirements of the 2005 amendment to CPPNM.

Synopsis ID: [65]

Drive in Strengthening the Physical Protection Regime of Bangladesh

Kibria, A.[1], Alam, H. [1]

[1] Bangladesh Atomic Energy Commission, Bangladesh

Corresponding Speaker: A. Kibria

Bangladesh has been using nuclear technology in the fields of research and education, health, agriculture and industry for more than five decades. From the beginning, the country paid deep attention in ensuring the security of the nuclear and other materials in use, their associated facilities and activities. Bangladesh is always aspiring in fulfilling the essential and obligatory needs by formulating and revising the responsibilities of its nuclear security regime in view to achieving a better sustainability. The Convention of the Physical Protection of Nuclear Material (CPPNM) entered in Force in Bangladesh from 10 June 2005. Bangladesh is working to become a party to the amendment of the CPPNM which entered into force in 2016. IAEA IPPAS mission was carried out in Bangladesh in 2009 when the physical protection system of the country was reviewed. According to the recommendations for improvements, upgrades of physical protection systems of different nuclear and radioactive facilities were carried out. Among them the TRIGA MARK II Research Reactor, Radioactive Waste Management Unit, Co-60 Irradiators, Radio therapy units are remarkable. Now, Bangladesh has Atomic Energy Regulatory Act 2012 and Atomic Energy Regulatory Authority. In the national regulation, the country is committed to protect nuclear and other radioactive materials in use, storage and transport and their respective facilities. The Regulatory Authority, operator i.e. Bangladesh Atomic Energy Commission (BAEC) and the relevant national stakeholders are working together in strengthening the nuclear security and physical protection regime of the country for the successful implementation of its 1st nuclear power plant (NPP). It is notable that Bangladesh has signed a Cooperation Agreement and Inter Governmental Agreement (IGA) with Russian Federation for setting up two VVER 1200 MWe nuclear power reactor at Rooppur of Bangladesh. The country is as usually setting and strictly performing the stepwise necessary nuclear security and physical protection tasks by abiding national laws, international obligations, extending cooperation with neighboring countries, vendor country and relevant international organizations. The Regulatory Act 2012 adopted that the physical protection of nuclear material and nuclear installation shall be ensured according to the requirements of the CPPNM. It is notable that Bangladesh is a signatory of both IAEA Safeguards Agreement and Protocol Additional in connection with NPT. The country has an approved IAEA INSSP. It also has an agreement with USDOE regarding the development of physical protection of nuclear and other radioactive materials and their facilities. Through IAEA, USDOE and by implementing national policy on human resource development (HRD), the country is consecutively developing its nuclear security regime by giving emphasize on the physical protection

system of nuclear and other radioactive materials which the country presently have and will have in near future especially in the 1st NPP. It is notable that during the development of INSSP for Bangladesh, a lot of gaps regarding the national nuclear security and physical protection regimes were identified. As Bangladesh is a new comer country in NPP, it requires more cooperation and exchange of knowledge with the countries having NPP and obviously with the IAEA. Although, threat on nuclear and radioactive materials and their facilities is increasing worldwide day by day, Bangladesh is committed to develop its nuclear security and physical protection regime till achieving better sustainability for the sake of the country and others.

Synopsis ID: [105]

Development of Physical Protection Regulatory Requirements

Shah, S.[1], Abbas, M. [1], Shakoor, A. [1]

[1] Pakistan

Corresponding Speaker: S. Shah

The International Instruments including Convention on Physical Protection of Nuclear Material (CPPNM) amended, United Nations Security Council Resolution 1540 and IAEA Nuclear Security Series documents recommend the States to establish, implement, maintain and sustain a national legislative and regulatory infrastructure that governs physical protection of nuclear material and nuclear facilities. A State's physical protection regime consists of legislative and regulatory framework; the institutions and organizations within the State responsible for ensuring implementation of the legislative & regulatory framework; and physical protection measures/systems for facility and transport. The International Instruments and the best practices adopted by international community recommend a number of areas and activities which should be considered for the development of regulatory requirements. Among many, these include but not limited to, objectives of the physical protection program, responsibilities of stakeholders,threat assessment or design basis threat ,fostering security culture, confidentiality of information, quality assur- ance, sustainability of physical protection measures/systems, concept of defense in depth and graded approach, interfaces of physical protection system with safety and NMC&A, performance testing, contingency plans and compensatory measures , access authorization program. The regulatory requirements are developed considering the followings:

- State's obligations under international instruments;
- National legislative requirements;
- Best practices adopted by na- tional and international community;
- Current evaluation of the threat;
- Operational experience feedback;
- Technological advancements.

Pakistan is currently regulating physical protection of nuclear material and facilities using IAEA INFCIRC 225/Rev.5 along with national regulations for licensing, design and operation of nuclear installations. At the same time Pakistan is in process to promulgate its detailed regulations on Physical Protection of Nuclear Material(s) and Nuclear Installations which are consistent with the

recommendations of CPPNM as amended and INFCIRC 225/Rev.5 as well as the best practices adopted by the international community. This paper will address in detail Pakistan's case for development of regulatory requirements.

Synopsis ID: [150]

An Introduction of Draft Regulations on Nuclear Security

Wang, L.[1]

[1] China State Nuclear Security Technology Center, China

Corresponding Speaker: L. Wang

On March 24th 2014, at the third Nuclear Security Summit in Hague, President Xi Jinping pointed out that "we are in the process of drafting national regulations with a view to putting nuclear security endeavor on an institutional and legal footing." China Atomic Energy Authority (CAEA) had been leading State Nuclear Security Technology Center (SNSTC) to develop the Regulations on Nuclear Security. In January 2016, the draft Regulations on Nuclear Security was submitted to the State Council. The draft comprises nine sections and fifty-four articles. Section A shows us the general requirements on nuclear security in China, and there are eight articles in the section. Section A declares that China will adopt graded approach to the security on nuclear materials, nuclear facilities, other radioactive substances and associated facilities, according to the potential consequence, if such materials or facilities were illegally occupied or maliciously attacked. And in the section, the responsibilities of all related competent authorities (such as: China Atomic Energy Authority, Ministry of Public Security. . .) are clarified. Section B gives the requirements of the threat assessment to nuclear security at national level and facility level. All the competent authorities should work together to make out the Design Basic Threat at national level. And operators should develop their Design Basic Threat for facilities operated by the operators, and submit the facility level DBT documents to CAEA for approval. Section C deals with the security of nuclear materials and nuclear facilities in China. The Physical Protection System of nuclear materials or nuclear facilities should not be constructed unless the design of Physical Protection System has got the approval by CAEA. And there is similar approval process for the Physical Protection System it is to be put into operation. Section D sets out the requirements for security to other radioactive substances and associated facilities, and there are five specific rules in the section. Section E deals with the security to nuclear materials and other radioactive substances during transportation. Section F gives the requirements of cyber security. It is clear that the operators of nuclear facilities should assess cyber threat periodically and take measures to improve the reliability of cyber system. Section G shows us the rules of response and practice to nuclear security incidents. Section H announces the qualification and training requirements for nuclear security personnel, and requirements of purchasing, installation, debugging, operation and maintenance for nuclear security equipment. Section I defines the legal responsibilities to all the organizations and individuals who are involved in nuclear security.

Synopsis ID: [249]

Combining International Best Practices and Local Specifics in Developing National Physical Protection Regulations

Kovchegin, D.[1]

[1] Russian Federation

Corresponding Speaker: D. Kovchegin

Development of national regulations supporting physical protection is important part of ensuring security of nuclear materials and sites. IAEA Guide "Milestones in the Development of a National Infrastructure for Nuclear Power" (henceforth "Milestones") defines legislative and regulatory frameworks (that include physical protection) as one of the twelve essential elements for nuclear security. One should also understand that other eleven essential elements are not independent from legislative and regulatory framework. Instead, to be practically implemented these eleven elements must me codified in national legislation and regulatory documents. "Milestones" further recommend that Nuclear Energy Programme Implementing Organization phase I report that defines and justifies a national strategy for nuclear power should identify the elements of a legal framework for nuclear security and legislative and regulatory frameworks for nuclear security should be put in place during phase II of developing the infrastructure necessary to support a nuclear power programme before the country is Ready to invite bids/negotiate a contract for the first nuclear power plant.

Nuclear newcomers and states that have less developed national regulatory infrastructure for physical protection often resort to international experience and international assistance to support development of their national regulations governing physical protection. Model structure for national regulatory framework and content for national regulations can be obtained from multiple documents available at IAEA, as well as from countries that have significant expertize in ensuring physical protection of their nuclear sites, such as Russia, the U.S. or other countries heavily involved in exporting nuclear technologies. However, best practices from IAEA documents and regulations developed by countries with significant nuclear expertise can hardly be implemented in newcomer countries without any adjustment. While fundamental principles of nuclear security are universal, specific implementation that must be captured in national regulations and executed through national institutional infrastructure varies depending on the wide array of in-country environments. Attempts to implement international best practices without any adjustment can result in national regulations that cannot be implemented due to conflicting institutional structures, insufficient capabilities to implement them or lack of stakeholders buy-in driven by local cultural specifics.

Based on experience supporting international cooperation programs aimed at development of national nuclear security regulations in Russia, Ukraine and Belarus authors of the paper recommend

that those involved in development of national regulations implement approach that includes, but not limited to, the following measures:

National legal experts and organizations responsible for the development physical protection component of nuclear programme should work together, engaging international support if necessary, to identify institutions whose participation is critical and procedures that must be followed to develop and implement a set of physical protection regulations. Procedure for the development of physical protection regulations must comply with country's procedure applicable for the development of any other regulation. Based on the results of analysis, national plan for the development of regulations should be developed and implemented.

Identify components of physical protection infrastructure that require regulatory coverage. This is necessary to determine scope of regulations to be developed. If country plans developing relatively simple nuclear program, then it can require relatively simple set of regulations avoiding sophisticated structures necessary for countries with extensive nuclear programmes. On the other hand, certain local specifics might require developing regulations that would be unique to the country. Progress in developing national regulations should be measured against identified setof physical protection infrastructure components until all of them are provided with regulatory coverage.

Based on available international best practices, capture the nuclear security goals to be achieved. Then analyze local practices contributing to the achievement of these goals, and adjust best practices to ensure feasibility and buy-in of the local stakeholders and personnel. When transferring nuclear security best practices, do not insist on copying them, as implementation practices and mechanisms that work well in one country can be fully dysfunctional in another one.

Start development of national capabilities necessary to comply with newly established regulatory requirements before or at least no later than actual regulation development. This will ensure that regulators are capable to enforce regulatory requirements, operators are capable to comply with them, as well as facilitate reflecting local specifics in developed regulations. Capability development may include personnel training, best practices exchange, equipment supplies, site upgrades, etc.

Implementation of this approach will help establishing national regulatory framework that reflects each country specifics, yet reflects international best practices.

Synopsis ID: [300]

Legal and Regulatory Framework and Situation for Physical Protection of Nuclear /Radioactive Materials in Ethiopia

Aregga, B.[1]

[1] Ethiopian Radiation Protection Authority, Ethiopia

Corresponding Speaker: B. Aregga

Ethiopia has been working aggressively to build its regulatory infrastructure by establishing the required framework for the control of malicious use of nuclear and radioactive sources. There is a hierarchy of responsibilities within our institutional framework, from the Ministry of Science and Technology to the regulatory body and to the organizations responsible for and the persons engaged in activities using nuclear/radioactive sources in industries, medical facilitates and research institutes. With a view for ensuring the protection of people and the environment from harmful effects of nuclear/radioactive and radiation sources, establishing appropriate regulatory control infrastructure, safety, physical protection & security standards of nuclear materials in compliance with the IAEA fundamental safety requirements is given first priority. The Government of Ethiopia approved its revised nuclear and radiation protection legislation Law on 13 June/2017 with an expanded scope of implementation of physical protection and security of nuclear materials, through the Ethiopian Radiation Protection Authority (ERPA).

It is evident that applications of specially radioactive sources have increased in many sectors in types and sizes in conection with the expansion of industriazliztion in the country. Thus; effective physical protection systems are therefore required to protect nuclear material and facilities from theft and sabotage for both non-proliferation and radiation safety purposes. Ethiopia is therefore; in the process of negotiation with the IAEA and conduct safeguards workshop in April/2017 to sign additional and small quantity protocols to adhere to the international rules and procedures and to fully benefited from the cooperation for the control and protection of nuclear materials and facilities at the national level and in the region. Though; the responsibility clearly rests with the Government to ensure that such physical protection systems are properly established and operated; it is also important to strengthen international cooperation since incidents in one State can have consequences across national borders in a hostile region like east Africa where it is faced with terrorist attacks.

This paper presents the legal and regulatory framework for the physical protection and security of nuclear materials, implementation, progresses, agreements and cooperation related to it. In addition it addresses further actions, gaps and recommendations what to be done at the national level and in the region.

Synopsis ID: [286]

Comparative Analysis on the National Approaches for the Legal Implementation and Criminalization of the Offences under the Convention for the Physical Protection of Nuclear Material (CPPNM) and its Amendment

Siserman, C. [1]

[1] University of Vienna, Faculty of Law, Austria

Corresponding Speaker: C. Siserman

Physical protection against theft, unauthorized diversion or sabotage of nuclear materials by individuals or groups has long been a matter of national and international concern. Traditionally, this area has remained entirely within the responsibility of each State, despite expanding into a complex set of legal, administrative and technical measures to "physically" protect nuclear material, However, in the past decades it has become more evident that many States are not indifferent to what extent that responsibility is fulfilled. Starting from this premise, the present study will analyze the legal measures that various States have transposed or adopted in their national legislations to implement the Convention on the Physical Protection of Nuclear Material (CPPNM) and its Amendment, which is the only legally binding international instrument in the area of physical protection of nuclear materials used for peaceful purposes.

One of the main objectives of this study is to enhance the understanding of the CPPNM and its Amendment by providing a comparative legal analysis on the way illicit acts listed in these instruments have been made a punishable offence by Parties under their national law. The research will begin with a historical overview of the CPPNM and its Amendment, and it will briefly discuss their three key components: the scope of protection; the criminalization of offences; and the international cooperation and information exchange. For the purpose of this study, however, the research will mainly focus on the criminalization component and discuss the legal mechanisms put in place by various national systems to deal with these offenses. More specifically, the paper will provide concrete legislative examples on how, for instance, States parties have made a punishable offence under their national law the "intentional commission of an act without lawful authority which constitutes the receipt, possession, use, transfer, alteration, disposal or dispersal of nuclear material, which causes or is likely to cause death or serious injury to any person or substantial damage to property" (Article 7 (a) of the CPPNM). It will also address other offences covered by the Amendment, such as the theft and robbery of nuclear material, and the established new ones such as the smuggling of nuclear material.

Moreover, the study will also address the challenges associated to transposing the international legislation into the national system in a manner that concisely, accurately and consistently codifies the differently framed provisions in the international instruments that are currently in force and relevant for the area of physical protection of nuclear material. It will discuss matters related to the legal and regulatory actors that play a role in establishing and maintaining the physical protection regime, the enforcement procedures such as detection, investigation and prosecution of the illicit acts mentioned above, as well as issues related to sanctions and penalties. Being aware that various countries have different legal systems, the author believes that a comparative study will offer the opportunity to identify model legislative elements that could be useful for States that are currently in the process of drafting legislation for criminalizing the offences under the CPPNM and its Amendment.

Keywords: criminalization, penalties, CPPNM, Amendment, enforcement, criminal codes.

Synopsis ID: [92]

Development of Physical Protection Vulnerability Assessment Tool TESS

Kang, Y.[1]

[1] Korea Institute of Nuclear Nonproliferation and Control (KINAC), Republic of Korea

Corresponding Speaker: Y. Kang

A physical protection system (PPS) integrates people, procedures, and equipment for the protection of assets or facilities against theft, sabotage or other malevolent attacks. Even when a strong PPS is provided, without regular assessments, a PPS might waste valuable resources on unnecessary protection or, worse yet, fail to provide adequate protection at critical points in a facility. The evaluation of the effectiveness of a PPS using tool is expected to become more and more necessary. The ROK conducts a force on force (FOF) once a year to measure the effectiveness of the physical protection of the facility. However, the fact that training can not be repeated many times with unavoidable constraints and opportunity costs, is a necessary reason. Early establishment of a physical protection model requires much effort, but it is very useful because it allows you to evaluate a partial change of a facility or a hypothetical scenario. At present, the level of the domestic regulatory agency is carrying out tasks for the purpose of research for the future, and is not used for regulation yet. In evaluating the effectiveness of a PPS, there are two main perspectives. The first addresses a path analysis of potential outside attacks and the second deals with neutralization. However, in this paper, we introduce the general introduction of the physical protection effectiveness evaluation tool developed by KINAC, excluding the neutralization, and briefly introduce element technology and algorithm that are used in system. KINAC is currently developing a physical protection vulnerability assessment tool. As part of it, we use AVERT, a commercial program, to model and validate actual nuclear facilities. AVERT is capable of detailed modeling and detailed simulation through various relationship among the components and is based on Monte Carlo simulation basically. We analyzed the advantages and disadvantages of commercial tool and used it to develop TESS. TESS provides a three-dimensional modeling environment and visualization. However, the internal data structure is generated in two dimensions, and thus the algorithm for validity evaluation is also tow-dimensionally constructed. TESS is basically developed to verify and regulate commercial programs such as AVERT, So AVERT library is used for physical protection system modeling. We are working on modeling the other parts as closely as possible and analyzing only the differences in the algorithms used to calculate the validity of TESS and AVERT. Through this approach, we expect to be able to make meaningful analyzes by comparing AVERT and TESS, and comparing them with FOF results. In this paper, we describe the basic structure of TESS and its use procedure, the description of Critical Detection Point (CDP) which is the basis of system development, the method of generating 2D Mesh which is the basis of algorithm structure, We will discuss the results of validation of TESS for a hypothetical nuclear power facility.

Synopsis ID: [250]

Best Practices on Methodologies and Techniques to Assess the Effectiveness of Physical Protection Measures and Systems

Parrilla, M.[1]

[1] National Nuclear Security Administration, United States of America

Corresponding Speaker: M. Parilla

Through the Vulnerability Assessment process, the VA department develops expectations and assumptions of the effectiveness of physical protection systems. To validate these expectations and assumptions, the VA department collaborates with performance testing personnel in developing credible performance tests to determine the effectiveness of the protection system. The VA determines criteria for varying testing methodologies, such as operability testing, effectiveness testing, adversarial testing (to include insider related), and black-hat testing. Performance testing and VA personnel collaboratively develop a test plan to ensure objectives and testing parameters are met. Depending on the importance of the protection measure or system being assessed, the testing frequency will vary. Discussion of multiple examples of testing systems and associated methods of testing (operability vs. adversarial) to be added to presentation. Data from the performance test is gathered and tracked using multiple tool to develop figure-of-merits. These probabilities either validate or invalidate the assumptions/expectations of the VA, and are entered into modeling tools to determine the site system effectiveness.

Synopsis ID: [263]

Assessment Methodologies and Evaluation of the Physical Protection System

Chetaine, A.[1]

[1] University of Mohammed V, Faculty of Sciences, Morocco

Corresponding Speaker: A. Chetaine

Physical protection consists of a variety of measures to protect nuclear facilities and material against sabotage, theft, diversion, and other malicious acts. It's the integration of people, procedures, and equipment used to protect assets or facilities against theft, sabotage, or other malicieuse human attacks. The PPS functions are detection, delay and response, Before the design of the PPS we must see what we must protect (facility categorization), what i must protect against (against which the PPS must be designed) and level of protection is adequate (facility categorization and data base threats). The design of the PP scan be implemented during the design of the facility or Nuclear material. Before that we can trust the PPS we must make assessment and evaluation of the system to verify the effectiveness and see if the PPS verify the functions (detection, delay and response)

Before that we can trust if the PPS is adequate and effective, it must first be verified that it fulfills the essential functions: detection, delay and response.

This can be done with an assessment and depending on the response an update is carried out. The assessment and overview must be done on different elements of the PPS and periodically and then evaluates the proposed design to determine how well it meets the objectives.

In this work we can see the assessment of different elements and if necessary the updates of equipment's or procedures.

Synopsis ID: [290]

Summary of Analysis Methodology Results of the Nuclear Security Assessment Methodologies (NUSAM) Coordinated Research Project

Snell, M.[1], Rivers, J. [2], Shull, D.[3]

[1] Sandia National Laboratories, United States of America

[2] Nuclear Regulatory Commission, United States of America

[3] Department of Energy, United State of America

Corresponding Speaker: M. Snell

This paper reports on analysis methodology results developed and documented during the International Atomic Energy Agency (IAEA) Coordinated Research Project (CRP), the Development of Nuclear Security Assessment Methodologies (NUSAM) for Regulated Facilities. The main objective of the NUSAM Project was to establish a risk-informed, performance-based methodological framework, addressing both insider and outsider threats to facilities and transport involving nuclear material. One of the NUSAM Working Groups, the Analysis Working Group (AWG) looked specifically at analysis techniques and methods.

This paper discusses and compares several types of modeling and simulation tools that exist today and are used internationally to support physical protection system effectiveness evaluation, as part of risk-informed security. The AWG was able to work directly with the developers of these different methods and tools to document the strengths and weaknesses of each. With its technical expertise, the AWG was able to document the technical and mathematical basis for several of the different techniques, at a level that has not been published to date. The AWG developed summary diagrams that relate how all of the tools to date can best be used in conjunction with one-another

Synopsis ID: [179]

ISCN's Activities to Promote Universalization of INFCIRC/225/Rev.5

Noro, N.[1], Matsuzawa, R. [1]; Nakamura, Y. [1]

[1] Japan Atomic Energy Agency, Japan

Corresponding Speaker: N. Noro

As a regional Center of Excellence (COE) on nuclear security in Asia, Integrated Support Center for Nuclear Nonproliferation and Nuclear Security (ISCN) of Japan Atomic Energy Agency has been supporting IAEA and international community to promote universalization of IAEA's nuclear security recommendations (INFCIRC/225/Revision 5 or Nuclear Security Series 13 (NSS 13)) through its activities. ISCN has been providing various nuclear security trainings since its establishment in 2010, targeting mainly countries in Asia. ISCN conducted 83 trainings in the past 6 years and accepted more than 2,100 participants. This paper will describe how ISCN has developed its capacity building support program to assist international effort to effectively implement recommendations in NSS 13. First, ISCN directly supported IAEA to develop a training course on NSS 13. ISCN, with the National Nuclear Security Administration of the US Department of Energy (DOE/NNSA) and subject matter experts (SMEs) of the Sandia National Laboratories (SNL), developed several nuclear security training courses for the regional countries. One of the course was a two-day workshop on NSS 13 ISCN and DOE/NNSA/SNL developed in 2011. The workshop was adopted by the IAEA as its first NSS 13 workshop in 2012. ISCN and DOE/NNSA/SNL joined the consultancy meeting of IAEA to develop a five-day training course on NSS 13, and ISCN hosted the first IAEA NSS 13 course in Tokai, Japan, in 2013. Second, ISCN has developed several nuclear security training courses which comply with the recommendations of NSS 13. ISCN jointly developed the basic introductory-level regional training course on physical protection (PP RTC) with DOE/NNSA/SNL, which focuses on the performance-based approach to the design and evaluation of the physical protection system, as recommended in NSS 13. ISCN offers PP RTC annually since 2011, and more than 160 participants attended the course (as of April 2017). In order to enhance the effectiveness of the training and promote understanding of NSS 13 recommendations, ISCN developed training tools such as Virtual Reality (VR) System and Physical Protection Exercise Field (PPEF). VR System and PPEF complement each other, and participants are able to learn the concept of performance testing of physical protection system effectively by using both VR system and PPEF in PP RTC. The paper also describes how ISCN developed training curricula using these training tools. Other than PP RTC and NSS 13 training course, ISCN gradually increased training courses it offered, such as nuclear security culture, computer security, performance testing and insider threat, all of them were advocated in NSS 13. Third, ISCN complements IAEA's activities by assisting other Member States in Asia to build their own capacity for implementing recommendations of NSS

13. For example, ISCN has provided training courses upon request from the partner country. Such bilateral cooperation includes joint curriculum/material development and dispatch of ISCN lecturers. Since 2015, ISCN is working closely with Indonesia to assist their capacity building at COEs of regulatory authority and license holders. ISCN was also requested by Kazakhstan COE to support them building their own capacity, together with US DOE/NNSA. By sharing Japan's experience, knowledge and methodology of training, ISCN has been contributing to build capability of effective implementation of NSS 13 recommendations in the partner country. The purpose of this paper is to share Japan's experience in promoting implementation of NSS 13 through the human resource development assistance activities in the region, and thus contribute to the universalization of NSS 13. During the Nuclear Security Summit Process (2010-2016), many countries made commitment to establish a COE to support global effort to strengthen nuclear security. ISCN is one of the COE who commenced its activity at the earliest stage. Through its activities, ISCN has realized that the needs for capacity building support is quite high among many countries. IAEA alone cannot meet the request of the Member States, thus the role of COEs is essential for promoting implementation of NSS 13 recommendations. This paper will serve as a good reference of such effort.

Synopsis ID: [167]

Strengthening Physical Protection Regulatory Requirements based on INFCIRC 225 Rev.5 in Indonesia.

Suharyanta, S.[1]

[1] Department of Licensing of Nuclear Installations and Nuclear Material (BAPETEN), Indonesia

Corresponding Speaker: S. Suharyanta

Indonesia in establishing and developing a new regulation refer to the regulations and guidelines of the IAEA is an option and harmonized with existing national regulation, including the regulation for physical protection of nuclear installation and nuclear material. In order to strengthen the physical protection system, Indonesia has developed regulatory on Guidance for Physical Protection in Nuclear Installation and Nuclear Material with reference to INFCIRC 225/Rev 5. This paper will describe elements of physical protection system which are strengthened in the new regulation. The ultimate goal is in order to perform regulatory review the effectiveness of physical protection plan implementation in nuclear installations. It also describe experience an combined field-exercise of both together of the contingency security plan and emergency plan.

Key words: elements of physical protection.

Synopsis ID: [225]

INFCIRC/225/Rev.5 Implementation at a Facility-Level: Common Issues and Best Practices

Bukharin, O.[1]

[1] Nuclear Regulatory Commission, United States of America

Corresponding Speaker: O. Bukharin

The significance of the IAEA publication INFCIRC/225, "Nuclear Security Recommendations on The Physical Protection of Nuclear Materials and Nuclear Facilities," the latest revision (Revision 5) of which was published by the IAEA in January 2011, is difficult to overstate. The document reflects the operating experience and the corporate knowledge of the international physical protection community. It is a critical technical reference and a valuable resource to nuclear regulators, policy makers, facility operators, and the public. INFCIRC/225 establishes the common terminology and methodology for physical protection and allows for effective communication between experts in different countries.

Although INFCIRC/225 has the nature of a recommendations document, some countries are known to use it as a more formal physical protection standard to address domestic security or international nonproliferation requirements. Indeed, INFCIRC/225 is frequently referenced in peaceful nuclear cooperation agreements between countries; some countries incorporate the document in their domestic nuclear security regulations; and some adopt it as an export licensing requirement. Additionally, IAEA uses INFCIRC/225 as a minimum physical protection standard in its Project and Supply Agreements and IAEA teams utilize the document during International Physical Protection Advisory Service missions.

Facility-level evaluations of physical protection measures against the recommendations in INFCIRC/225 therefore may need to be performed on certain occasions. This paper argues that any such evaluation should seek to determine whether the physical protection measures meet the intent of the INFCIRC/225 recommendations as opposed to using direct word-for-word comparison of the conditions on the ground to the text of the document. This approach recognizes the importance of country- and facility-specific circumstances (such as the threat environment or historical context) and acknowledges that there is frequently more than one way to establish an effective nuclear security system. Additionally, at times, strengths of the security system in some areas may compensate for its weaknesses in others.

Operating experience and discussions with international physical protection experts suggest that INFCIRC/225 evaluations are not always straightforward or easy. The application of INFCIRC/225 recommendations at a facility level must take into account facility-specific features and conditions.

Additionally, the document itself contains ambiguities and generalities that call for a nuanced and technically-credible interpretation of some of its recommendations. For example, practical measures for implementing the recommendation that "[V]ehicles, persons and packages entering and leaving the . . . area . . . should be subject to search . . . as appropriate" require consideration of the risk significance of nuclear materials, credible scenarios of malicious activities, and other factors.

INFCIRC/225 recommendations address both national programs (such as a legal and regulatory framework for physical protection) and facility-level physical protection measures. This paper focuses on the latter. In particular, it discusses common issues and best practices related to the interpretation of INFCIRC/225 recommendations in the following areas: designation of facility security boundaries, entry and exit security searches, nuclear material and nuclear facility categories, vehicle barriers, alarm stations, secure communications, response force exercises, and sabotage analysis.

The paper concludes that a successful facility-level assessment of the physical protection measures against the recommendations in INFCIRC/225 must include both consideration of physical protection fundamentals (such as access control, and detection, assessment, and response functions) and an effective interpretation of INFCIRC/225 recommendations. The operator's ability to look at their facility from the INFCIRC/225 perspective and to articulate how the security measures and procedures relate to the document's recommendations is also highly valuable.

Synopsis ID: [272]

Uganda's Experience in the Implementation of the CPPNM and its Amendment

Luwalira, N.[1]

[1] Atomic Energy Council, Uganda

Corresponding Speaker: N. Luwalira

Uganda became a member of the International Atomic Energy Agency (IAEA) in 1967 and acceded to the CPPNM in 2003 and has not ratified the its Amendment as of May 2017. There was some degree of delay for Uganda to ratify the amendment to the CPPNM which came into force in 2016. However, there has been progress in the implementation of the convention in Uganda. The implementation requires the commitment of the state and the involvement of several government institutions at different levels coupled with the support of international community and the IAEA. . So far Uganda has no nuclear materials to be reported to the IAEA as required by all member states although preliminary surveys indicate the possibility of the existence of uranium deposits in some parts of the country.

Uganda also keeps an inventory of all radiation sources and any nuclear materials in the country by the regulator, the Atomic Energy Council. These sources are used in various applications in medicine, industry, agriculture, research and education. Until 2011, there was only scanty information regarding the quantity of nuclear materials as well as the number and category of radioactive sources in Uganda when a registry was established. There have been incidents of orphan and disused sources out of regulatory control ending up in unauthorized possession. This posed a nuclear security threat in the country that required to be addressed partly through the implementation of the provisions of CPPNM and its amendment. These nuclear materials and radioactive sources if not managed safely and securely protected, pose high risk to human health and the environment.

Despite the benefits and risks associated with nuclear materials and radioactive sources, there was no effective regulatory infrastructure to control these sources until 2008 when the Atomic Energy Act No.24 ofn2008 was enacted. The coordination and follow up on the implementation of the CPPNM and fast tracking the ratification of the amendment to the CPPNM in Uganda depended largely on the national legal systems and framework. The implementation of the CPPNM and its implementation required the commitment of government and all its institutions and agencies both at the national and international levels. In order to fully implement the provision of the Convention and its amendment not only required the international cooperation but also requires a review of the national local laws for domestication purposes. In particular a review of the Uganda Penal Code Act Cap 120 and the Atomic Energy Act No. 24 of 2008 are necessary to establish the offences and penalties that emanate

from the implementation of the CPPNM and its amendment. Although there is usually a long process of domesticating international conventions, treaties and protocols and the involvement of the executive and the parliament from the operational up to the policy levels, it is a necessary and an indispensible procedure to be under taken by the state.

The implementation of the CPPNM and its amendment therefore requires the establishment of a strong legal and regulatory framework that support all oversight mechanisms on the applications and movements of all nuclear materials and all radioactive sources. Efforts are required to be made for Uganda to assent to the IAEA conventions and treaties in the area of nuclear Security to effectively implement the requirements in the CPPNM and its amendment as well as in the IAEA Code of Conduct on the Safety and Security of Radioactive Sources and its associated Guidance to which Uganda gave political support in 2014. This would enhance Uganda's regulatory oversight and security of nuclear materials and other radioactive sources and as such contribute to the global nuclear security regime.

Key words: Amendment, radioactive sources, inventory, Implementation

Synopsis ID: [14]

The Physical Protection of Nuclear Materials and Ionizing Radiation Sources in Chad

Alifei, M.[1]

[1] Chadian Agency of Radiation Protection and Nuclear Security (ATRSN), Chad

Corresponding Speaker: M. Alifei

The Chadian Agency of Radiation Protection and Nuclear Security (ATRSN) is the regulatory authority for radiation protection and nuclear security in the Republic of Chad. It was created by Law No. 002 / PR / 2008 on Radiological Safety, Nuclear Security and Guarantees. Chapter 4 of the Act sets out the conditions and obligations for ensuring the physical protection of nuclear substances and ionizing radiation sources. Obligation of the State and of establishments using nuclear materials. In Chad, the State ensures physical protection of radioactive substances during importation, exportation, transit or transport in accordance with international requirements. Therefore, the Government assigned to the ATRSN the responsibility: To establish sustained cooperation in this field with the other Member States and the IAEA In order to maintain rigorous control of movement of nuclear substances. In the case of lost, theft or diversion of a radioactive source or nuclear material, the licensee should inform the ATRSN and the gendarmerie or police authorities within a period of 24 hours. The licensee should therefore put in place a system for the physical protection of radioactive substances and sources of ionizing radiation. Any transfer of radioactive substance or ionizing radiation sources may only take place between right persons authorized by the ATRSN. The transmission of confidential information on measures of Physical Protection to an unauthorized person is prohibited in Chad. The above-mentioned Act clearly identifies the ATRSN as the competent authority and assigns its role and responsibility to regulate activities involving ionizing radiation sources and radioactive substances. Therefore, it is responsible for: - Inspect installations and activities involving ionizing radiation. - Issuing, Renewal, Modify, Suspend or Cancel; - Ensure, in collaboration with relevant institutions, of compliance with international legal instruments relating to nuclear safety and security; - Define with the institutions concerned the threat in the field of Nuclear Security; - ATRSN coordinates with the institutions concerned all activities related to the implementation of a national strategy to regain control of orphan sources; - This is subject to the discretion of the Government. National Register of Ionizing Radiation Sources:

According to the national inventory of of ionizing radiation sources carried out between 2013 and 2015, Chad has recorded 134 sources and distributed as following: Category II, III, IV and V sources are used in Chad: Category II: 10 Category III: 14 Category IV: 62 Category V: 48 These radioactive sources are recorded in the RAIS 3.3 Web system and periodically updated. Administrative and technical measures implemented in Chad for physical protection include duly signed and confirmed

authorizations, video surveillance, and dual key system held by different persons and the presence of law enforcement agencies all around the sites.

Synopsis ID: [76]

Sanctions as a Legal Deterrence Mean in the National Physical Protection Regime

Elsisi, F.[1]

[1] Egyptian Nuclear and Radiological Regulatory Authority (ENRRA), Egypt

Corresponding Speaker: F. Elsisi

States seek to protect nuclear materials and facilities under its jurisdiction from theft, sabotage and other malicious acts during use, storage and transport through establishing, implementing, maintaining and sustaining an effective physical protection regime. The State's physical protection regime – as mentioned in (NSS 13), (INFCIRC / 225 / R.5) - should seek to: - Prevent any malicious act by means of deterrence and by protection of sensitive information, - Manage an attempted malicious act or a malicious act by an integrated system of detection, delay, and response, - Mitigate the consequences of a malicious act. One of the means to prevent criminal or intentional unauthorized acts involving or directed at nuclear material and facilities and also to deter adversaries - as mentioned in CPPNM and its amendment - is to criminalize such acts and to impose an effective and appropriate sanctions under national law, whether the offence was completed or just an attempt to commit it. Physical protection regime strategy - as a part of nuclear security regime – relies on two elements to achieve its objectives, the first one is to deter the adversary and the other is to defeat him. Both elements will not be achieved on their own just like the crime will not disappear on its own, there must be sufficient means to do that. We cannot deny the importance of sanction and its role in deterring adversaries, reducing potential threats and preventing adversaries from committing criminal acts. Sanctions is the mean by which individuals are forced to respect the law, not to commit criminal acts so as not be punished and to prevent a person's criminal motives from coming to human society because of the fear of pain that will be caused by sanctions.

If sanctions succeed in creating a sense of fear, we will have sufficient real deterrence to prevent commission of offences. Deterrence has more than one type and can be achieved by more than one mean, but this paper will address deterrence of sanctions. Attempting to commit a criminal act reveals that deterrence has not been achieved either by sanctions or by physical protection measures, so deterrence comes first before prevention, in this context, this paper will explains the difference between deterrence and prevention despite their similarity A lot of challenges facing sanctions in deterring adversaries such as non-knowledge of sanctions, (how can deterrence be achieved for a potential adversary from something he does not know?!), or the inadequacy of sanctions with the serious nature of offences and their consequences, or ineffective sanctions to deter recidivists in some cases and other challenges facing sanctions in deterring adversaries. This paper will address these challenges and their solutions. This paper will also explain contribution of appropriate sanctions together with protection of sensitive information and nuclear material accounting and control system

in reducing the risk of insiders. Especially as countries rely heavily on strict sanctions to protect public funds against their employees. Egyptian legislator relied on the purpose and time of committing the offence and its consequences in determining sanctions for offences involving or directed at nuclear material and facilities and in estimating their suitability. Finally I will conclude with a set of recommendations that may contribute to and support sanctions in achieving sufficient deterrence for adversaries in the national physical protection regime.

Synopsis ID: [89]

Current Nuclear Security Regime in Japan-Efforts for Compliance with NSS-13 and CPPNM Amendment-

Uetake, N. [1], Miyamoto, N. [1]; Kuroki, M. [1]

[1] Nuclear Regulation Authority, Japan

Corresponding Speaker: N. Uetake

NRA, Japan was established as the only independent regulatory body for nuclear safety and security in 2012 after the accident in Fukushima Daiichi Nuclear Power Station. NRA, Japan has improved the Japanese nuclear security regulation based on NSS-13 in order to respond public requirements for prevention of radiological consequence from any nuclear incidents.

Main points of current Japanese nuclear security regime,

Performance based approach The operators should develop the nuclear security plan (NSP) for their nuclear facility based on State's requirements containing DBT if applicable. NRA reviews and approves their NSP. The operators should constantly review and improve their physical protection system using PDCA (Shewhart) cycle. NRA should check the operators' activity in the inspection. Using this approach, site specific improvement by the operators themselves can be realized.

Risk informed approach NRA prepares DBT by cooperation with the police and the Japanese coast guard. The operators who have Cat.I nuclear materials or possibility of radiological consequence over URC by sabotage should protect their facilities to meet DBT provided by NRA. NRA doesn't use HRC and URC is an only threshold of radiological consequence for graded approach.

Defense in Depth NRA requires operators to set newly the limited access area over conventional areas based on NSS-13. Moreover, NRA also requires operators a barrier, intrusion detector and CCTV at the border of the limited access area with consideration for earlier detection and sufficient delay for intruders.

Computer security NRA has developed regulatory requirements and the related guidance for cyber security programs of nuclear facilities. NRA requires operators to use standalone systems for sensitive information management systems and physical protection systems. And also NRA requires to adopt one-way data control system and defense in depth for important I&C systems. Life cycle management is also required for insider threat.

Response force As any private guards cannot have firearms in Japan, guards in the nuclear facility are composed non-armed guard. Therefore, State has installed police special force in nuclear facilities as an onsite armed response force.

Insider threat mitigation NRA requires operators to implement strict two person rule using access control systems or constant surveillance by CCTV for access to vital equipment. It had been difficult to reach consensus for trustworthiness check by the State for long period. However, after publication of NSS-13, NRA has established a policy of trustworthiness check for nuclear facilities.

Exercise The operators are required regular implementation of exercise with response force in the nuclear facilities. NRA and the police jointly evaluate the result for future improvement.

Nuclear security culture After Fukushima Daiichi Accident, awareness on the safety first has been[U+3000]permeated. NRA is also cultivating “nuclear security culture”. The operator’s “effort” to foster nuclear security culture is required by regulation in Japan. And NRA also developed the “Code of Conduct on Nuclear Security Culture” for NRA staff in January 2015. NRA commissioners hold regular dialogues on nuclear security culture with top executives of the operators.

Criminalization of malicious acts Japan newly developed “Act on Punishment of Acts to Endanger Human Lives by Generating Radiation” to supplement Penal Code. This act prescribes penalty for any radiation generation by malicious act containing preparation, attempt etc. Japan deposited the instrument of acceptance of the CPPNM Amendment in 2014 as a result of these efforts.

NRA has developed nuclear security regime using performance based approach based on NSS-13 not only for solid compliance with the CPPNM Amendment but also for reliable protection of the nuclear facility and people around the facilities.

Synopsis ID: [184]

Nuclear and Aviation Security - A Comparative Analysis

Howsley, R.[1]

[1]World Institute for Nuclear Security (WINS)

Corresponding Speaker: R. Howsley

Aviation and nuclear security share many similarities and objectives, and some notable differences, but there ha;s never been a comparative analysis of the security arrangements in these two sectors. The World Institute for Nuclear Security (WINS) is leading a joint team from the aviation and nuclear sectors to benchmark arrangements in the two sectors for the first time. The study is addressing the way in which threat assessments are conducted in the two sectors, the approaches to regulation and security management, the extent to which issues such as cyber security are regulated and implemented, and the effectiveness of the international verification and audit arrangements. This paper will provide an update to the conference on the current status of the benchmarking programme.

At international level, both the aviation and civil nuclear sectors have specialised UN agencies that oversee the international standards and recommendations for the State-level safety and security regimes. On the one hand, the International Civil Aviation Organization (ICAO), based in Montreal, Canada, oversees aviation safety and security and on the other, the International Atomic Energy Agency (IAEA), based in Vienna, Austria, has a comparable role for civil nuclear safety and security. Both were established over 60 years ago, ICAO in 1944 and the IAEA in 1957.

However, one important distinction between these organisations has been their approach to the formulation and imposition of safety and security "standards". ICAO sets mandatory standards for both aviation safety and security. The IAEA's role is different, in that it establishes voluntary recommendations and guidance for nuclear safety and security which can be interpreted and implemented according to each State's preferences, including the provisions of the Convention on the Physical Protection of Nuclear Material and its 2005 Amendment which came into force on the 8th May 2016.

Another difference is that ICAO conducts mandatory inspections of each State's aviation security arrangements, called the Universal Security Audit Programme Continuous Monitoring Approach. The decision to introduce mandatory standards and an international audit programme was made by ICAO immediately following the terrorist attacks in the USA in September 2001. The High-level, Ministerial Conference on Aviation Security (19-20 February 2002) endorsed a global strategy for strengthening aviation security worldwide, adopted a number of conclusions and recommendations,

and issued a public declaration. A central element of the strategy was an ICAO Aviation Security Plan of Action, which included regular, mandatory, systematic and harmonized audits to enable the evaluation of aviation security in all Member States. Results from these audits are published so that all Member States can view the findings on a restricted website.

The IAEA has also taken measures since 2001 to enhance the security guidance available to its Member States and has increased its activities and budget, largely through voluntary funding. A significant proportion of its current budget is spent on providing awareness courses on nuclear security that are run at both national and international level but, unlike ICAO, the IAEA does not provide certified courses for nuclear security practitioners. In 2004, ACI (Airports Council International) and ICAO established a formal partnership to provide a universally available management training programme for the global airports community. Their Aviation Security Professional Management Course is the most advanced aviation security training programme in existence and carries a formal certification (AVSEC PM). The programme aims to provide aviation security middle and senior management personnel with new management skills that have become mandatory in today's aviation environment, as aviation security management personnel are required to perform more complex and diverse tasks and display greater communicative and management skills to meet new and emerging threats to civil aviation.

The differences in the way the international community has addressed aviation security compared to nuclear security are striking. Aviation security has international minimum standards to which States must comply, an independent audit programme to verify compliance, the publication of audit results to all Member States, and a professional certification programme for security for personnel with accountabilities for aviation security. By comparison, the arrangements for civil nuclear security look immature. However, first impressions could be deceptive; some might argue that the continued failures in airport and airline security could point to a less than rigorous oversight and implementation security programme. The extent of the "minimum standards" for aviation security might be poor, and States may be able to find exceptions so as not to comply. The audit arrangements could be superficial or delegated to State or regional entities. Subjects like cyber security and human reliability (vetting) might be excluded from the scope of the aviation standards.

The review described here aims to address these issues, to better inform both sectors and thereby contribute to an improvement in aviation and nuclear security.

Synopsis ID: [273]

A Model for Performance Based Method for Designing a PPS

Sharma, G.[1]

[1] Department of Atomic Energy, India

Corresponding Speaker: G. Sharma

Nuclear renaissance and growth of nuclear programmes is vital to combat climate change challenges. Taking cognizance of the threat posed by potential nuclear terrorism, global efforts have been initiated to address this issue. Nuclear Security is the prevention and detection of, and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear material, other radioactive substances or their associated facilities [1]. One of the most important part of nuclear security is the physical protection of nuclear material and nuclear facilities. The WTC event on September 11, 2001, in the US had led the world to rethink and improvised its approach for design, implementation and assessment of PPS for nuclear material and facilities. In the conventional PP approach, this event could not have been thought of as design basis threat because its occurrence probability was very low. This event proved the "risk" is pertinent and deterministic. Deterministic threat perception is based on zero risk and hence require well-defined performance based approach. IAEA had also stressed on a performance-based approach, in addition to prescriptive-based approach serving as the basis for PPS in INFCIRC/ 225/Rev.5 (Rev.5) [2]. This paper proposes a model for performance based method for designing a PPS for a facility.

The prescriptive and performance based approach are being used for various fields like fire safety analysis, civil engineering etc. The same philosophy can be explored for designing a PPS for nuclear material and nuclear facility. "Prescriptive" or specification-based approach for physical protection is based on how a system should be designed, implemented and maintained. This could be done by using design parameters that prescribe (describe) what is to be protected, what are requirements for protection, how these requirements are to be met, and how compliance is to be verified. A performance-based approach, on the other hand, is broader and detailed. It does not limit the design parameters to only prescribed functional details. Rather, it relates the design and performance under certain conditions; how well a system performs in defeating a defined adversary with protection in depth concept, minimum consequence of failure and a balanced protection based on preset performance objectives. For nuclear facility and nuclear material, designing a PPS depends on a number of parameters with well-defined functional details laid out by regulator. The operator must comply and should designs the PPS to meet these requirements in an economically efficient manner by judiciously selecting the use of either prescriptive or performance-based approach.

An approach for prescriptive and performance based model for designing a PPS for a nuclear facility has been envisaged by the authors is shown in Fig.1. In this model, the competent authority can make a decision to choose between prescriptive or performance based methods depending on design parameters [Fig.1]. If the design requirements are prescriptive in nature,

e.g. for transportation of NM (cat. I), if the prescribed requirement is to provide X no. of security guards to deter the adversary, then prescriptive based method should be selected. In this method, outcome is deemed to satisfy solution as inputs are more prescriptive and standard in nature. However, if the design parameters are based more on performance criteria, e.g. for transportation of NM (cat. I), design matrices defined are : alerts or signal the presence of adversary through N no. of ways after detection, delay the progress of an adversary using different methods, immediate effective response with minimum response time, well equipped and trained response forces to control the adversary in minimum time, N no. of response forces (on site guards, off-site police or military personnel) etc. than PPS should be designed on performance based approach. For performance based method, the outcome is a solution to achieve a desired condition, the prevention of an undesired condition, or satisfying the acceptance criteria. This paper also presents an iterative - model of performance based method used for designing a PPS for a nuclear facility as shown in Fig 2. This method requires a performance criteria metrics based on which performance should be evaluated, measured, predicted, and evaluated for compliance with goals, functional objectives; these criteria are integral to a performance-based system.

Reference

IAEA, Nuclear Security Glossary 2010 Ed.

IAEA, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities, IAEA Nuclear Security Series No. 13, Vienna (2011).

Synopsis ID: [136]

Security Layer Failures and Integrated Dependency

Maxwell, B.[1], Greenhalgh, D. [1]

[1] Department of Energy, United States of America

Corresponding Speaker: B. Maxwell

The physical protection against unauthorized removal of nuclear material and against the sabotage of nuclear facilities or transports has long been a matter of international concern. A fundamental design principle used to protect against sabotage and unauthorized removal is Defence in Depth, which is defined in INFCIRC/225/Revision 5 as "the combination of multiple layers of systems and measures that have to be overcome or circumvented before physical protection is compromised." Each layer may consist of a combination of personnel procedures, structural or physical, and/or organizational entities. Within each layer, detection, assessment, delay, and response should form an integrated system designed to allow response forces advantageous engagement with the adversary. A complete layered design provides a set of independent delay, detection, and response capabilities intended to increase the difficulty (time, tools, and/or knowledge and expertise) required for an adversary to obtain unauthorized access and control of target materials. Typically, each layer of the protection system integrates multiple physical components and procedures (which may vary from one layer to the next), and each layer operates independently of all others so in the event that one layer is circumvented or breached, the other layers continue to function as designed. Layers are designed and deployed to mitigate inherent vulnerabilities of detection and delay equipment within each layer as well as other layers. For example, if an adversary attempts to penetrate an outer layer by trying to defeat a particular delay system (and the associated detection system), other means of detection and delay at this layer (and all other layers) continue to function and provide for the planned tactical response. If all detection at this layer were compromised, defeat of the delay barrier would occur without responder notification and the contribution of that layer to overall protection effectiveness would be negated. However, the expectation is that the inner detection and delay layers are not affected, and reasonable protection system performance is maintained through the inherent redundancy of the overall system design. Unfortunately, reality can be much different. In many cases, the components within and among layers are not independent because they rely on shared infrastructure and characteristics. The loss of a single protection element (for example, detection) within an outer layer of protection may directly impact the overall system effectiveness more than might be expected. Security layers are not truly independent and protection system effectiveness predictions based solely on removing the affected component at the individual layer (as is sometimes assumed in simulation and modelling) could significantly overestimate protection system effectiveness. Interior and exterior detection and assessment components, though placed in multiple locations, may share common installation methods, communication protocols, network infrastructure, and power sub-systems. A fault or attack against one of these may disable or degrade similar

components in one or multiple layers and therefore the assumption of redundancy and independence is speculative, and detection probabilities may be substantially reduced and warning times for response forces may be decreased or become inadequate. This is further compounded by the fact that the response function(s) are generally provided by personnel who rely on detection and assessment to initiate a response to counter the adversary threat. This means that the design functions of detection, delay, and response are serial in nature and must be provided in that order for the entire system to be effective. If one of them is removed at one or more layers, the system effectiveness rapidly diminishes. In this case, a response is less likely to be successful because detection or delay may not be provided within the time period needed for an effective and timely response. Since protection layers are not truly independent, performance testing focused primarily on component or individual layer testing may be inadequate. Performance testing is generally accomplished on individual components or layers (e.g., intrusion detection systems or the protective force) within a narrow focus, such as a force-on-force exercise that assumes effective exterior intrusion detection system. The exercise may only validate layer components independently. If testing is completed in a similar manner at each layer, on each component, the fallacy of system effectiveness is perpetuated. Many potential solutions to this problem exist, but, whatever solution is adopted, it is vital that performance testing includes an evaluation of overall protection system performance by viewing all security layers (and therefore their associated functions of detection, delay, and response) as an integrated system, in addition to the testing conducted on individual components or layers. Performance testing conducted with the assumption that determining the performance of components and/or layers individually can give a false sense of security when interdependencies exist. When security layers are dependent on each other (including their common failure modes), the common failure modes are not typically addressed when determining system effectiveness through modeling and simulation and performance testing.

Synopsis ID: [140]

The Best Practice of Acceptance Test for Physical Protection System at Nuclear Facility

Zhao, Z.[1], Han, Y. [1], Chen, H.[1]

[1] State Nuclear Security Technology Center (SNSTC), China

Corresponding Speaker: Z. Zhao

This paper discussed the definition of Site Acceptance Test for Physical Protection System at nuclear facility, and analyzed the connection and difference between Site Acceptance Test with project acceptance, and site assessment (including nuclear security inspection, physical protection system effectiveness evaluation, etc.). By analyzing the long standing issues that exist in operation, maintenance, inspection and assessment, the necessity of carrying out the acceptance test in the following aspects was pointed out: change of threat situation, update of the regulations and criteria, improvement of design, remedy of the shortages of equipment, clarification of units of responsibilities and deadlines, and protection of owners' rights and interests. Based on the physical protection system of mock facility in the Center of Excellence on Nuclear Security in China, the acceptance procedures and field work forms are developed. By listing the existing (e.g., State Council Decree No. 412, National and Industrial Standards including GB50348, GB10408 and EJ1054, as well as technical guidance including HABD and HAD Series) and currently-being-prepared (e.g., regulation of Physical Protection System Acceptance of nuclear facility) legislative and regulatory documents for physical protection system acceptance test, the establishment of one integrated system of management and legislative and regulatory documents was proposed, which would significantly insure the effectiveness and the legitimacy of acceptance test. Methods of Physical Protection System Test and Assessment of nuclear facility that are most commonly used at present are introduced and at the same time, the advantages and disadvantages were analyzed. A portable acceptance test kit was developed by State Nuclear Security Technology Center. The shortcomings of current acceptance tests criteria was elaborated. Future outlook of follow-up work was also analyzed.

Synopsis ID: [86]

U.S. Department of Energy Alternate Protection Strategy for Nuclear Fuel Elements - Description of an Alternative Approach for Analyzing the Protection of Nuclear Fuel Elements

May, M.[1], Sparks, M. [1], Pocratsky, Carl [1]

[1] Department of Energy, United States of America

Corresponding Speaker: M. May

Limiting terrorist access to nuclear materials has been an objective of the international counterterrorism and non-proliferation communities for decades. The United States participates in these communities and has endorsed this objective through significant investments and established safeguards and security programs for nuclear materials. Sites and facilities owned by the US Department of Energy (DOE) and the National Nuclear Security Administration (NNSA), and that possess nuclear materials, are required to protect those materials from specified threats and attack scenarios. The protection requirements are defined by DOE policies using a graded approach, and consist of a combination of prescriptive, or "compliance-based" requirements, and "performance-based" requirements that often prompt significant analysis and testing. These requirements are aligned substantially with the safeguards tables used by DOE and the International Atomic Energy Agency (IAEA).

In the case of spent nuclear fuel a significant security system design consideration is that highly irradiated fuel can sometimes be considered "self-protecting" when it is sufficiently radioactive to ensure a high probability of failure of tasks that an adversary would carry out during an attack. In 2011, in recognition of terrorist willingness to commit suicide during an attack, DOE revised its Nuclear Material Control and Accounting Order definition of "highly irradiated nuclear material" for determining the amount of radiation that must be emitted for spent fuel to be considered self-protecting. In many cases this has resulted in a need to re-evaluate protection strategies to meet today's threat environment, often at great cost. Many sites have not taken full advantage of the flexibility of DOE policies, which allow for alternatives to be considered, instead of using a traditional "one-size-fits-all" approach.

After evaluating several site requests to deviate from protection requirements for nuclear fuel elements, the U.S. DOE Office of Security decided to document the key factors or points that each deviation was evaluated against, including inherent factors and features of the fuel that a site could

consider and possibly take advantage of without sacrificing security or increasing overall risk. These documented evaluation points have evolved into the "Alternate Protection Strategy (APS) for Nuclear Fuel Elements".

The APS captures evaluation points, associated criteria, and numerical criterion that, when summed, provide an indication of protection adequacy, and if a site may/may not have a valid argument for using an alternate protection strategy for their nuclear fuel elements. The strategy evaluates the following fundamental protection questions that a site should consider: [U+2500] Do I have fissile material that is a concern? [U+2500] Is the material attractive to an adversary? [U+2500] Will I know if someone is attempting to steal the material? [U+2500] Is the material difficult to access or gather? [U+2500] Can a theft in progress be stopped? [U+2500] Is my protection system balanced?

Quantitative scores for each of these questions are determined by criterion in the APS, and minimum allowable scores in each area are also established to ensure that balanced protection can be achieved.

The initial focus of the APS is on the theft of fuel elements containing safeguards Category I or II quantities of special nuclear materials. The APS is ultimately intended to serve as a guide for both the HQ staff that must evaluate proposals to deviate from policy requirements, and for field personnel that must prepare and submit the deviation proposals. It highlights how sites might be able to take credit for inherent protection properties of their fuel that may already exist, making them unattractive targets for an adversary. It identifies parameters from multiple safeguards and security functions – NMC&A, physical protection and vulnerability/security risk analysis, and integrates them into a single resource or tool. The APS results provide an indication that a site may, or may not, have a good argument for using an alternate protection approach. However, adequate protection must still be demonstrated and confidence must be established that a defined adversary will not be allowed to remove the nuclear material from the site.

The APS is currently a working concept that is used by the Office of Security to evaluate deviation requests from security requirements, and is available to DOE and NNSA programs and facilities for use. It is the intention of the Office of Security to work with our sites to continuously update and improve the APS as an internal planning resource for the Department. This paper will provide a general description of the U.S. DOE APS including key concepts, evaluation criteria, guiding principles, benefits, uses, and next steps.

Synopsis ID: [79]

Changes in the Croatian Legal and Regulatory Framework for Physical Protection

Medić, M.[1], Medaković, S. [1]

[1] State Office for Radiological and Nuclear Safety (SORNS), Croatia

Corresponding Speaker: M. Medić

State Office for Radiological and Nuclear Safety (SORNS) is the regulatory body entrusted with the implementation of the legislative and regulatory framework. The SORNS, as the state administration body, is the competent authority for all activities pertaining to radiological and nuclear safety, as well as for the activities pertaining to physical protection of nuclear and radioactive material. In Croatia, the issues related to the physical protection of nuclear and radioactive material are covered by the Act on Radiological and Nuclear Safety and Ordinance on the Physical Security of Radioactive Sources, Nuclear Material and Nuclear Facilities. In line with changes on the international security scene and the growing risk that nuclear or radioactive material could be used with malicious intents SORNS has decided to conduct a thorough review of the legal framework in the field of physical security of nuclear material and radioactive substances. The process goes hand in hand with the Amendments to the Act on Radiological and Nuclear Safety that are being implemented for harmonization with the European Council Directive 2013/59/EURATOM. This provides the basis for development of a new approach to the security of nuclear material and radioactive substances. The current licensing process requires from the Operator to create the Security plan that is not based on the threat assessment and DBT. Also, the current regulatory framework requires minimal involvement of law enforcement and intelligence services throughout the process. As a result, the current mode of physical protection planning is not fully aligned with international standards and is not adapted to new forms of threat. Without proper communication and coordination between law enforcement and intelligence services on one side and SORNS on the other there is no data exchange and planning and implementation of common measures and activities. The new Ordinance on Nuclear Security introduces, along with numerous new terms such as threat assessment, DBT, contingency plan, cyber security plan, nuclear security culture, etc., the obligation of security vetting of all employees working with sources of category 1, 2 and 3 as well as with the nuclear material. This new obligation will not be well received among license holders. To somehow stimulate the necessary cooperation, SORNS has taken the initiative and asked for help from international experts from Sandia National Laboratories in organizing a workshop that would bring the planned changes closer to law enforcement and intelligence services. Opinions of the workshop participants about their new future commitments were very different.

Synopsis ID: [268]

Legal Element for Physical Protection Regime Sudanese as Case Study

Mahmoud Hamid Mohammed Ali, M. [1]

[1] Sudanese Nuclear & Radiological Regulatory Authority

Corresponding Speaker: M. Mahmoud Hamid Mohammed Ali

This paper deals with legal bases for nuclear security focus on physical protection regime first, its analysis the international legal framework for nuclear security (PPS) AND analysis the legal bases for import and export control of nuclear or radioactive sources the purpose of the paper is to evaluation the Sudanese legal framework for nuclear security (physical protection). Including requirements for PPNM

Introduction:

term 'nuclear security' is generally accepted to mean "the prevention and detection of, and response to, theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear material, other radioactive substances or their associated facilities") The State responsibility is to establish and maintain legislative and regulatory framework for nuclear security, define what the nuclear security and establish or designate a competent Authority responsible to implement and control framework for nuclear security (2). The operators' responsibility is to implement and enforce the laws and regulations, establish guidance documents implementing security requirements of national laws and regulations relevant to their specific activities, establish and implement security plans and procedures based on the national laws and regulations. There is a new international nuclear security framework is emerging () based on obligations contained inthe Convention on the Physical Protection of Nuclear Material (CPPNM) and its Amendment, the International Convention for the Suppression of Acts of Nuclear Terrorism, the relevant Security Council resolutions and the non-binding Code of Conduct for the Safety and Security of Sources and its supplementary Guidance 4

Synopsis ID: [122]

The Development of Guidelines for the Transport of Nuclear Material in Germany

Wiesbaum, A.[1]

[1] Federal Office for the Safety of Nuclear Waste Management, Germany

Corresponding Speaker: A. Wisebaum

In Germany most of the Nuclear Material is transported on the road or by railway. In order to get a licence for a transport of Nuclear Material the carrier has to prove, that his measures fulfill the requirements on physical protection of the carried material and the requirements on the personnel involved in the process of the transport named in the national guidelines. The guidelines for the use, the storage and also the transport of Nuclear Material are based on the national design basis threat (DBT). The German DBT is created by a cooperative working group of members of the state and the federal states (Bund and Länder) and is reevaluated not less than every 3 years. That means, that also the guidelines are revised frequently. This year a new guideline for the transport of Nuclear Material via road or railway came into force in Germany. Additionally a new guideline for the personnel involved in a transport of Nuclear Material via road or railway was created. This talk is about the development of guidelines for the transport of Nuclear Material in or through Germany. The focus of this talk will be the process of the development of new guidelines and the main differences between the old guideline for the transport of Nuclear Material und the new enforced one. For the creation of a new guideline the Federal Ministry of Environment, Nature, Conservation, Building and Nuclear Safety is responsible. The Ministry takes into account the actual DBT and information given by the Federal Criminal Police Office and the Federal Office for Information Security. A working group consisting of members of the Bund and Länder is created for the purpose of writing the new guideline. Analogue to the international rules, the transported Nuclear Material in Germany is graded into three categories. Depending on the category the security requirements for the transportation of the material differ. Each chapter of the new guideline for the transport of nuclear material via road or railway deals with a specific vehicle type, like car or waggon, used for transport. There is also a chapter about a transportation control room, which is necessary in every case. Each chapter lists requirements for the three different categories of Nuclear Material. There are also chapters for organizational measures and measures for the cooperation with the police, which have to be fulfilled by the carrier. In Germany it is also necessary to hand in a contingency plan to get a licence for a transport. The new guideline for the transport of Nuclear Material via road or railway differs from the previous ones in many details and two big points. The first main difference is a new protection goal in the guideline. So far in Germany the protection goals in the guidelines for transport were listed as: prevention of the release of radioactivity from the transport cask (1) and prevention of the theft of Nuclear Material (2). The new guideline for the transport of Nuclear Material also contains

the protection goal: prevention of the release of radioactivity at a different place after the theft of Nuclear Material (3). The second new point is a new and additional categorization of the Nuclear Material taking into account the possibility of a release of radioactivity. If the transported material is categorized as release-relevant, additional measures are necessary. This leads to a whole new set of calculations, additional physical barriers and higher requirements for all parts of the transport.

Synopsis ID: [216]

Rostechnadzor Experience in the Use of the IAEA Recommendations during Improvement of the Regulatory Framework for the Physical Protection of Nuclear Material and Nuclear Facilities

Ivanov, M.[1]

[1] Federal Environmental, Industrial and Nuclear Supervision Service of Russia, Russian Federation

Corresponding Speaker: M. Ivanov

Nuclear Security Fundamentals [NSS 20] defines a set of nuclear security activities that establish and maintain the effective nuclear security regime within a State. One of such activities is the physical protection of nuclear material and nuclear facilities. Usually, physical protection of nuclear material and nuclear facilities is established at two levels – State's and Site's. At the State level the form and content of physical protection are defined by policy makers and competent authorities who regulate physical protection of nuclear material and nuclear facilities.

In the Russian Federation an authorized body of safety and security regulation in atomic energy uses (a federal state supervisory body in the field of atomic energy uses) that also regulates physical protection of nuclear material and nuclear facilities is the Federal Environmental, Industrial and Nuclear Supervision Service (Rostechnadzor). Rostechnadzor is a competent authority of the Russian Federation under the Amendment to the Convention on the Physical Protection of Nuclear Material. As the regulatory body Rostechnadzor develops legislative and regulatory framework, establishing requirements for physical protection and reflecting features of processes of licensing and inspections related with physical protection.

The paper will contain basic statements of physical protection regulation for nuclear material and nuclear facilities in the Russian Federation, requirements for physical protection of nuclear material and nuclear facilities established in the unique Series of normative and legal acts developed by Rostechnadzor – the Federal norms and rules in the use of atomic energy. Since the Federal Law of the Russian Federation No. 170-FZ of 21.11.1995 "On the Use of Atomic Energy" establishes the obligation to take into account international recommendations when Federal norms and rules are developed and improved, the paper will present the experience of Rostechnadzor on the application of the IAEA recommendations in improving the regulatory legal framework for physical protection of nuclear material and nuclear facilities. In particular, changes that had been made in Federal norms and rules of NP-083-15 "Requirements for physical protection systems for nuclear materials, nuclear facilities and storage facilities for nuclear materials", among other things, for harmonization with

IAEA recommendations on the Nuclear Security Series will be discussed in the paper. The paper is focused, first of all, on the representatives of regulatory bodies in the IAEA Member States both with the already established regulatory infrastructure and for the newcomers in the nuclear industry.

Synopsis ID: [258]

U.S. Nuclear Regulatory Commission Safety and Security - Policy and Oversight

Sieracki, D.[1], Thompson, C. [1]

[1] Nuclear Regulatory Commission, United States of America

Corresponding Speaker: D. Sieracki

The NRC recognizes that it is important for all organizations performing or overseeing regulated activities to establish and maintain a positive safety culture. The NRC's approach to safety culture is based on the premise that licensees bear the primary responsibility for safety. The NRC addresses safety and security through expectations detailed in policy statements, procedures and regulations, including the NRC's Safety Culture Policy Statement (SCPS), the Reactor Oversight Process (ROP), and the Allegation and Enforcement Programs.The NRC's SCPS sets forth the Commission's expectation that individuals and organizations establish and maintain a positive safety culture commensurate with the safety and security significance of their activities and the nature and complexity of their organizations and functions. The SCPS is not a regulation. It applies to all licensees, certificate holders, permit holders, authorization holders, holders of quality assurance program approvals, vendors and suppliers of safety-related components, and applicants for a license, certificate, permit, authorization, or quality assurance program approval, subject to NRC authority.Regulatory oversight of safety and security is conducted through the Reactor Oversight Process (ROP) which is the NRC's program for assessing the performance of operating commercial nuclear power reactors. In 2004, the NRC took steps within the ROP to strengthen the agency's ability to detect potential safety culture weaknesses during inspections and performance assessments. In 2006, guidance and procedures for inspecting and assessing aspects of licensees' safety culture, which includes security, were included in the ROP. The ROP uses inputs from performance indicators and inspection findings to develop conclusions about a licensee's safety performance. Performance is evaluated systematically and on a continuous basis through planned inspections, and assessment meetings.In addition to the ROP, the NRC's Allegation Program and Enforcement Program can address safety culture, if necessary, through the use of chilling effect letters (CELs) and, in certain cases where there is a violation of NRC regulations with a nexus to safety culture, can issue confirmatory orders (COs). The NRC generally issues a CO as part of the enforcement Alternative Dispute Resolution (ADR) Program. These programs and actions are applicable to all NRC licensees, applicants and vendors, and can be used to address safety culture issues, if appropriate, based on safety and security concerns.

Synopsis ID: [95]

Nuclear Security Regulatory Authorization and Assessment Process for Barakah NPP in United Arab Emirates

Alsaadi, S.[1], Alshehhi, O. [1], Winter, D. [1], Ismail, S. [1], Alhammadi, F. [1], Almuhairi, F. [1]

[1] Federal Authority for Nuclear Regulation (FANR), United Arab Emirates

Corresponding Speaker: S. Alsaadi

In September 2009 the Federal Authority for Nuclear Regulation (FANR) was established to be the regulatory body for the nuclear sector in the UAE in accordance with Federal Law by Decree No 6 of 2009, Concerning the Peaceful Uses of Nuclear Energy, which was issued by the UAE President H.H. Sheikh Khalifa bin Zayed Al Nahyan. FANR protects the UAE's public, its workers and the environment by conducting nuclear regulatory programmes in safety, security, radiation protection and safeguards, which fulfill key objectives in licensing and inspection in accordance with best international practices. FANR also oversees the implementation of the UAE's obligations under the international treaties, conventions and agreements in the nuclear sector, and determines administrative standards, which support excellence in regulation. Adhering to international nuclear security standards so that our nation remains safe, this paper introduces the legislative framework for nuclear security in the United Arab Emirates (UAE), then describes FANR with respect to the developed regulations and regulatory guides to protect the use, storage and transport of nuclear materials and facilities. Specifically, it describes FANR Regulation (FANR-REG-08), which concerns the physical protection for Nuclear Material and Nuclear Facilities, and the developed regulatory guides concering nuclear security. Furthermore, the approach with respect to nuclear security for oversight of construction and the granting of an Operating Licence for the first nuclear power plant in the UAE to assure the achievement of the national policy goals for security. The paper presents the nuclear security authorization process set up by FANR for a construction and operational licence that is implemented under FANR's Integrated Management System (IMS) in accordance with the International Atomic Eeregy Agency (IAEA) recommendations. In order to ensure the protection against radiological sabotage and unauthorized removal of nuclear material, FANR developed a process for security review and assessment, as well as conducting inspections to ensure the physical protection of nuclear facilities and nuclear material in use, storage and transport, which is included in this paper. This includes the process of securiy review and assessment, as well as the security inspections and enforcement to ensure the physical protection of nuclear facilities and nuclear material in use, storage and transport in order to protect against radiological sabotage and unauthorized removal of nuclear material. Moreover, the paper outlines the content of the operating licence application submitted by the applicant and reviewed by FANR focusing on the security

regulatory review and assessment of the physical protection plan which provides an overview of the entire physical protection program for the construction phase and the operation phase of Barakah Nuclear Power Plant. Finally, the paper describes the basic elements required by FANR for the decision-making regarding the issuance of the Operating Licence including integration of the results of security review and assessment with that of safety and safegaurds in line with international best practices.

Synopsis ID: [224]

Assessment of the U.S. Nuclear Regulatory Commission Security Baseline Inspection Program

Bailey, M.[1]

[1] Nuclear Regulatory Commission, United States of America

Corresponding Speaker: M. Bailey

Following Commission direction, the U.S. Nuclear Regulatory Commission (NRC) staff is conducting an assessment of NRC's security baseline inspection program, including the Force-on-Force program, to identify improvements and efficiency gains. This paper describes the NRC staff's assessment and follow-up actions, and the potential policy recommendations to the Commission for improvements to the NRC security inspection program.

The Commission specifically instructed the staff to avoid attempting a fundamental redesign of the program. Thus, the staff focused on those activities most likely to yield improvements and efficiencies. For example, the staff completed a comprehensive review of the NRC's Security Inspection Manual Chapters and all Baseline Security Inspection Procedures for nuclear power reactors. The review identified multiple opportunities for efficiencies, such as improved inspection schedule coordination, consolidating redundant inspection items, and revising the periodicity of certain inspections. The staff is in the process of revising the security inspection procedures to incorporate the recommendations from this comprehensive review. The staff also initiated a complete review of the NRC's security Significance Determination Process to ensure that inspection findings are evaluated objectively and at the appropriate level of significance.

Regarding the Force-on-Force program, the staff initiated an effort to revise the Contingency Response Force-on-Force Inspection Procedure. The purpose of this effort is to focus Force-on- Force inspections on performance-based mission planning and evaluation inspection activities, and eliminate compliance-based activities that are redundant or should be addressed in other baseline security inspection procedures. Further, after a review of past Force-on-Force exercises, the staff determined that, for the majority of exercises, more than fifty percent of exercise time was spent in timeout periods. As such, the staff is developing an approach or proposal for reducing exercise artificialities and improving exercise planning.

Per Commission direction, the staff is also evaluating: the use of vulnerability assessments to evaluate the effectiveness of licensee protective strategies; crediting operator actions during a contingency event, or the use of additional equipment, such as FLEX equipment, that was installed to enhance safety but can also provide a security benefit; and crediting local, State, or Federal law enforcement response to establish coping time for security events.

In its assessment of the security inspection program, including Force-on-force, the staff is considering input from NRC inspectors, licensees, the nuclear industry and other stakeholders. In particular, the staff is evaluating industry proposals for streamlining the security baseline inspection program, improving the effectiveness and efficiency of the Force-on-Force exercise inspection schedule, conducting a defense-in-depth Force-on-Force exercise, and conducting a Security Event Mitigation Assessment.

Synopsis ID: [110]

IPPAS Mission in Germany

Kroeger, H.[1], Koschel, P. [2]

[1] German Federal Ministry for the Environment, Nature Conservation, Building and Nuclear Safety, Germany

[2] Ministry for the Environment, Energy and Climate Protection of Lower Saxony, Germany

Corresponding Speaker: H. Kroeger

The IAEA provides its International Physical Protection Advisory Service (IPPAS) since 1996. Since then, more than 75 missions to member states have been conducted. While Germany has been active in supporting these activities through experts in the field of nuclear security, a mission in Germany was not arranged until 2016. The main reason for this was the fact that Germany is phasing out of the commercial use of nuclear power until the end of 2022.

Since the German utilities are not owned by the state but rather by various companies, convincing them to participate in an IPPAS mission was difficult as the value of the service appeared limited with regard to the limited lifetime of the nuclear power plants (NPPs) until the beginning of their decommissioning. Additionally, the state the NPP is located in had to be convinced to participate in the mission as well. In early 2016, both the state of Lower Saxony as well as the NPP Emsland agreed to participate in an IPPAS mission in Germany. It was determined that the scope of the mission should encompass the modules on the national nuclear security regime, the module covering the physical protection at a nuclear facility and the module on computer security, and that along with the NPP Emsland the interim storage facility at the same site would also be participating in the mission.

A workshop accompanied the prep meeting in early 2017 for the mission taking place later in September and October 2017. The workshop was very helpful in convincing the utility that an IPPAS mission could still be a valuable undertaking for an NPP scheduled to begin decommissioning within the next five years. All agencies involved in nuclear security on the federal level as well as on the state level were working together to prepare for the mission, which in itself was a helpful process, as the fragmented system of regulators and authorities in a federal state can be quite complex and some of the people involved had never directly cooperated before. The self-assessment from the IPPAS Guide will be particularly helpful in future years when new employees will have to be trained in the field of nuclear security, as there still will be storage facilities and final depositories that require physical protection and regulations for computer security. Among the topics suggested to the IPPAS team for the mission were the integrated concept for nuclear security in Germany, the use of nuclear material and accountancy control versus physical protection and the use of mostly generic regulations.

The recommendations as well as the best practices recommended by the IPPAS team will be presented in this paper as far as possible, and the experiences gained through the preparations for the mission will be discussed.

Synopsis ID: [159]

Lessons Learned from the IPPAS Follow-Up Mission to Hungary

Stefanka, Z.[1], Szepes, Z.[1], Hódosi, V.[1], Viplak, A.[1], Vincze, A.[1]

[1] Atomic Energy Authority, Hungary

Corresponding Speaker: Z. Stefanka

At the request of the Government of Hungary (received from the Hungarian Atomic Energy Auhtortiy HAEA by IAEA on 20 June 2012), the IAEA agreed to conduct an IPPAS mission to Hungary in May – June 2013. The IPPAS mission to Hungary was conducted from 26 May to 7 June 2013. As a result of the mission the experts determined 9 recommendations, 57 suggestions and 12 good practices.

On 2 June 2015, the Director General of the HAEA sent a request letter to IAEA about Hungary is ready to welcome an IPPAS follow-up mission. At the end of June HAEA received the acceptance letter from IAEA and started to organize the mission. As agreed, the date of the mission is 25th June to 7th July 2017 and the primary subject of the follow-up mission is the assessment of the fulfilment of the recommendations and suggestions determined by the IPPAS mission report in 2013. Moreover, attention will be paid on the introduction the changes in the regulatory system since 2013, the developments in the field of cyber security and the security arrangements of the planned new units at Paks. Moreover, the scope of the follow-up mission will include the following IPPAS modules:

- Module 1: National review of nuclear security regime for nuclear material and nuclear facilities
- Module 2: Nuclear facility review
- Module 4: Security of radioactive material and associate facilities and associated activities
- Module 5: Information and computer security review

Based on the above listed modules, the international expert team of the IPPAS follow-up mission reviews the Hungarian nuclear security legislative and regulatory framework for nuclear and other radioactive material and associated facilities, regulatory practices (licensing, inspections and enforcement) and cyber security, enhancing the developments and changes since 2013. The scope of the mission also covers the review of the security arrangements concerning the planned new NPP units and the state system of nuclear material accountancy for and control will be revised from physical protection point of view. The presentation provides information on the preparation for the mission and the content of the mission report describing the results of assessment (i) of the fulfilment

of the recommendations and suggestions from the prevous mission and (ii) the Hungarian nuclear security regime and (iii) provides lessons learned from the conclusions drawn by the IPPAS expert team.

Synopsis ID: [9]

Safeguards and Security Limited Notice Performance Testing: A Systems Approach

Messer, T.[1], Vanveghten, R.[1], Dubose, F.[1], Gradle, C.[1], Lamb, F.[1], Rasmussen, G.[1]

[1] Department of Energy, United States of America

Corresponding Speaker: T. Messer

The U.S. Department of Energy (DOE) has conducted comprehensive multi-topic safeguards and security (S&S) assessments since the mid-1980s. These assessments cover a broad S&S program by assessing the various topical areas (i.e., Protection Program Management, Physical Security Systems, Protective Force, Personnel Security, Information Security, Material Control & Accountability, etc.). They are typically announced months in advance and require extensive, coordinated planning with the assessed organization. This includes onsite scope determinations, detailed scheduling, exchanging large amounts of data, and teams of approximately 24 subject matter experts (SMEs) who are onsite for up-to-three weeks collecting, analyzing data, and documenting the results.

These multi-topic assessments have proven successful over several decades. Specifically, the results culminate in an executive summary which provides an overall status of the S&S program, while the body of the report communicates, by topic-level, the specifics of the various S&S disciplines assessed at any given point in time. Additionally, organizations benefit from preparing for these types of assessments (e.g., updating internal processes, procedures, training programs and conducting detailed self-assessments). Measuring performance through this approach is resource intensive, often assessing a program at its best, and are only conducted at a 30-36 month periodicity. Therefore, following the well-publicized security incident at the DOE Y-12 National Security Complex in July 2012, the Secretary of Energy directed the DOE's Office of Enterprise Assessments (EA) to develop a no-notice performance testing program to provide a "real-time" evaluation of site S&S readiness. In response to that direction, the Office of Security Assessments (EA-22) within EA teamed with various DOE stakeholders and determined that a no-notice testing program could not be safely executed in an environment protected by security police officers/Federal Agents equipped with live firearms. However, the team determined that a limited-notice testing program was a viable option. This approach uses a "trusted agent" process to identify minimal personnel at the site who are required to safely plan and conduct performance testing at their facility. This has been as few as two people at some locations. Working with these trusted agents and leveraging the organization's existing performance-testing program; limited–notice tests are identified, planned, and executed using a very

small team of SMEs. This team can safely collect data under real time conditions, with minimal advanced notice to tested personnel, and minimal impact to mission operations.

The DOE's EA-22 has conducted numerous limited-notice tests at most of its high-hazard facilities since 2013, resulting in the identification of lessons learned and program improvements. One of the more significant lessons learned is the realization that security organizations have strong internal communications, especially when an outside organization is conducting an assessment. The team quickly realized the element of surprise associated with the limited-notice performance testing was lost after the first test. In response, the limited-notice testing program adopted an integrated testing approach, focusing on the dynamics of interaction between the system components, rather than the components themselves. This approach tests the overall function of a physical protection system with one stimuli. For example, the test may begin with a balanced magnetic switch door alarm, followed by a protective force response, leading to a safeguards assessment, and ending with a material inventory. This paper discusses the benefits of using this approach to exam the dynamics of the interactions between the processes, and assessing the performance of the system when there may be no inherent weaknesses in individual system elements. The purpose of the presentation is to communicate the lessons learned by the DOE to an organization that is considering adopting a similar testing approach, such as use of the systems-level testing approach; using trusted agents, safety risk assessment

Synopsis ID: [262]

Protecting Nuclear Materials and Facilities against the Full Spectrum of Plausible Threats

Bunn, M.[1], Roth, N. [1], Tobey, W.[1]

[1] Harvard Kennedy School, United States of America

Corresponding Speaker: M. Bunn

Reducing the risk of theft of nuclear materials or sabotage of nuclear facilities to an acceptable level requires protecting them against the full spectrum of capabilities and tactics that adversaries might plausibly use to accomplish their objectives. The amended Convention on the Physical Protection of Nuclear Materials and Facilities recognizes this, obligating states to provide protection against nuclear theft and sabotage that should be based "on the State's current evaluation of the threat. (Fundamental Principle G) Elaborating on this thought, INCIRC/225/Rev. 5 recommends that states establish a "design basis threat" (DBT) to be used for designing and evaluating systems to prevent nuclear theft and sabotage; that states base this DBT on a regularly updated assessment of the threat, using all available credible information; and that they design and maintain their physical protection systems to provide enough protection against the adversaries included in the DBT to maintain acceptable levels of risk. We would argue that UN Security Council Resolution 1540, which obligates all states to provide "appropriate effective" security and accounting for all nuclear weapons and related materials, requires that such security and accounting systems provide effective protection against all the various types of adversary theft attempts that might plausibly occur.

How can states judge what particular types of capabilities and tactics to include in their DBTs (or in their threat assessments, if that is what they use for activities such as protection of radiological material)? On the one hand, it is critical to be effectively protected against real threats, but on the other, no one wants to waste money or impose undue inconvenience in protecting against unrealistic dangers. The problem is complicated by the fact that adversaries learn, adapt, and change, making the past a less reliable guide to the future. For example, the number of attackers adversaries have used in past assaults may simply reflect the number they judged were needed to accomplish their objectives; they might use more in the future, if they judged more were needed, and if they judged that they could organize a larger attack without being detected in advance by intelligence and law enforcement agencies.

We propose two complementary approaches to address this problem. First, states should examine real incidents of theft from or attack on secured facilities, both nuclear and non-nuclear, to learn lessons about the types of capabilities and tactics adversaries have shown they can use. Intelligence information, information provided by other states or by international organizations, and open-source information can all be helpful in such an examination. States should consider developing a regularly

updated database of such incidents and lessons learned from them. First priority in such an examination should go to incidents within the state itself, but incidents in nearby countries and elsewhere in the world should not be ignored. Some promising work in recent years has helped countries develop DBTs using such approaches. The paper outlines several illustrative incidents that highlight capabilities and tactics against which nuclear materials and facilities should be protected.

Second, a strong case can be made that no state is so safe that it can afford not to protect against a common baseline level of threat. Anywhere in the world, a modest group of well-armed and well-trained outsiders, capable of operating as more than one team; a well-placed insider; and both the outsiders and the insider working together are plausible threats that nuclear materials and facilities should be protected against. Indeed, examination of insider thefts from secured non-nuclear facilities in recent years suggests that multiple insiders working together is also a plausible threat; states should give increased attention to the difficult problem of protecting against multiple insiders.

In short, all states using weapons-usable nuclear materials or operating nuclear facilities whose sabotage could cause unacceptable consequences should protect these materials and facilities against at least a baseline level of threat – and states whose assessment of recent incidents suggests that they face higher levels of adversary capability should protect against higher levels of threat. The paper elaborates somewhat on how interested states might commit themselves to such an approach and encourage others to do the same.

Having put such requirements in place, states should put in place effective mechanisms for assessment and realistic testing to ensure that their security systems really can defend against intelligent adversaries looking for ways to defeat them. In particular, if the state's regulatory system requires operators to provide protection against some threats and gives the state the responsibility to protect against other threats, both the state and the operator need to put in place, and regularly exercise, the capability to meet their respective responsibilities, and to work together in providing effective protection.

Synopsis ID: [40]

Identification and Assessment of Threats for a Nuclear Fuel Fabrication Facility (NFFF)

Elsayed, H.[1], Shaat, M. [1]

[1] Egyptian Atomic Energy Authority, Egypt

Corresponding Speaker: H. Elsayed

In uranium fuel fabrication facilities, large amounts of radioactive material are present in a dispersible form. This is particularly so in the early stages of the fuel fabrication process. In addition, the radioactive material encountered exists in diverse chemical and physical forms and is used in conjunction with flammable or chemically reactive substances as part of the process. Thus, in these facilities, the main hazards are potential criticality and releases of uranium hexafluoride (UF6) and U3O8, from which workers, public and the environment should be protected. Nuclear facilities are vulnerable to terrorist attacks or thefts of nuclear material, especially for fissile materials which can be used for nuclear weapons. The physical protection system (PPS) performed in the NFFF against the unauthorized removal of nuclear material and against sabotage of nuclear material and nuclear fuel fabrication plant. This paper provides modification and assessment for the design of the PPS, which can provide high assurance of protection against the design-basis threat (DBT) to the prevention of insider and external threats. Different scenarios of attack also will be performed in this paper to identify the gaps and weak points of PPS.

Synopsis ID: [127]

Development and Evaluation of the Design Basis Threat in Germany

Engelhardt, C.[1]

[1] Federal Ministry for the Environment, Nature Conservation, Building and Nuclear Safety, Germany

Corresponding Speaker: C. Engelhardt

In Germany, the protection against malevolent acts or other illegal interference by third parties is a licence prerequisite for nuclear facilities and nuclear transports. This is defined in the German National law, the Atomic Energy Act. Measures of the operator/shipper and the State have to be in place and are strongly intertwined to fulfil this licence condition. According to the IAEA implementing guide "Development, Use and Maintenance of the Design Basis Threat" (NSS N◦10), the basis of all necessary protective measures is a national threat assessment and a Design Basis Threat (DBT). In a Federal State, a lot of competent authorities of the federal state and the 16 states ("Länder") have to be engaged performing the threat assessment as well as developing and evaluating a DBT. Thus, a formal process of developing and evaluating a DBT is installed in Germany. The roles and responsibilities of the State, the competent authorities, the committees and the stakeholders that are involved in the process are well defined. There is stipulated a time period of three years at most for a periodic evaluation of the national threat assessment and the DBT. This time period can be shorter, if there is an indication that the postulated threat and/or the potential adversary scenarios for committing malicious acts as well as their unacceptable consequences are changed. Within the process of developing and evaluating a DBT all aspects of nuclear security have to be considered. Therefore, there are currently three separate DBTs for nuclear facilities, for computer security and for nuclear transports in operation in Germany. A blended-attack, i.e. a combined attack of a cyber-attack and a physical attack, is taken into account designing these DBTs. A DBT for other radioactive material is drafted. The DBTs comprise descriptions of potential adversary scenarios for committing malicious acts, characteristics of the postulated adversaries as well as specifications of weapons and tools. The motivation of the potential adversaries is not addressed in the DBTs, since there is no impact on the protective measures of the operator/shipper and the State. The postulated objectives of the potential adversaries performing malicious acts are to cause theft or sabotage of nuclear and other radioactive material. All German DBTs contain sensitive information and thus, are classified as confidential. The presentation will discuss the whole process of developing and evaluating the DBTs in the Federal State of Germany.

Synopsis ID: [84]

U.S. Department of Energy 2016 Design Basis Threat (DBT) Methodology

Callahan, S.[1], Hojnacke, M.[1], Benton, B.[1], Sparks, M.[1], May, M.[1],.McDowell, G.[1] , Pincock, M.[1], Rogers, J.[1], Uecker, N.1, Sandoval, J.[1]

[1] Department of Energy, United States of America

Corresponding Speaker: S. Callahan

Fundamental Principle G in the Amendment to the Convention on the Physical Protection of Nuclear Material [1] is that: "The State's physical protection should be based on the State's current evaluation of the threat." The U.S. Department of Energy (DOE) has used the concept of a design basis threat (DBT) for more than 25 years. The DBT in DOE serves a number of purposes. It defines the types of assets within DOE requiring protection and bins them in accordance with consequence of their loss; it defines the protection strategy the physical protection system must achieve for each asset; it implements a risk management framework; and it defines the types of threats and capabilities used as the basis for determining appropriate physical protection measures, and for use in planning, analyses, and performance testing.

The DBT in DOE is based on a threat assessment conducted to determine potential threats to nuclear facilities, but for a number of reasons, a threat assessment as provided must be interpreted and decisions made regarding what will form the basis for physical protection. As an example, a threat assessment may say a potential threat may have a high capability 'A' or a lower capability 'B', but there is uncertainty regarding the assessment. In development of the DBT, developers of the policy need to determine whether to very conservatively define the threat with both capabilities 'A' and 'B', use the highest capability only 'A', only use 'B', or, given the level of uncertainty, may even decide not to include 'A' or 'B'. This process is used in DOE, and all decisions, along with the rationale for each decision is documented as the basis for the final DBT. The DBT implements a graded protection for assets, based on consequence of loss, and assigns them a protection level. As an example, Category I nuclear material is one protection level, and Category II nuclear material is a lower protection level. The DOE DBT covers all its assets, including nuclear material, radiological sources and hazardous chemicals with the potential for unacceptable consequences from sabotage, hazardous biological materials, critical facilities, property, and even people. A unique concept used in DOE is termed roll-up, defined as the accumulation of smaller categories of nuclear material to acquire a higher category. Nuclear material is protected based on its discrete category, but if it is determined that other nuclear material can be acquired to result in a higher category, all the nuclear material must be protected at the higher category. Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) [2] recommends: "For protection against sabotage, the State should establish its threshold(s) of unacceptable radiological consequences," and the DOE

DBT defines thresholds for both on and off site dispersal of radiological (including nuclear) material and a threshold for use of the material to expose people to a direct radiation dose.

The DBT includes a range of threat types, and consideration is given not only to terrorist threats, but to threats from criminals and protestors. It defines threat capabilities, based on information from the threat assessment and other sources, for use in analysis and testing. Determination of the threat types and capabilities included a determination of the threats posed from insiders, as well as the potential for threats to acquire new and emerging capabilities, such as the ability to attack computer based systems used for safety, physical protection, and nuclear material accountancy and control. The number and type of capabilities potential threats may possess are many, but all of them cannot be used at one time. The DBT incorporates a scoring methodology to ensure adversary threat capabilities used are within specific bounds. Along with these defined threat types and capabilities, the DBT includes a defined set of baseline scenarios nuclear facilities must analyze.

And finally, the DBT implements a risk acceptance framework (identifying someone in the government ultimately responsible for acceptance of risk), to ensure DOE maintains an effective nuclear security regime.

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Amendment to the Convention on the Physical Protection of Nuclear Material, Vienna, (2005). [2] INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Nuclear Security Series No. 13, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), Vienna, (2011).

Synopsis ID: [41]

An Analysis on Effective Physical Protection System Development for Nuclear Materials and Nuclear Facilities in Bangladesh

Salahuddin, A.[1], Hossain, A.[1]

[1] Department of Nuclear Science & Engineering, Military Institute of Science and Technology (MIST), Bangladesh

Corresponding Speaker: A. Salahuddin

Nuclear material (NM) is widely used in legitimate applications like in industry, medicine, agriculture and scientific research. But its potential may be misused by the wrong perpetrators to achieve particular anti-state goal in the form of deterrence and violence. Hence, threat to NM and Nuclear Facilities (NF) is the main factor for the development of Physical Protection System (PPS). As of now, Bangladesh has only one NF available e.g. a 3 mega-watt research reactor that uses NM of 19.7% low enriched uranium for research purposes. Basing on the past and current threat scenario, although reasonably developed PPS are in place, but there are rooms for significant improvements as per IAEA guidelines. Besides, physical security of the upcoming nuclear power plant (NPP) covering the fresh nuclear fuel, spent nuclear fuel, nuclear waste and other industry-yields are of a time worthy concern for Bangladesh now. Moreover, Bangladesh being a signatory to International Convention on the Physical Protection of NM and Convention on Nuclear Safety, it is obligatory to have effective PPS for its NM and NF complying the associated instructions. Considering all these issues, development of an effective PPS for the NM and NF is a compelling necessity for Bangladesh now. This article presents a comprehensive analysis on the full spectrum of necessities to develop an effective PPS for NM and NF in Bangladesh specifically for the construction of the first NPP which will be in criticality by 2022.

As per IAEA guideline, there are recommended procedures and components of PPS essential for any NPP of the member states. Considering these as baseline requirements, this work proposes to have a comprehensive threat study to identify the pertinent threats for Bangladesh including possible threat vectors from the trans-border and trans-regional threat off-shoot from the southeast Asian countries to Bangladesh. Such a study would end up to a design basis threat (DBT) findings as per the current threat pattern. The DBT study would result to a threat matrix in which each threat would have a translated representation of threat grade (high, medium, low, etc.) based on its individual attractiveness as target. The threat grade and individual threat can then be quantified reasonably in terms of capability, intent and target values; and put under computational logics for threat encapsulation. This would basically be a threat modeling to enclosing all the threat dimensions and threat vectors under a controlled mechanism. The output of the threat model can be the input for

another computational logic sets to develop an intelligent tool for the most effective PPS regarding the facilities. This tool would act as an effective threat-security interface which can be inputted to the final stage developing another PPS validation program to determine its effectiveness. The PPS effectiveness can also be re-validated through using other physical means like conducting real time / table top exercises or others methods.

This analysis demonstrates that minimum three aspects should be taken into consideration for effective operation and maintenance of the PPS. Firstly, the NPP authority should have a designated organ as 'PPS operator' with required skill set and authority to ensure the physical security; and to establish nuclear security culture since the beginning of construction work. This should be a central body adequately empowered to manage independently the nuclear security profile of the NPP facilities covering the full range of operation and maintenance works including the response mechanism for threats beyond DBT. Secondly, there should be facility-specific covert intelligence organization of the NPP authority to audit the physical security performance as per the facility-specific regulatory frameworks. Lastly, as per IAEA regulation, state being fully responsible for the nuclear security, Bangladesh should engage her 'State Intelligence Organ' for counter-check functioning of the overall nuclear security regime covering the domestic and international scopes specially the trans-border activities.

This study also identifies that security merit widely varies at every stage of the nuclear fuel cycle (NFC). This is threat variance for which security role of the respective stakeholders of the associated facilities would also vary. Therefore, PPS would be very much facility-specific. Since Bangladesh presently falls neither in the front end nor in the back end of the NFC, therefore, the applicable PPS would be very much relevant to the plant facility only and during transportation of NM within the country.

In Bangladesh perspective, considering the prerequisites of PPS as the 'Demand' and the available capability as the 'Present Strength', a comprehensive gap analysis is also carried out in this study. The findings of the gap analysis reflect the country's current position and readiness in terms of PPS maturity. The findings also encompass the future works required for Bangladesh to run successful nuclear power programs ensuring standard nuclear security that would be compliant to relevant international regulations.

Synopsis ID: [168]

Developing and Sustaining a Physical Protection Regime for Nuclear Material during Transport, Use, Storage and for Nuclear Facilities

Touarsi, A.[1], Kharchaf, A. [1]

[1] University of Ibn Tofail, Morocco

Corresponding Speaker: A. Touarsi

While the development of different activities related to the use of Nuclear Material have been increased in the latest decade, Protecting Nuclear Material hosted within the state and Also during their International Transport, use, Storage and In Nuclear facilities has been not Just matter at the International level, but Also has been as neccessary concerns as a big challenges facing the international and national community. Therefore, keeping Nuclear Material more secured remains and requires the developement of Nuclear Security regime, which provides an equivalence between maintening a National Security regulatory and the creation of an intelligent national regulatory Framework, in order to enhance a High level of Nuclear Security measures for enhancing and ensuring a physical protection measures to detect ,deter,and delay any unauthorized removal of Nuclear Material. In addition, the International Atomic Energy Agency since was created in 1970 has made an effort during more than 60 years to keep Nuclear Material secured worldwide by the establishment, development and the creation of the conventions, fondamentals and recommandations related to the nuclear security aiming to Secure nuclear material and combat the illicit trafficking of nuclear material and ensuring a physical protection by the adaptation of the convention of protection of nuclear material management which the first publication was on 26 octobre 1979 and entered into force on 8 february 1987. The convention of protection of nuclear material manage aims specially to Maintening a physical protection regime for nuclear material during their lifes used in peaceful use. Facilate the cooperation between the states. Preventing and combatting any anhautorized removal for any nuclear material. It is Worth considering, That the state should develop a physical protection regime based on the graded approach, taking into account the categorization of nuclear material and Developing It national regulations under the review of the International Physical Protection Advisory Service (IPPAS),and the control of the International Atomic Energy Agency without forgot the improtant roles and efforts of the United Nations Security Council resolution 1540. Developing and sustaining a physical protection regime provides and requires an international and national efforts under the responsibility of the IAEA, as an international regulatory which plays a role of central Atomic Agency Autority by first ; strength the nuclear Security culture by establishing a new tools to teach the leaders on nuclear security the main elements to keep nuclear material more secured, help a

development countries to establish their national regulation if was inspired by the IAEA international security laws or define their own regulation. Furthermore, in This paper proposed we will highlight to examine what are the factors influencing the development and the sustaining a physical protection regime, and specially during the transport of nuclear material and during their use storage and for nuclear facilities as a vital area. Not just that we will also focused on studying the element system of physical protection and what are the role of the state to develop his regime, without forgotten the role of IPPAS and also the IAEA at the international level and the interface between nuclear Security and physical protection with defining what are the opportunities and the challenges facing the development of the physical protection regime

Synopsis ID: [294]

Nuclear Maritime Security Assurance Programme

Officer, R.[1]

[1] International Nuclear Services, United Kingdom

Corresponding Speaker: R. Officer

From an armed physical protection command and control perspective, how do multi model, specifically maritime, Category I Nuclear Material approved carriers provide evidence of having met compliance in accordance with international and national legislative frameworks as well as the expectation of regulatory bodies? In order to deliver safe and secure Category I nuclear material maritime transports International Nuclear Services (INS), in conjunction with its strategic partner the Civil Nuclear Constabulary (CNC), Her Majesty's Royal Navy, and with complete agreement and approval of the United Kingdom's Office for Nuclear Regulation (ONR), has developed a rigorous and robust quality assurance and operational capability check to ensure both internal and external expectations are met in terms of understanding, timeliness, completeness, and value. This INS bespoke Maritime Integration Training and Demonstration (MIT/MID) programme has been designed specifically to counter the threat posed from maritime and nuclear sector threat actors and vectors and has been successfully employed in advance of numerous live international and national security operations over the last 18 months to great effect, inclusive of the largest ever single global plutonium shipment.

In developing this assurance programme clearly defined outcomes and metrics generating both quantitative and qualitative deliver sufficient evidence over assertion which is consistent with relevant good practice and proportionate to the prevailing sector threat assessment, Design Basis Threat (DBT), and perceived maritime adversarial training, tactics and procedures (TTPs).

As the duty holder, risk owner and security intelligent customer, it behoves the corporate security directorate to provide a holistic training and exercise regime that adequately prepares the protection force and ships' command teams, acting in unison, to meet operational capability expectations, and thus provide the tools necessary in a pressurised but safe environment to deter, detect, and defeat those maritime threat actors one might reasonably expect to counter on passage.

To that end, a comprehensive programme of threat based scenarios and response drills have been developed to exercise the team alongside (fast cruise) where the protection force simulate being at sea, assessed by an internal assurance provision of suitably qualified and experienced persons (SQEP'D), prior to a regulatory demonstration at sea incorporating live firing with concomitant assessment through an external assurance expertise provider versed in the military maritime sector, namely, Her Majesty's Royal Navy gunnery and security experts of the Flag Officer Sea Training (FOST) organisation.

This paper will provide an overview of the planning, threat analysis, resource and force generation required to meet those outlined objectives, as well as aspects of the training and demonstration delivery, in order to better describe and elucidate on the 'INS way' and its nuclear maritime security assurance programme.

Synopsis ID: [118]

Regulatory Oversight and Control of the Physical Protection of Nuclear Materials and Nuclear Facilities and Compliance with the Requirements of the Convention on the Physical Protection of Nuclear Material and its Amendment

Pashayev, R.[1]

[1] State Agency on Nuclear and Radiological Activity Regulations (Regulatory Authority) of the Ministry of Emergency Situations, Azerbaijan

Corresponding Speaker: R. Pashayev

Background: December 9, 2003 the President of the Republic of Azerbaijan signed a Law number 547-IIQ on accession to the Convention on the Physical Protection of Nuclear Material. In April 24 of 2008 the President of the Republic of Azerbaijan signed a decree on creation of an independent regulatory authority, State Agency on Nuclear and Radiological Activity Regulations (SANRAR) under the Ministry of Emergency Situations, which gives the regulatory function in considerable extent to the sole body. With the establishment of regulatory body all the powers and duties related to the provision of supervision and control over nuclear and radiological activities, accounting and control of nuclear and radioactive materials, as well as the authority for authorization in this area were transferred to SANRAR. In the newly established Agency, one of the priorities of the activity was the review of international agreements and conventions and the preparation of proposals for their ratification. Thus, the necessary documentation and justification for joining to the Amendment to the Convention on the Physical Protection of Nuclear Material adopted on 8 July 2005 were prepared by SANRAR employees and submited for consideration. As result on March 18 of 2016 the Ammendment to the specified Convention was approved by the Law number 178-VQ of the President of the Republic of Azerbaijan.

Approach: According to its Statute, SANRAR performs the functions of the regulatory body, including authorization, inspection, emergency preparedness verification and emergency measures coordination, preparation of drafts of new legislative and regulatory acts, implementation of supervision and control systems, maintenance of the register of sources and nuclear materials and preparation of relevant reports, applies enforcement measures, etc. In this part of presentation describes the mechanisms of existing regulatory infrastructure and the level of their compliance to the Convention and its Amendment requirements.

Findings or Results: Independence in decision-making, established organizational structure and financing mechanisms allow the fulfillment of the main functions of the regulatory authority at

present. At the same time, there are challenges related to the legislative base and staffing of regulatory authority with the highly qualified staff in connection with the planning of expansion of activities in the field of nuclear technologies.

Conclusion: The decision on development of nuclear technologies for peaceful purposes and planning of the construction of research reactor in the future requires improving the structure and capabilities of the Regulatory Authority and also improving the legislative framework for the possibility of comprehensive execution of regulatory functions. In this part of presentation is also provided proposals to improvement of existing infrastructure in considerable to extent to the Convention and its Amendment requirements.

Synopsis ID: [15]

Regulatory Oversight of the Physical Protection of the Nigeria Research Reactor -1 (NiRR-1) and other Category 1 Radiological Facilities in Nigeria

Bello, N.[1], Ofoegbu, E. [1], Adamu, A.[1]

[1] Nigerian Nuclear Regulatory Authority, Nigeria

Corresponding Speaker: N. Bello

Nigeria in 1995 promulgated the Nuclear Safety and Radiation Protection Act (Act), which established the Nigerian Nuclear Regulatory Authority (NNRA) with the responsibility to ensure protection of life, health and the environment from the harmful effects of ionizing radiation, while allowing beneficial practices involving exposure to ionizing radiation. Regulatory oversight is one of the core functions of the NNRA as provided by the Act and physical security inspection is one of the inspections conducted by the NNRA. Physical security inspection is conducted on quarterly basis in all the high risk nuclear and radiological facilities in the country which include the Nigeria Research Reactor (NIRR-1) with Category 3 nuclear material, a Co-60 irradiator facility, three (3) Radiotherapy facilities with Co-60 sources and the Temporary Radioactive Waste Storage Facility. Nigeria signed and ratified the Convention on Physical Protection of Nuclear Material and Nuclear Facilities (CPPNM/NF) which came into force in May 2016. In order to domesticate the provisions of the CPPNM, the NNRA commenced the development of Regulations on Physical Protection of Nuclear Material and Nuclear Facilities in 2013. The Draft Regulations was developed using the recommendations in the IAEA Nuclear Security Series Number 13 (INFIR/CIRC/225/Rev 5). Furthermore, Nigeria signed a Nuclear Security Cooperation Agreement with the United States Department of Energy (USDOE) on physical security upgrade of some nuclear and radiological facilities in the country under the USDOE Global threat Reduction Initiative Programme currently known as Office of Radiological Security. In this regard, physical security upgrades have been carried out in five nuclear and radiological facilities in Nigeria with the assistance of the USDOE and the IAEA. Also plans are underway for fresh upgrade at these facilities including the National Institute for Radiation Protection and Research where we have the Secondary Standard Dosimetry Laboratory. The objective of this paper therefore is to discourse the lessons learnt from the eight years regulatory oversight of the physical security of the all high risk nuclear and radiological facilities in Nigeria and the future plan in regulating the proposed nuclear power programme in terms of physical security.

Synopsis ID: [135]

The Role of the Nuclear Regulatory Authority of Argentina in the Implementation of the Convention on the Physical Protection of Nuclear Material (CPPNM) and its Amendment

Roston, M.[1], Zunino, P.[1], Acosta, G. [1]

[1] Nuclear Regulatory Authority of Argentina, Argentina

Corresponding Speaker: M. Roston

The Argentine Republic signed the Convention on the Physical Protection of Nuclear Material (CPPNM) in 1986 and ratified its Amendment in 2011 (prior to its entry into force on May 8, 2016). As the CPPNM is the only legally binding international instrument in the area of physical protection, it is a key element of the international legal framework for nuclear security.

During the last few years, nuclear security has become a very important concern at the international level and Argentina has demonstrated a strong commitment with this matter. Argentina has always highlighted the importance of IAEA's role in order to strengthen global nuclear security and has supported the efforts made by the Agency in it.

The Nuclear Regulatory Authority (ARN) of Argentina was created by the Nuclear Activity National Act as an autonomous body reporting to the country's Presidency, and is independent of any organization dedicated to the use or the promotion of nuclear energy in any of its forms. ARN has the final objective of protecting the people and the environment from the potential harm of ionizing radiations. With this goal it has federal competence to regulate the nuclear activity on specific areas: radiological safety, nuclear safety, safeguards and physical protection. As a regulator, ARN dictates regulatory standards, issues the permissions and licenses authorizing practices and installations, controls the compliance with standards, requirements and license conditions, enforces this compliance and has a leading role in the preparation and response to radiological and nuclear emergencies.

In summary, regarding physical protection, ARN is the competent authority responsible for the implementation of the regulatory functions on the physical protection of nuclear material and facilities and radioactive sources, and therefore has a key role in complying with the CPPNM and its Amendment.

Specifically, ARN issued the "Standard of Physical Protection of Nuclear Materials and Facilities" establishing general criteria of physical protection of nuclear materials within nuclear facilities and during transport. It identifies levels of protection, the general features that a physical protection system should include and main aspects of its assessment. This standard, AR 10.13.1, had a first revision in 2002 and is under a broader process of general revision nowadays.

In this paper we will analyze the current status of the Argentine physical protection standards (in terms of normative, requirements and license conditions) and the challenges that the Amendment poses to our national legislation since new offences were incorporated to Article 7 of the Convention. It will also elaborate on the specific role of ARN in the implementation of CPPNM and its Amendment.

Synopsis ID: [85]

The U.S. Department of Energy's Use of Defense in Depth in Physical Protection

Sparks, M.[1], Curry, G.[1]; May, M.[1]; Sandoval, J. [1]

[1] U.S. Department of Energy, United States of America

Corresponding Speaker: M. Sparks

Fundamental Principle I in the amendment to the CPPNM defines defense in depth as ". . . a concept of several layers and methods of protection (structural or other technical, personnel and organizational) that have to be overcome or circumvented by an adversary in order to achieve his objectives." The U.S. Department of Energy (DOE) physical protection system requirements have been based on the defense in depth principle since the 1970s. It was initially based on requirements to enclose high consequence assets within a layered succession of physical barriers, all of which must be penetrated for the asset to be acquired as part of an attempt to steal or to sabotage the asset. The intent of implementing the defense in depth principle was to deter potential threats by making a facility's defenses seem formidable and, if a threat was not deterred and attempted a malicious act, to provide time for a response force to respond and prevent the act.

Requirements based on the concept of defense in depth in DOE are graded, and are based on the category of nuclear material or the consequences of sabotage. DOE defines a number of required security areas depending on the type of asset, including general access areas, property protection areas, limited areas (equivalent to limited access areas in NSS-13), specially designated security areas (e.g., CAS and SAS), protected areas (same as defined in NSS-13), and material access areas (equivalent to inner areas in NSS-13) and vaults (equivalent to strong rooms in NSS-13). Each area type has defined protection requirements, with significant PPS requirements for protected areas and material access areas. The layers are required to have defined access control points and clearly defined boundaries (signs, demarcated boundaries, fences).

In addition to defense in depth principles for PPS elements that provide the functions of detection and delay, DOE requires implementation of a concept termed tactical doctrine by response forces. The concept of the tactical doctrine is to design an area defense plan with fixed strong points, or fighting positions, that encompass a target and lie within a concentric arrangement of intrusion detection systems and barriers. Combined with mobile forces that can fire and maneuver in coordination with the fixed positions, the objective of the tactical doctrine is to detect, delay, and engage the adversary as far from the target as possible.

Defense in depth as implemented within DOE also includes nuclear material accountancy and control (NMAC) measures in addition to the traditional PPS measures. NMAC measures required by DOE include material containment and surveillance measures, which in conjunction with other PPS

elements such as personnel and vehicle searches, increase the effectiveness of detecting, assessing, and responding to insider threats. Material containment measures control the storage and movement of nuclear material, and material surveillance measures are intended to detect insider adversary activities, and includes the use of technical devices and personnel observation to detect unauthorized movements of nuclear material, tampering with containment of nuclear material, falsification of information related to location and quantities of nuclear material, and tampering with safeguards devices.

Synopsis ID: [152]

Application to Vital Area Identification of Nuclear Power Plants based on PSA

Kang, M.[1], Koh, M. [1]

[1] Korea Institute of Nuclear Nonproliferation and Control (KINAC), Republic of Korea

Corresponding Speaker: M. Kang

A vital area is defined in INFCIRC/225/Rev.5 as "an area inside a protected area containing equipment, systems or devices, or nuclear materials, the sabotage of which could directly or indirectly lead to unacceptable radiological consequences". Vital Area Identification (VAI) is the process for identifying areas containing nuclear materials, structures, systems or components to be protected from sabotage, which could directly or indirectly lead to unacceptable radiological consequences.

Procedures of Vital area identification(VAI) based on Probabilistic Safety Assessment(PSA) which is one of the base techniques for physical protection regulation is developed. Traditionally, the physical protection of safety-critical systems has been a boundary protection of systems. In addition to the boundary protection, the protection of vital areas such as building and areas inside the facility boundary has been introduced as an active physical protection. Under this situation, the vital area identification(VAI) methodology is the base technology for the physical protection regulation.

VAI is a procedure to determine a set of rooms to be protected in order to suppress or avoid Unacceptable Radiological Consequences(URC) such as core damage. The Target Sets are minimal sets of room destructions that can cause core damage and the Prevention Sets are minimal sets of room protections that suppress core damage. The Target Sets and Prevention Sets are calculated from the Sabotage model. The Sabotage model can be obtained by replacing basic events of component failures in a PSA fault tree with room failures.

The developed VAI procedure is more specifically as follows: (1) collecting the internal level 1 PSA model and information, (2) developing the fire/flood/pipe rupture model based on level 1 PSA model, (3) integrating the fire/flood/pipe rupture model into the sabotage model, and

(4) calculating Target Sets and Prevention Sets using VIPEX(Vital area Identification Package EXpert) software, which was developed by KAERI(Korea Atomic Energy Research Institute) for identifying the vital areas, (5) Select optimal prevention sets and designate them as vital areas. When two Target Sets {A, B} and {A, C, D, E} are calculated from the Sabotage model, four Prevention Sets {A}, {B, C}, {B, D}, {B, E} can be calculated from the two Target Sets. By choosing one of Prevention Sets and protecting rooms in the chosen Prevention Set, all Target Sets can be avoided. As an example, by choosing the second Prevention Set {B, C} and protecting two rooms B and C in the chosen Prevention Set, all Target Sets cannot contribute to the URC. The PSA method used in this paper, including

internal as well as external events, is known as the most complete and consistent method for identifying various accident sequences in nuclear power plants through which radioactivity might be released to the environment. Thus, it is logical and natural to use the PSA techniques and results for the VAI of nuclear power plants.

The Nuclear power plants should provide physical protection to the identified vital areas. For the efficient identification of vital areas, the methodology introduced in this paper is being developed based on PSA technology, particularly with respect to the top event prevention set analysis. And also, VIPEX software is considered to be very useful for the selection of target sets of a physical protection. The method in the present paper is consistent and the most complete for identifying vital areas, since it is based on well-proven PSA technology.

Synopsis ID: [87]

U.S. Department of Energy - A Qualitative Physical Protection System Risk Assessment Methodology

Hojnacke, M.[1], Callahan, S.[1], Sandoval, J.[1], Sparks, M.[1], Benton, B.[1], May, M.[1] , McDowell, G. [1] , Pincock, M.[1] , Rogers, J.[1], Uecker, N.[1]

[1] U.S. Department of Energy, United States of America

Corresponding Speaker: M. Hojnacke

Nuclear Security Series 13 (NSS-13) emphasizes applying risk management principles and the use of a graded approach in maintaining a State's nuclear security regime. In addition, it recommends that States: ". . . ensure that evaluations based on performance testing are conducted by operators at nuclear facilities and, as appropriate, by shippers and/or carriers for transport." In the U.S., methods and tools to conduct evaluations to determine the effectiveness of a physical protection system (PPS) and understand the risks to a facility from a defined threat, based on the potential consequences of theft of nuclear material or sabotage of a nuclear facility or nuclear materials have been developed and used for more than 40 years. The majority of the methods and tools are complex and quantitative, rely on the availability of extensive facility and PPS performance data, and require dedicated analysts to build and analyze complex models in path analysis tools and computer simulations. In the absence of validated performance data and skilled analysts, uncertainty regarding the fidelity of the data used in the analysis yields results that provide little value. For many smaller facilities, the effort and cost to perform a complex analysis is not feasible.

In the U.S., Department of Energy (DOE) DOE policy requires the use of complex, quantitative risk assessment methodologies for its very highest consequence sites (Category I, Category II, and sites with the potential to exceed thresholds of unacceptable radiological consequences), but allows the use of less rigorous, qualitative methods for all other nuclear facilities. In order to standardize the methods used by these sites, a qualitative method designed to be used in conjunction with a tabletop analysis was developed. Although it requires subject matter experts from the facility to aid in providing qualitative estimates about how elements of the PPS will perform against a given threat, it does not require personnel with expertise in the use of computer-based physical protection system models or simulations.

The model begins with a process to apply a graded approach to assets, based on the consequence of loss or sabotage. The assets are divided into high, moderate, and low consequence bins. The next step is to define the threat that will be used for the analysis. The threat or threats typically are defined by the State. The facility is then characterized, with an emphasis on defining PPS components at the facility that provide the functions of detection, delay, and response, and divided into logical layers

(e.g., limited access area, protected area, inner area). Scenarios are developed based on the defined threat capabilities and the assets. A tabletop exercise is then conducted where participants "walk through" the scenario, and use the results of performance tests and expert judgement with look up tables to aid in estimating how the PPS components perform the functions of detection, delay, and response at each layer. Qualitative effectiveness values of low, medium, or high are determined, and entered into a spreadsheet for each layer. Once the scenario has been completed, the effectiveness estimates are used first to get a layer rating, then an overall system effectiveness rating. An overall, qualitative risk rating is then assigned based on the consequence of loss and the effectiveness of the PPS.

The method applies the concepts of risk management and a graded approach in a manner that can be applied at nuclear facilities without the ability to conduct a complex, qualitative analysis, while still providing reasonable and consistent estimates of the effectiveness of a PPS and risk based on consequence of loss.

Synopsis ID: [66]

Meeting Outcomes Based Regulation through Performance Assessment

Rodger, R.[1], Edwards, J. [1], Baker, M.[1],Thompson, K.[1]

[1] National Nuclear Laboratory, United Kingdom

Corresponding Speaker: R. Rodger

The nuclear security regulator in the United Kingdom, the Office for Nuclear Regulation, has introduced a new policy document, 'Security Assessment Principles for the Civil Nuclear Industry' to apply to the assessment of security arrangements defined in a facilities security plan. The principles provide a framework for consistent regulatory judgements on the adequacy of security arrangements. As a Duty Holder the National Nuclear Laboratory (NNL) must have an approved site security plan; in fact we have three facilities with their individually approved plans. To get those approvals we must provide a 'claims, argument and evidence' approach to substantiate why our proposed and existing arrangements are adequate to protect the nuclear material under our care from the postulated threats detailed in the nuclear industries malicious capabilities planning assumptions (NIMCA), the UK's design basis threat (DBT). This paper will discuss how NNL went about reviewing the security assessment principles (SyAPs), identifying the impact that they have on our existing site security plan(s) and proceeding to build the 'claims, argument and evidence' case to justify the arrangements. We will look at how we have used performance assessment approaches to create the evidence to substantiate our claims and maintain approval of our site security plan(s). Without disclosing restricted information, we will be using a real-life facility as the case study to demonstrate theoretical and academic approaches being used efficiently and effectively. It will show how a useful insight is gained into the likely performance of the arrangements when challenged by malicious actions. This information will be of value to all facility operators irrespective of the regulatory regime they operate within.

Synopsis ID: [98]

Nuclear Energy Institute Proposed Approach for Crediting LLEA Response to a Security Event

Young, D.[1], Perkins-Grew, S. [1]

[1] U.S. Nuclear Energy Institute, United States of America

Corresponding Speaker: S. Perkins-Grew

Purpose

The Nuclear Energy Institute (NEI) is developing an approach for allowing U.S. power reactor licensees to consider response assistance available from a Local Law Enforcement Agency (LLEA) when assessing the ability to implement a mitigation action during a security event in order to prevent radiological sabotage. The approach provides specific criteria that, when met, allows a licensee to assume the availability of LLEA tactical response resources within a specified time limit. This time limit is referred to Security Bounding Time (SBT), and was formerly known as Security Coping Time. The SBT criteria consist of planning requirements, expected response capabilities, and periodic familiarization and practice opportunities that collectively provide reasonable assurance that LLEA tactical resources can establish the site conditions necessary to permit performance of a mitigation action following an attack. This will allow a licensee to use the expected performance of an action to inform vulnerability assessments, and the evaluation of tactical response drills and force-on-force (FOF) exercises.

Background

In accordance with U.S. regulation, 10 CFR 73.55, Requirements for physical protection of licensed activities in nuclear power reactors against radiological sabotage, a licensee must establish and maintain a physical protection program, to include a security organization, which will have as its objective to provide high assurance that activities involving special nuclear material are not inimical to the common defense and security and do not constitute an unreasonable risk to the public health and safety. To satisfy this performance objective, the physical protection program must protect against the design basis threat of radiological sabotage as stated in 10 CFR 73.1, and be designed to prevent significant core damage and spent fuel sabotage. In meeting these and related requirements, each licensee has established a site protective strategy and a performance evaluation program that periodically evaluates the effectiveness of the strategy. Licensees also interact with LLEAs to make arrangements for prompt threat response assistance.

With respect to a physical attack on a nuclear power plant, the objective of an adversary force is to produce significant core damage or spent fuel sabotage by preventing a combination of equipment and/or operator actions from performing their intended safety functions (i.e., a target set is compromised, destroyed, or rendered nonfunctional). Following the loss of equipment and/or operator actions, some amount of time would elapse during which the fuel would heat-up to the point where there is non-incipient, non-localized fuel melting and/or core destruction, or a loss of spent fuel pool water inventory and exposure of spent fuel. If plant operators can take certain actions during this period, then the progression to fuel damage may be arrested and reversed. Depending upon several factors, it may be necessary for a LLEA tactical team to establish the site conditions necessary to permit performance of an operator action to mitigate the event.

In Staff Requirements – SECY-16-0073 – Options and Recommendations for the Force-on-Force Inspection Program in Response to SRM-SECY-14-0088, the U.S. Nuclear Regulatory Commission (USNRC) Commissioners directed the staff to assess the security baseline inspection program to identify potential improvements and efficiencies. The assessment was to include a determination whether crediting of operator actions, the use of portable accident mitigation equipment, or response by local, State, and Federal law enforcement would make FOF exercises more realistic. The SBT criteria developed by NEI are intended to address the crediting of responses by local, State, and Federal law enforcement.

Synopsis ID: [306]

Physical Protection is the Keystone of Security

Maltsev, V.[1], Sarbukova, T.[1]

[1] Rosatom, Russian Federation

Corresponding Speaker: V. Maltsev

The Russian Federation has ratified and adhered to the Convention on the Physical Protection of Nuclear Material (CPPNM) and the Amendment to the Convention.

The Russian Federation has established and maintains an appropriate physical protection regime. The Russian physical protection regime is based on the fundamental principles in accordance with the Amendment to the CPPNM.

The Russian Federation:

established a legislative and regulatory framework to govern physical protection, entered into force necessary legislative acts, developed requirements for the physical protection systems of nuclear facilities;

designated the State Atomic Energy Corporation Rosatom as a competent authority on the physical protection and it was provided with appropriate functionality and authority; designated the Federal Service for Ecological, Technological and Nuclear Supervision as an independent regulatory body and it was provided with appropriate authority;

created a licensing system and defined responsibilities of license holders; ensures maintenance of a high level of nuclear security culture;

defined procedure of threat assessment against each nuclear facility; developed graded approach for physical protection requirements; introduced Defense in depth concept at all nuclear facilities;

established and implements quality assurance program; developed and exercises on practice contingency plans;

established requirements for protecting confidentiality of information.

The primary goal is to maintain an effective physical protection regime in the circumstances when new threats appear. The Russian Federation supports the current activities of the IAEA in the field of physical protection.

Key words: physical protection, physical protection regime, CPPNM, Amendment to the CPPNM, fundamental principles

Synopsis ID: [288]

The Role of Nuclear Forensics in Implementing International Nuclear Security Conventions such as the Convention on the Physical Protection of Nuclear Material and its 2005 Amendment (CPPNM/A) United States of America

Schnaars, D.[1], Wellington, T.[1]

[1] U.S. Department of State, United States of America

Corresponding Speaker: T. Wellington

Focus: This paper will discuss the role of nuclear forensics can play in the implementation of international conventions such as the Convention on the Physical Protection of Nuclear Material and its 2005 Amendment (CPPNM/A).

Background: Nuclear forensic science is a growing discipline that supports nuclear material security, associated international conventions and national efforts to implement obligations in the conventions. According to Article 5 of the Convention on the Physical Protection of Nuclear Material and its 2005 Amendment (CPPNM/A), signatories are required to return radioactive and nuclear (R/N) material outside regulatory control (MORC) to its owner. Similarly, Article 18 of the International Convention for the Suppression of Acts of Nuclear Terrorism (ICSANT) requires signatories to return illegally used RN material or devices to their owners. Nuclear forensics examination of R/N materials found outside of regulatory control can identify signatures, such as physical measurements and enrichment levels, which help assess material provenance. National Nuclear Forensics Libraries (NNFLs), or similar assemblies of R/N material information and associated expertise, are also valuable tools for comparing nuclear forensics data from R/N material found out of regulatory control against the country's national holdings. Finally, for R/N material that is found by one country but belongs to another, queries between NNFLs also help to identify ownership. This paper discusses the role of nuclear forensic characterization, NNFLs and queries between NNFLs in implementing the Amended CPPNM, as well as associated best practices. In addition, the paper will highlight how these nuclear forensic techniques, tools and practices help address threats posed by MORC and strengthen nuclear material security.

Synopsis ID: [68]

Integration of Security into a Concept Design for a Facility

Rodger, R.[1], Edwards, J.[1], Baker, M.[1], Owens, K.[1]

[1] *National Nuclear Laboratory, United Kingdom*

Corresponding Speaker: R. Rodger

Integrating security into a facility design early in a project results in improved understanding between the security and safety specialists, allows the interactions and boundaries to be more clearly understood so that a 'right first time' outcome is achieved, reduces the potential for conflict between needs, influence operations and result in project and facility cost-savings. This paper will address some of the major considerations to be addressed and the steps to be taken that allows security to contribute to the efficient progress of the design process. It will use a 'real world' facility as the basis of a case study that illustrates a successful process, identifying what needs to be addressed, the output documents that aid the efficient running of the project and influence the design, and where safety and security specialists can work together to ensure that the design is efficient, safe and secure. Challenges in the timing of information requirements, the scheduling of key activities will be highlighted, along with successes of project/discipline integration leading towards the delivery of a coherent safety and security design, with operational input. The process is inevitably iterative, and relies on different communities/disciplines interacting in an open and transparent manner, whilst balancing legitimate security considerations. Elements of cultural awareness relating to nuclear security, and the security of information, and how these were used to enhance an integrated team based approach, rather than security appearing to be an after-thought will be described. This will hopefully go some way to dispelling the perception that security is something that is done to a project and leads to additional complications, costs and effort, and highlights the genuine benefits of safety-security integration. The case study will show how the guidance found in the Nuclear Security Series (NSS) documents are translated into underpinning approaches that help an operator to meet their regulatory requirements.

Synopsis ID: [289]

AIEA: Enhancing Security Conference Protecting Nuclear Sensitives Sites

Lautier, J.[1]

[1] Electricité de France (EDF), France

Corresponding Speaker: J. Lautier

Protecting French nuclear sites relies on sharing of responsibilities between the French state and operators. The state defines the threats and the objectives in terms of protection, provides for intelligence gathering and intervention, as a supplement to the obligations incumbent on the operator. The operator has a requirement to deliver results based on a reference case of threats supplied by the state as well as with reference to regulatory requirements. Electricité de France (EDF) must therefore protect its 58 reactor units within its nuclear fleet based on French soil. So as to fulfill its responsibilities, EDF has chosen an original model, relying on both material resources for physical protection and human resources. Some personnel are from the private civil sector classified as EDF staff (site security personnel), while others fall within a convention agreement with the interior ministry, these state forces being financed by EDF. These response units, called 'PSPG' are missioned to respond on behalf of the operator to the highest levels of threat. As these are state forces, these response units also constitute the first-tier response coordinated by the French state. The Gendarmerie is also present as a territorial police force and provides the special forces from regional and national level. The advantage and the suitability of this model, with allows flexible coordination between the operator's resources and those of the state, was underlined by the members of the IPPAS mission that was held in France at the end of 2011. The reference case of threats is regularly updated by the French state and leads EDF to periodically review its security arrangements for nuclear facilities. Our conference will present the progress achieved during the last three years.

This conference will also focus on few examples about cooperation between EDF and Gendarmerie to design protection for first-tier response and design barriers protection such as fences and special doors.

The design analyses need firstly to know threats to take into account given by the French state. In a second time, the design analyses need testing protection and the cost of this protection in order to choose the right protection regarding the amount of global investment to reach the goal assigned.

At the end, you have to choose the implementation on site of the chosen protection such as wall, fences and special doors. This last step needs to share tactical experience and need to deal with the existing facilities. This step needs to share analyses between EDF (who know the facilities) and Gendarmerie (who know for example the way of using of weapons and the effect of these weapons).

Synopsis ID: [296]

Supply Chain Security – Where's your weakest link?

Whittard, B.[1]

[1] International Nuclear Services Ltd, United Kingdom

Corresponding Speaker: B. Whittard

International Nuclear Services (INS) is wholly owned subsidiary of the UK's Nuclear Decommissioning Authority (NDA) and is responsible for managing and executing a large portfolio of domestic and international contracts for nuclear fuel recycling and transport services, and is the world's leading maritime transporter of specialist nuclear materials. Last year, INS completed an unprecedented number of Category I transports of nuclear materials on board its purpose built nuclear transport vessels, and in doing so, INS continues to support the UK and other States in their efforts to discharge commitments made at the various Nuclear Security Summits enacted under the Obama Administration.

A key enabler to these important and sensitive recycling and transport programmes are the many and varied suppliers that INS work with. These suppliers support INS in a number of ways, and without them we would simply be unable to provide the high levels of service we offer today. By their very nature, many of these suppliers are engaged in services which involve the exchange and/or processing of what is known in the UK as 'Sensitive Nuclear Information' (SNI) and work that is often very politically sensitive. In doing so, it is incumbent upon us to ensure they are protecting our SNI appropriately, in whatever form it is.

Across a range of industrial sectors we are beginning to see a trend in the number of security incidents, issues and risks that occur within the supply chain. Taking this trend and sharing amongst the nuclear community will hopefully go some way to ensuring that the nuclear sector is well prepared and is actively taking steps to reduce the risk around its supply chain. This paper will seek to highlight the importance of having a robust supply chain security programme in place by describing the potential consequences if were to go wrong, it will discuss the benefits of a strong and sustainable supply chain security programme and describe some of the things INS has done to ensure its supply chain is as world leading as the services it offers.

Synopsis ID: [12]

Physical Protection Systems Education at Pakistan Institute of Engineering and Applied Sciences (PIEAS): Current Status, Lessons Learnt, and Future Prospects

Majeed, T.[1], Ulhaq, I.[1]

[1] PIEAS (Pakistan Institute of Engineering and Applied Science), Pakistan

Corresponding Speaker: T. Majeed

Physical Protection Systems (PPS) education was initiated as part of nuclear security education at PIEAS in October 2009. In this regard, a one semester course of 3 credit hours was introduced in October 2009 in the 4th semester of MS Nuclear Engineering program at PIEAS. Since then, this course is offered on regular basis every year. The main contents of this semester long course were designed in accordance with guidelines provided by IAEA Nuclear Security Series No. 12 (Educational Program in Nuclear Security). All essential topics related to PPS, such as design requirements, vital area identification, threat analysis for preparation of DBT, intrusion detection sensors, alarm communication and display, entry control, contraband detection, response systems, evaluation of the designed system are covered in detail. A hypothetical facility data, commonly used in IAEA's training courses on physical protection systems for nuclear facilities and nuclear materials, has been used to conduct exercises for in depth understanding of PPS concepts. Different topics, related to physical protection systems, are assigned as term projects to student with report writing and presentation in class as mandatory requirements of the course. About 20% of the total course grade is reserved for this term project assignment and other homework assignments related to hypothetical nuclear facility. Two one-hour sessional tests and one comprehensive terminal examination are used for course evaluation purposes. During the course, the students are taken to visit the physical protection systems interior laboratories, established at National Institute of Safety and Security (NISAS) by Pakistan Nuclear Regulatory Authority (PNRA), to observe the real sensors working for intrusion detection along with other systems of facility access control and contraband detection. The students also visit Pakistan Center of Excellence in Nuclear Security (PCENS), where they are briefed about different types of response systems. Sometime, a live demonstration of the response has also been conducted to show them a real life response carried out by security personnel in case of an attack on a nuclear facility or hijacked specialized nuclear materials or radioactive materials during transport. A role playing exercise has also been used inside the class to clarify different PPS concepts, such as determination of critical detection point, early detection, late detection, arrangement of detection systems for defense-in-depth methodology, adversary beating the detection systems, response in time, delayed response, introduction of delay systems and their effect on adversary progress, etc. The use of this role playing exercise has been found very effective in getting the in-depth understanding

of these crucial PPS concepts by the students. A total of 78 students have passed this course successfully.The main lesson learned is the overall enhancement of nuclear culture among scientists and engineers working at nuclear facilities and other associated facilities with in-depth understanding of PPS at the respective facilities and facilitation to those responsible for implementation of PPS.The graduates who are working as operators have helped in reinforcing the nuclear safety and security interface. Those who joined as regulators have facilitated in updating the nuclear security regulations by upgrading the physical protection requirements for nuclear material and facilities. The visit of the exterior physical protection laboratories, recently completed by PNRA at PCENS in collaboration with IAEA, will become part of the routine visit by students to PCENS. This will facilitate students in clarifying PPS concepts about exterior intrusion detection sensors and operation of central control room. PIEAS has recently established physical protection interior laboratory with the assistance of IAEA for PPS education. Development of computer code is also in progress at PIEAS for modeling and simulation designing, implantation and evaluation of an effective PPS on any facility. The PPS education experience of PIEAS, in collaboration of IAEA, can play a vital in the promotion of PPS education at regional level as well as at global level. In this paper the details of PPS education at PIEAS will be discussed. It will also present the experiences and lessons learned related to enhancement of nuclear security culture by implementing PPS education. Furthermore, the mechanism how PIEAS is interacting with other NSSC institutes in the area of PPS education will also be discussed. Also the details of the physical protection interior labs will be summarized.

Synopsis ID: [51]

Master of Science Program in Nuclear Security (MiNS) – A Project Overview and Future Challenges

Holl, F.[1]

[1] Institute For Security And Safety (ISS) At The Brandenburg University Of Applied Sciences, Germany

Corresponding Speaker: F. Holl

Regulatory changes, as well as persistent threats are major drivers in the field of nuclear security. To respond to these challenges, nuclear security expertise is needed. For example, States Parties to the Convention on the Physical Protection of Nuclear Material (CPPNM) will need to implement new legislative measures as the amendment to the convention came into force on May 8, 2016. Moreover, the fourth Nuclear Security Summit in early 2016 underlined the urgent need felt by the international community to enhance international cooperation to prevent terror attacks with nuclear material. In order to educate future experts needed to respond to these challenges, the International Atomic Energy Agency (IAEA) has called for universities to implement Master's programs in Nuclear Security.

In this context, the Institute for Security and Safety (ISS) at the Brandenburg University of Applied Sciences o[U+FB00]ers a unique distance learning program in Nuclear Security as of autumn 2017. After successful completion of the program, students receive an internationally recognized Master of Science (M.Sc.) degree in Nuclear Security from the Technische Hochschule Brandenburg – University of Applied Sciences. MiNS builds upon the lessons learned from the previous EU pilot program "Master in Nuclear Security".

The Master's program curriculum is based on the IAEA Nuclear Security Series No. 12 (NSS 12): "Educational Programme in Nuclear Security" and the teaching materials of the International Nuclear Security Education Network (INSEN). Therefore, it is one crucial step ahead of the current state of the art in teaching nuclear security. The language of instruction is English. The Master's program spans over three terms, which usually takes 18 months and covers various courses, such as nuclear security management, physical protection or cyber security.

The ISS, in close cooperation with international partners, organizes and implements the Master's program. The partners are experts from the following institutions: Technische Universität Wien

– Atominstitut, Austria; King's College London, U.K; Purdue University, U.S.; Texas A&M University, U.S.; and University of Ontario Institute of Technology, Canada.

All project partners are INSEN members. The Master's program provides theoretical and practical knowledge. Interactive web-based teaching sessions are led by highly experienced international experts. The distance learning courses will be provided as e-learning, academic letters or "paper-based" with interactive web-based teaching sessions. In order to gain practical experience we offer additional classroom based learning opportunities and hands-on laboratory work together with our partners. To enhance the positive learning outcomes of each student, web-based instruments such as social media, electronic learning systems for distance learning and videoconferencing are used.

The Master's program aims at providing participants with the ability of finding synergy in thinking between security risks, security methodology and corporate governance. While providing extensive knowledge, skills and practical experience, the Master's program also enables students to work at a strategic level within the field of nuclear security management.

This applies, for instance, to employees of nuclear installations, power plants and industry, nuclear security officers in national authorities and federal ministries, research/academic institutions, police and intelligence services, as well as regulatory authorities. In a nutshell, MiNS is a cost- effective way of educating and rewarding nuclear security managers and strategic talent in various functions.

The presentation will give a detailed overview of the major project implementation steps, as well as current perspectives and issues. Furthermore, it will provide an analysis of relevant challenges and priorities in the given context in the future. As a case study, IAEA NSS 12 will be introduced as the main curriculum structure for MiNS.

Synopsis ID: [133]

A Proposal for the Role of Nuclear Security Support Center to Sustain a National Nuclear Security Regime

Hazzaa, M[1], Shaban, S.[1],El-Tayebany, R.[1]

[1] Egyptian Nuclear and Radiological Regulatory Authority (ENRRA), Egypt

Corresponding Speaker: M. Hazzaa

An effective nuclear security system requires the provision of capability to prevent ,detect and respond to a criminal or unauthorized act with nuclear security implication, involving nuclear or other materials to strengthen nuclear security culture within competent authorities and relevant stakeholders in nuclear security. This is reached through establishment of sustainable and human resources development through establishing sustainable technical and scientific support service at the nuclear security support center (NSSC).This center can combine high level technical and scientific expertise to assess alarms, alerts and evaluation of any nuclear or radioactive materials founded and building capacity in human resources development (HRD), which train the newcomer persons with special training courses for physicist and engineers inspectors. Also these courses contain theoretical and practical train within limited time (how many hours per course) and test in the end of courses in order to qualify and prepare them in various types of inspections (for example inspector and reviewer for physical protection system). The NSSC consists of administrative department, training department, where containing Physical Protection Laboratory (Access Control Systems Lab, Intrusion Detection Systems Lab, CCTV lab, Facility Mock-up for PPS Demonstration) aims to train on various physical protection devices, provide technical support to the operators of nuclear facilities in the field of physical protection, technical and scientific support service department, also Mobile Expert Support Team (MEST) Laboratory for the detection and the response to nuclear security events in a country, a MEST include a person equipped and trained to use basic radiation monitoring instruments and perform simple assessment tasks. The MEST also include a forensic evidence management team (FEMT) which collecting, packaging and transporting evidence to the laboratory (including both the procedures as well as the equipment).The primary role of the training center is to provide education and training programs for enhancing awareness of nuclear security and non-proliferation based on the Systematic Approach to Training (SAT). This program divided to two categories depend on the job of employees at organization and qualifications. (a) Basic training program, required for all employees. (b) Advanced training program, focuses on specialized or technical skills training. Also the role of center can participate in preventing nuclear security events which combine high level technical and scientific expertise to repair and maintenance devices to assist for border, port staff and provide assistance to other stakeholders in developing design specifications

and procurement of equipment related to nuclear security. As well as Education program provide guidance for universities and other academic institutions (signed MoU) for a Master of Science programme, a certificate programme and e-learning modules in nuclear security. It can also be used for R&D (Research and development) purposes. Finally, this paper will recommends steps to further improve the Role of Nuclear Security Support Center to Sustain a National Nuclear Security Regime.

Synopsis ID: [194]

Implementation of IAEA INFCIRC/901: Promoting Certification, Quality Management and Sustainability for Nuclear Security Training

Johnson, D.[1]

[1] World Institute for Nuclear Security (WINS)

Corresponding Speaker: D. Johnson

The international community has spent considerable time, money, and effort attempting to establish a series of national and regional Centres of Excellence (COEs) for nuclear security, most of which have joined the IAEA's Nuclear Security Support Centre (NSSC) Network. Now with the end of the Nuclear Security Summit process, sustainability is a key consideration for many NSSCs. However, these Centres tend to have a wide variety of objectives, structures, and methods of delivery; no internationally accepted standard exists on how they should operate. The IAEA has produced some excellent guidance (TECDOC 1734), but by virtue of its role has stated that it cannot provide standards for benchmarking success.

Against this backdrop, a number of States, Foundations, and Industry supported the development of the World Institute for Nuclear Security (WINS) Academy, an initiative to provide practitioners with opportunities to earn certification in Nuclear Security Management. Underpinning the program is certification in accordance with the ISO 9001 and ISO 29990 quality management standards. These standards provide an internationally recognized external benchmark of quality; demonstrate credibility, competence and professionalism; and give potential employers and others in the industry an objective measurement of participants' knowledge. WINS recommends that NSSCs follow a similar model, in which their participants receive an evaluation leading to qualification or certification, and using professional standards developed by a recognized, respected certifying body rather than developing their own ad hoc arrangements, which may ultimately be unsustainable.

WINS has sought political and industry commitments to expand the Academy initiative, and these efforts were recognized at the 2016 NSS in a Joint Statement on Certified Training for Nuclear Security Management. This Joint Statement, signed by 12 States, was subsequently published as IAEA Information Circular 901 (INFCRIC/901), and commits signatory States to support the development of international certification through advocacy, peer review support, contributions or other means necessary. Signatory States have also committed to promote cooperative efforts between WINS and the IAEA NSSC Network and the International Nuclear Security Education Network (INSEN). Other States, supported by industry and civil society, are being encouraged to join the INFCIRC and provide a tangible commitment in support of the WINS Academy and certified professional development for nuclear security.

Synopsis ID: [31]

Education, Knowledge, Competence – Fundamental Prerequisites for Successful Implementation of Nuclear-and-Radiation- Related Physical Protection

Jovanovic, S.[1]

[1] University of Montenegro, Centre for Nuclear Competence and Knowledge Management (UCNC), Montenegro

Corresponding Speaker: S. Jovanovic

Successful implementation of international norms on the security of nuclear and radioactive material and facilities requires a number of prerequisites at the State – including the provision of adequate legal, institutional, financial, technical and human resources. Physical protection in nuclear/radiation field is specific in many sense, and should be given utmost consideration, which often simply means priority. Among the security prerequisites, it is commonly taken for granted that necessary knowledge and competence do exist per se throughout human resources (HR) for physical protection. However, this is not always the case, just the contrary – time, efforts and assets are frequently wasted because these HR fundamentals are not set solid at first. Education and training are paramount in building knowledge and competence. It is crucial to recognize the importance of formal education, primarily at universities and dedicated security education institutions. IAEA based international nuclear security education network (INSEN), even not so long in existence, proved pivotal in the field. Standardization of educational programmes and thoughtfully conceived development of textbooks/literature on key NS subjects turned out to be highly appreciated in Member States. Especially small, developing, non-nuclear countries, starting their NS education from the scratch, are profiting from the network. Formal education, preferably following INSEN gudelines, is thus fundamental for HR development in NS, physical protection in particular. Results are quickly visible once the country sets on this course. Training is another aspect of HRD, equally important – however quite different in nature from education. Another international network (Nuclear Security Support Centres – NSSC) deals, inter alia, with training aspects of competence. While education basically stands for knowledge, training contributes to its practical applicability – both being essential constituents of competence. For competence to be complete, one should also include experience and ethics. Training cannot replace education – attempting so, one falls into a typical competence pitfall. Training is thus meaningful only when superposed onto an adequate education. Messing up these terms will lead to a false perception of knowledge and competence (quasi-knowledge and quasi-competence); eventually, security will inevitably be compromised. The same is valid for experience – although always welcome and respected, experience cannot replace neither education, nor training,

not to speak both of them. Only on the top of the two, experience makes sense and gives a fine touch of maturity to competence. Ethics is perhaps the least questioned among competence ingredients – it is also often taken for granted. Without going into elaboration, it is enough to think of a knowledgeable, trained, experienced and malevolent person at a responsible position somewhere in nuclear sector physical protection – a serious security issue per definition. Quasi- knowledge and quasi-competence are more perilous for NS than ignorance and incompetence (i.e. clear lack of knowledge and competence), because the latter are more explicit and easier to recognize/prevent/rectify. It is important to note that quasi-knowledge and quasi-competence can be traced behind nearly all nuclear mishaps – from minor/benign incidents (like just clumsy handling of some situations in nuclear community, e.g. poor communication with public/media), to major accidents with grave consequences. All aspects of competence should thus be properly addressed – education, training, experience and ethics – with adequate place and emphasis for each. There are very few things which can contribute so beneficially to security like knowledge and competence; there are even less of those which can cause so much harm as the lack and/or false perception of them.

Synopsis ID: [282]

Holistic Approach to Nuclear Safety, Security and Safeguards: Opportunities and Challenges

Karanam, R.[1]

[1] Department of Atomic Energy, India

Corresponding Speaker: R. Karanam

Advent of nuclear energy and its utilisation for the welfare of the humankind brought along with it many opportunities and challenges. Peaceful utilisation of atomic energy should ensure that (i) nuclear material and nuclear facilities, other radioactive materials and associated facilities are secured with adequate physical protection measures adhering to a well laid out and internationally acceptable safety and security culture, and (ii) Nuclear material is safeguarded with adequate nuclear material & control (NMAC) measures adhering to a well laid out and internationally acceptable safeguards culture. Thus the triad of nuclear safety, security and safeguards is critical and indispensable in peaceful utilisation of atomic energy. Inadequacy in implementation of any of the three result in vulnerable situations necessitating corrective and remedial measures. All the three organs of this triad should always be treated together lest in isolation they lose their effectiveness. For instance: (a) We may have an acceptable NMAC measures for effective safeguards but inadequacy in safety and security measures render the nuclear material vulnerable; and (b) We may have an acceptable physical protection measures but inadequacy in safeguards and security measures render them ineffective. A holistic approach is therefore desirable to take the cognizance of the fact that the triad organs are not independent of one another. The best practices of each of the elements shall have to be pooled together to realise the wholesome advantage. Such an exercise is essential both from the point of view of economics, optimum use of technology and human resources. There has been good number of literature references to realise this. Mention may be made of "Integrating Safeguards and Security with Safety" or "Perspectives on Interfaces and Synergies between Safety and Security" etc. It is of critical importance to bear in mind the significant difference in implementation of nuclear safeguards on one hand and of safety and security on the other hand. The Statute of IAEA authorises the Agency to apply safeguards, at the request of the parties, to any bilateral or multilateral arrangement, or at the request of a State to any of the State's activities in the field of atomic energy and in this context safeguards agreements with member states are crucial. The Agency has legal mandate to implement nuclear safeguards in nuclear facilities of a member state. However, this is not the case with nuclear safety and security. When it comes to nuclear safety and nuclear security, these two are the responsibility of individual State and to a large extent, the Agency has only an advisory role or at the most on request, an audit role without any legal authority to enforce its observations by the State. Another fact to be considered is that both safeguards agreement and Convention on Physical Protection of Nuclear material are limited to nuclear material and nuclear facilities only. A non-binding

code of conduct is available for radioactive sources. It should be mentioned that nuclear security encompasses both nuclear material and nuclear facilities as well as other radioactive material and associated facilities. There should be a mechanism to account for the other radioactive material in a State, similar to NMAC for realising nuclear security of these materials. Additionally, recent international events have entrusted a more central role to IAEA in matters of nuclear security. There are four agencies identified to address different facets of nuclear security and IAEA is supposed to play "central role". It is essential to define exactly this "central role" of the Agency. The aim of this presentation is to focus on these challenges and opportunities the solutions bring when a holistic approach to nuclear safety, security and safeguards is adopted

Synopsis ID: [44]

Enhancement the Surveillance Programme of Nuclear Facilities based Safety and Security Synergy Concepts

Abdelaal, M.[1]

[1] Egyptian Atomic Energy Authority (EAEA), Egypt

Corresponding Speaker: M. Abdelaal

This paper introduces the applicable concepts of the synergy between safety and security of nuclear facilities to enhance the surveillance and maintenance programme. The inspection and maintenance task of the ETRR-2 control system is very difficult because of depth of water and location of the control mechanism. The reloading of the guide box, which housing the control rods should be done underwater. We proposed using of underwater sealed camera with four channels digital video recording (DVR) to connect the operators working area (reactor hall) and the maintenance working area (control mechanism room) to optimize the integration of both groups and enhance safety and security culture, maintenance attitude and performance of the reactor staff. The application made the task easier and successfully completed. The application is used as a tool for training and education as a learned lesson of the synergy between safety and security.

Synopsis ID: [191]

Training and Exercising the Nuclear Safety and Nuclear Security Interface Incident Response through Synthetic Environment, Augmented Reality and Virtual Reality Simulations

Waller, E.[1], Chaput, J.[2]

[1] University of Ontario Institute of Technology, Canada

[2] International Atomic Energy Agency

Corresponding Speaker: E. Waller

Nuclear safety and nuclear security are key elements of a State's national program for the safe and secure use of nuclear technology. During the planning stages, the linkages and interfaces between nuclear safety and nuclear security personnel remain strongly coupled to the fundamental safety objective, which with respect to all circumstances that give rise to radiation risks, is to protect people and the environment from the harmful effects of ionizing radiation . With respect to both nuclear safety and nuclear security there is a clear potential for events which require a response within a State's local or national level infrastructure. A response could be dedicated to issues relating exclusively to nuclear safety (such as a technological failure of a system at a nuclear power plant) or exclusively to nuclear security (such as attribution of discovered material out of regulatory control to a potential hostile actor). Regardless of the triggering circumstances of the event, there is always a potential for the nuclear safety or the nuclear security responses to have repercussions on the other. During the 2011 response to the accident at the Fukushima Daiichi nuclear power station, there was an obvious nuclear safety response taking place. At the same time, due to the damage to infrastructure onsite there was an impact on the operation of nuclear security related equipment (fences, camera, sensors, etc.), which would have necessitated cooperation between security and safety personnel which were functioning to meet their specific objectives and goals. The impact of the accident at the Fukushima Daiichi nuclear power station on the security infrastructure and the response capabilities onsite remains one of the very few areas where there is a potential for many lessons to be learned which have not already been identified in other exhaustive and nuclear safety focused reviews . In 2013, Mexico reported a stolen category 1 (extremely dangerous) source to the international community . During this nuclear security event police forces were tasked in locating the device and the suspects, which could have had nefarious intentions. Such a nuclear security event also triggered a radiological emergency situation as there was a potential for members of the public to be unintentionally exposed to this lost material. The response interface between nuclear safety and

nuclear security personnel required tight cooperation to successfully respond and address the overlapping (safely locating the material) and exclusive (forensics investigation to identify suspects) issues of each sides. A reasonable conclusion is that for events of significance, a nuclear safety event (nuclear or radiological emergency) has the potential to trigger a nuclear security event and a nuclear security event has the potential to trigger a nuclear or radiological emergency. Recognizing this therefore requires State's to ensure there are clear interfaces between nuclear safety and nuclear security not only during the response but during the planning phase. The objective of a State's nuclear security regime is to protect persons, property, society, and the environment from harmful consequences of a nuclear security event . The goal of emergency preparedness is to ensure that an adequate capability is in place within the operating organization and at local, regional and national levels and, where appropriate, at the international level, for an effective response in a nuclear or radiological emergency . Both the objective of nuclear security and the goal of nuclear safety are closely related with only minor academic differences. Training for cooperation and exercising the interface between nuclear safety and nuclear security responders can be a challenging and costly endeavor. Nuclear safety exercises can require the use of radiological material and extending planning to create technological scenarios which are both realistic and significantly taxing on emergency response personnel. Nuclear security exercises can require planning for the use of simulated adversaries, access to facilities which are used on a regular basis (e.g. a nuclear power plant) and the careful incorporation of neutralization devices (weapons) such that the responders are able to have their full suite of response capabilities at hand. Technologies are available which have the potential to make these types of cross-functional exercises easier and less costly to implement. This paper and presentation will: • Discuss the challenges of organizing exercise scenarios which successfully evaluate both nuclear safety and nuclear security aspects • Provide examples of technologies which can be used to generate scenarios for training and exercising the response to combined nuclear safety and nuclear scenarios via synthetic environments, augmented reality and virtual reality systems • Provide an example and demonstration of the application of virtual and augmented reality to a nuclear safety and nuclear security scenario • Discuss the potential future opportunities for States to cooperate on improving the current response interfaces between nuclear safety and nuclear security

Synopsis ID: [197]

Security/Safety Interface in Practice: Lessons Learned From the Swedish Joint Regulatory Project

Sjöström, J.[1]

[1] Swedish Radiation Safety Authority, Sweden

Corresponding Speaker: J. Sjöström

Introduction In 2008 the Swedish Radiation Protection Institute and the Nuclear Power Inspec- torate merged to form a new authority – the Swedish Radiation Safety Authority. With the new authority, a need for updates and changes to regulations were identified and in 2013 the director general launched two projects with the purpose to develop a regulatory structure with regulations and guidance that covered all aspects of the authoritys' regulatory mandate. One project deals with regulations for nuclear facilities and the other project with radioactive sources, technical installations and health care applications. The need for a new regulatory approach was further emphasized by the 2011 IPPAS mission, 2012 IRRS mission as well as the introduction of Euratom 2013/59 and Euratom 2014/87 and WENRA SRL. Early on in the projects it was decided that security requirements should be an integrated part of all regulations as opposed to be handled in its own publication. The discussion in my presentation will focus on the safety/security interface, examples of joint regulations, and the positive and negative consequences that results from the integration of security into new regulations for nuclear power plants.

The Swedish regulatory project Top legislation consists of relevant EU-legislation and directives as well as the Radiation protection act and the Nuclear activities act. The regulatory structure is based on a hierarchical structure in three levels: Level one: "Fundamental requirements for ionizing radiation" and is not nuclear power specific. Level two: Contains requirements on facility (activity) level. For nuclear facilities there are three separate publications regarding Design & Construction, Assessment & Analysis, and Operations. Level three: More detaild regulations on specifik aspects of radioation safety Here we found lifting devices, preassure-bearing devices as well as Information and IT security.

Security requirements and examples of integration (DiD) The new regulations is based on a, primarily, performance based approach with some prescriptive requirements. As an example, the Design & Construction regulation consists of requirements for limited access area, protected area, and vital areas. Requirements also cover protection of CAS as well as the main control room. However, requirements does not explicitly state the level of protection required for each area or barrier. Instead, references are made to the design basis threat (DBT) and the Plant state conditions. The analysis

regulation outlines the regulatory requirements for the various types of anlysis that are required for the nuclear reactor. In Sweden, the postulated initiating events have historically consisted of three parts: internal events, internal hazards, and external hazards. Postulated malicious acts have not been included in the scope of postulated initiating events, but handled separately in a largely separate set of regulations. In the new requirements for initiating events, postulated initiating events include malicious acts in addition to internal events and external events. This is a result of the holistic approach to safety that SSM has applied in the update project, where the acceptably safe outcome of an event, the protection of humans and the environment from the harmful effects of radiation, is the same regardless of the type of event. integrated Defence-in-depth (DiD) model which is based on the safety DiD where the respective levels from the DBT has been added. The purpose is to help the operator to understand what systems and functions that must be operational for every DBT level as well as providing acceptable release rates for every DiD level. It also serves as a priority indicatior for the operator when analyzing vital areas. Implications for security Following are some positive and negative implications for security: + Increased awareness of security requirements as they can't be ignored or "forgotten" when in the same document as opposed to being in a separate document only read by security professionals. + Clear link to requirements for competence, staffing, overall construction requirements + Security seen as one aspect of the overall safety of the reactor just as power supply + More performance based as opposed to prescriptive approach gives a more balanced PPS clearly connected with the safety DiD - Difficult to find all security related requirements when they are organized under different chapters and sometimes in different publications. Example of this is all requirements for the main control room and central alarm station are located under the "Control Room" section. - Security is not visible in its own regulatory publication Summary The proposed update of the regulations aims at jointly regulating all aspects of radiation safety, i.e. safety, security, radiation protection, and nuclear non-proliferation. The benefits of this holistic approach to safety is a more balanced construction of a reactor based on a better understanding of the actual safety significance of different structures, systems and components.

Synopsis ID: [18]

Safety–Security Interface at Bhabha Atomic Research Centre, Mumbai, India

Rajdeep, R.[1], Jayarajan, K [1]; Taly, Y.[1]

[1] Bhabha Atomic Research Centre, Mumbai, India

Corresponding Speaker: R. Rajdeep

Bhabha Atomic Research Centre (BARC) is the premier organization of India actively involved in the research and developmental activities related to nuclear science and technology for the benefit of society and the nation. BARC has various facilities like nuclear fuel fabrication facilities, research reactors, spent fuel storage facilities, nuclear fuel re-cycling facilities, radioactive waste management facilities and various Physics and Chemistry laboratories. In BARC, aspects related to safety and security are given paramount importance from the stage of concept to commissioning and design to decommissioning.

BARC Safety Council (BSC) is the apex committee in the three tier safety and security review framework of BARC. BSC functions as regulatory body for BARC facilities. The second tier has Operating Plants Safety Review Committee (OPSRC), Conventional & Fire Safety Review Committee (CFSRC), Committee to Review Applications for Authorization of Safe Disposal of Radioactive Wastes (CRAASDRW) and Physical Protection Systems Review Committee (PPSRC) in addition to 14 Design Safety Review Committees for the new projects. The third tier has 16 domain dependent Unit Level Safety Committees (ULSCs). Each committee consists of 8 to 12 experts, including a Chairperson and a Member-Secretary.

For integrating safety and security review of BARC facilities, an expert committee named Physical Protection Systems Review Committee (PPSRC) has been introduced in the second tier of safety and security review framework of BARC. PPSRC is responsible for the review of operational, maintenance and performance aspects of Physical Protection Systems (PPS) and their up-gradation for the existing facilities. PPSRC carries out review of PPS design and PPS requirements for the new projects. Review of security related incidents is also carried out by PPSRC. PPSRC recommends matters related to PPS and security to BSC for further review, if required.

PPSRC has constituted a regulatory inspection team which inspects and evaluates the performance of the Physical protection systems and security of BARC facilities at regular interval. Based on the recommendations of Regulatory Inspection Team-Physical Protection Systems (RIT-PPS), the Physical Protection Systems are continuously reviewed, augmented and upgraded. This paper describes the successful attempt of integrating safety and security at BARC which improved Physical Protection Systems and nuclear security.

Synopsis ID: [33]

Training on Nuclear Material Accounting and Control (NMAC) for Emerging Countries in Asia

Robertson, K.[1], Vidaurre-Henry, J.[2] , Hirai, M.[1]

[1] Integrated Support Center for Nuclear Nonproliferation and Nuclear Security, Japan Atomic Energy Agency, Japan

[2] Japan Atomic Energy Agency, Japan

Corresponding Speaker: J. Vidaurre-Henry

This paper describes the framework for implementing nuclear material accounting and control (NMAC), both from the perspective of nuclear security and from the perspective of nuclear safeguards. It compares and contrasts international instruments as well as IAEA publications and guidelines in these two fields. There are some important differences between the objectives of security and safeguards. However, NMAC tools, concepts, resources, and activities used in support of security often overlap significantly with those used in safeguards. The efficiency and effectiveness of NMAC may be enhanced by taking a holistic approach, coordinating efforts between security and safeguards. Based on this framework, this paper identifies the capacity-building support needs of regulatory authorities and operators responsible for NMAC in support of security and safeguards. The Integrated Support Center for Nuclear Nonproliferation and Nuclear Security (ISCN) of the Japan Atomic Energy Agency (JAEA) is a Center of Excellence that conducts a variety of training courses in the fields of nuclear security and safeguards, primarily for participants from Asia. Among these courses, the ISCN has designed a series specifically on NMAC, in cooperation with the U.S. Department of Energy/National Nuclear Security Administration (DOE/NNSA). These courses take advantage of the ISCN's training aids and environments, including real equipment for non-destructive assay (NDA) and containment/surveillance, as well as a realistic Material Balance Area (MBA) Kit developed by DOE/NNSA and Pacific Northwest National Laboratory (PNNL). The JAEA has also begun applying its Virtual Reality System as a hands-on tool for NMAC training. The ISCN implemented its first dedicated NMAC course in an emerging country (nuclear newcomer) in Asia in January 2016. In designing the course, the ISCN has taken a holistic approach to NMAC training. The results achieved so far demonstrate that a Center of Excellence can provide training in NMAC as a standalone discipline, satisfying both safeguards requirements and security objectives. This paper explains how the ISCN has developed these courses and presents possible future actions for consideration by the IAEA and other Centers of Excellence.

This paper represents the views of the authors. It does not represent the views of any institution.

Synopsis ID: [120]

Application of NUCMAT for improving nuclear materials accounting for and control practice

Bznuni, S.[1], Amirjanyan, A.[1]; Katsenelenbogen, S.[2]

[1] Nuclear and Radiation Safety Center, Armenia

[2] ADSTM

Corresponding Speaker: S. Bznuni

The software tool called NUCMAT was developed with the purpose to facilitate implementation of an integrated nation al-level nuclear materials inventory management system in countries with medium and small nuclear program (NPPs, research reactors, LOFs etc). NUCMAT is comprehensive nuclear material accounting and control software that has three main pillars:

Safeguards: Accounting for and reporting of nuclear materials in full compliance with the IAEA requirements and regulations 2) Nuclear Security: Interface between nuclear material accounting and protection of nuclear material 3) Information Security: Sensitive data protection in multiuser environment against external attacks and insider threat. NUCMAT is web-based program employing ASP.NET and Microsoft SQL technologies that allows to apply it both at state and facility/LOF levels using either single server or distributed network configurations through protected (e.g. VPN+) communication channels. NUCMAT could be used in stand-alone option as well. NUCMAT allows user to perform all inventory changes except for uranium category changes. It automatically calculates and updates inventory of nuclear materials of all types and categories: source materials and special fissionable materials as well as to close balance of nuclear materials. Besides all IAEA required reports (PIL, ICR, MBR) NUCMAT allows user to generate additional reports to facilitate regulatory body/IAEA inspections, like LII, and generate free format report applying powerful filtering and sorting tools available in NUCMAT to facilitate nuclear security efforts. NUCMAT has strong internal QA/QC system to prevent inadvertent errors of users via generation of warnings and blocking unacceptable actions, e.g. in case of entering data outside of acceptable data parameters, not allowed symbols, duplicate records, date conflicts, missing information, unauthorized action etc. In NUCMAT the user-entered information was minimized by drop-down lists and logical cross-links. In addition, to prevent user effect NUCMAT accepts information from external files, for example nuclear fuel vendor files in case of NPPs and research reactors. Furthermore, accounting reports generated in MS Excel format are fully compatible to pass QA/QC control via IAEA QCVS program. To support material protection efforts NUCMAT provides user with recoverable history of each nuclear material with exact specification of the location as well as comprehensive, traceable log information covering user

activity, inventory changes, backup/restore, report generation. This allows to prevent attempts to alter data in existing record, delete record, Furthermore, NUCMAT provides special user categories and hierarchy that assures effective and efficient cross-check and control to combat with insider threats. In NUCMAT strong multi-layer means were deployed to guarantee secure storage and transfer of sensitive information. It has been achieved by applied development technique (Dot.NET), secure code, used protocol (https), user action and access rights, limited access to database (access only to the MBA/KMP/Location to which user have access granted), strong password rules and requirements (password minimum, uniqueness, history, age), screen locking. In addition, NUCMAT protects data from external robot-attacks via using CAPTCHA and locking out of user after permanent failed attempts. NUCMAT passed independent security vulnerability test with overall good grade indicating that the capabilities/approach is the best option evaluated and aligns with industry best practices.

Synopsis ID: [205]

U.S. Experience Implementing Nuclear Material Accountancy and Control (NMAC) & Physical Protection (PP) for Nuclear Security

Lafleur, Adrienne[1], Martin, O. [1], Browne, M.[1],Winowich, N.[2]

[1] Los Alamos National Laboratory, Department of Energy, United States of America

[2] Sandia National Laboratory, Department of Energy, United States of America

Corresponding Speaker: A. Lafleur

The ability to effectively and efficiently quantify the type and amount of nuclear material, as well as protect and secure the material at a broad range of nuclear facilities is essential to ensuring PP and NMAC measures meet domestic and international standards and recommendations. The International Atomic Energy Agency (IAEA) Information Circular (INFCIRC)/225 Revision 5, "Physical Protection of Nuclear Material and Nuclear Facilities," emphasizes the need for both PP and NMAC to prevent and identify any unauthorized removal of material during use, in storage, or in transport. A nuclear facility will likely contain nuclear security, safety, and safeguards programs, each with specific requirements and objectives. Despite the different goals of each program, a fundamentally accurate quantification and characterization of nuclear and radioactive materials (form, mass, age, etc.) is critical to achieving overall objectives of nuclear security, safety and safeguards.

Global terrorism, cyber security attacks, and regional instabilities underscore the need to strengthen information security (access to information about nuclear material) and physical protection measures (access to nuclear material). Nuclear security, safety, and safeguards pro- grams involve access to nuclear material information usually stored in databases, in order to ensure specific program requirements are met (e.g. criticality safety, radiation protection, NMAC, safeguards declarations etc.). A key challenge is establishing access controls, maintaining the databases and ensuring that each program is using consistent up-to-date data. NMAC, cyber security, and physical security present overlapping challenges that require integrated solutions while not hindering operations. By recognizing the interfaces between nuclear security, safety and safeguards and shared overall objectives and commonalities, all three can be executed in a more efficient and sustainable manner. Taking advantage of these mutually beneficial relationships is and will continue to be critical as new and more sophisticated threats evolve, and resources to address these challenges remain limited.

This paper describes the interfaces between nuclear security, safeguards, and safety, specifically focused on NMAC and PP; U.S. challenges and experience implementing NMAC and PP at nuclear

facilities both domestically and internationally; lessons learned and best practices based on U.S. experiences; and specific examples of areas where better integration of 3S would be beneficial.

Examples of the interfaces between nuclear security, safeguards, and safety and areas where better integration would be beneficial are given below: 1) Many safety and safeguards measures can also serve as security measures, e.g., thick concrete walls intended as radiation shielding can be leveraged as access delay with minor design attention, or emergency power provided for safety and safeguards measures could be integrated for security measures. 2) Dual role (safeguards/security) measures should be designed by practitioners of each discipline, in concert, e.g., tracking rad workers within a balance area for evacuation audit purposes can also provide a means to track them for material access or two person rule purposes. 3) Single role measures should be designed to minimize effect to other disciplines, e.g., detection and delay at the target is more effective for security and has less effect on workers/systems away from target.

Systems should be integrated, e.g., design should begin with project charter, to which all disciplines/interests contribute (safety, safeguards, tech security, response force, operations), and the main stakeholders (such as Operations and Response Force, who actually occupy the facility), must agree to all security and safeguards designs at each stage of design 5) Measures of success and sustainability could include human reliability programs and training.

The purpose of assessing the commonalities, U.S. specific experiences, and areas where better integration would be beneficial in our paper is to identify key mechanisms that could be implemented to better address evolving nuclear security and nonproliferation challenges.

Synopsis ID: [97]

WNTI Working Group on UF6 cylinder Identification

Charette, M.[1], Whitaker, M.[2]

[1] Cameco Corporation, Port Hope, Canada

[2] Oak Ridge National Laboratory, Department of Energy, United States of America

Corresponding Speaker: M. Charette

In May 2014, the World Nuclear Transport Institute (WNTI) formed an ad-hoc working group to focus on the identification of uranium hexafluoride (UF6) cylinders. WNTI was founded in 1998 to represent the collective interests of the nuclear transport industry, and those who rely upon it in the safe, secure, efficient, and reliable packaging and transport of radioactive materials. The working group scope adopted by over 25 members is to establish an industry-wide identification format that provide for uniquely identifying UF6 cylinders and to investigate methods for making the unique identifier (UID) machine-readable and independently verifiable by the International Atomic Energy Agency (IAEA). The working group held multiple conference calls and two face-to-face meetings to reach a consensus on recommendations for a preferred identification format and technology for machine readability and testing of key functionality. The standard is in draft format and expected to be issued this year. The paper will provide an overview of the standard and benefits to the IAEA and Industry of adopting a global cylinder identification system.

Synopsis ID: [234]

Comparison between Nuclear Material Accounting and Control for Nuclear Security and a State System of Accounting and Control for Safeguards

Larsen, R.[1], Gibbs, P.[2], Crawford, C.[2]

[1] International Atomic Energy Agency (IAEA)

[2] Oak Ridge National Laboratory, Department of Energy, United States of America

Corresponding Speaker: R. Larsen

In 2014, Nuclear Security became its own division, and in 2015 Nuclear Security Series Implementing Guide 25-G "Use of Nuclear Material for Accounting and Control for Nuclear Security Purposes at Facilities" was published. The publication of this guide established the new Material Accounting and Control (NMAC) Program. This newly established program was placed in the "Materials and Facilities" section of Nuclear Security as part of its core physical protection mandate and a new NMAC course was developed to address the principles of NSS 25-G. Prior to this time, courses existed pertaining to International Safeguards and, specifically, State Systems for Accounting and Control (SSAC), which has extensive overlapping functions with NMAC. While the SSAC is safeguards-focused, NMAC is security-focused, although not necessarily always identified as "security". In some states, the term "Safeguards" has been used interchangeably with what the IAEA has defined as the security-focused NMAC. The primary difference is that the SSAC focus on how states report on their safeguards obligations while NMAC focuses on domestic accounting and control at the facility-level to develop accurate accounting of material and control measures to prevent unauthorized removal by non-state actors and provide assurance that nuclear materials are present and being used for their intended purposes. The goal of accounting of material is the same for both organizations, however for Safeguards, the goal is to verify that the State has not diverted nuclear material whereas for Nuclear Security, the goal is to account for and protect material from unauthorized removal by non-State actors. To adequately communicate this difference, an NMAC course has been developed for Nuclear Security that provides the proper focus, perspective, and threat, while differentiating its goals from that of SSAC. While Safeguards are frequently discussed in relation to Nuclear Material Accounting and Control, .there are very distinct differences between the two programs: 1) Purpose: the safeguards inspection regime, which is conducted by the IAEA Safeguards organization monitors Member States subscribing to the Nuclear Non-proliferation Treaty (NPT). The purpose of IAEA inspection is to confirm States are not making use of nuclear materials outside of their commitments/agreements under the NPT. In contrast, the IAEA Division of Nuclear Security is

assisting Member States to develop a domestic NMAC system within individual Member States. The purpose of such a system is for Member States to protect, control, and account for its own nuclear materials. A domestic NMAC system runs under the authority of the State's government, in which the concern is theft of nuclear material that could result in weapons proliferation by a non-State Actor (see UNSCR 1540). An NMAC system allows a state to demonstrate that it has an appropriate system in place to detect the unauthorized removal of nuclear material by an adversary from a nuclear facility. 2) Timely Detection: IAEA safeguards requires a State to ensure that a significant quantity (SQ) of material diverted to a state-run, clandestine program would be detection in time. Given the complexities and cost to develop a weapons program, timely detection to the IAEA is measured in months and is based upon many of the technologies and infrastructures that would have to accompany the theft or diversion in order for a state to become operational. Conversely, a domestic NMAC system aims to detect removal of smaller quantities of material more quickly as well as provide routine assurances that nuclear materials are being used for their intended purposes. IAEA safeguards are implemented by international and national treaty, while Nuclear Security NMAC is an important national responsibility. At the technical level, significant synergies between NMAC and Safeguards exist, allowing a state to take advantage of functions conducted in one discipline better optimize resources and benefit from the exchange of experience and expertise between the two programs.

Synopsis ID: [5]

Computer Security Design Methodology for Nuclear Facility & Physical Protection Systems

Agbemava, N.[1], Gyekye, P. [1]

[1] Nuclear Regulatory Authority, Ghana

Corresponding Speaker: N. Agbemava

Currently, computer security is one of fundamental design attributes that are necessary in any integrated Industrial Control System (ICS) and design process. A standard design approach is to identify significant computer security risks in the ICS Architecture and implement protection layers to mitigate the risks in accordance to known International Standards, Guidelines or recommendations (i.e. IAEA NSS 17, ISA 99, IAEA NSS 13, INPO 10-008, NIST standards, and US Nuclear Regulatory Commission Guideline 5.71, IAEA NST045 Computer Security nuclear facility DRAFT Implementing Guide). A majority of these standards recommend embedding the DID (Defence in Depth) approach in the ICS architecture design. This is seen as a reasonable approach to protect the ICS from computer security attacks. For an ICS application in a nuclear facility, DID approach was adopted using the computer security protection layers within the nuclear ICS Architecture. Multiple analysis of the ICS architecture was performed during research reactor design process (i.e. such as target set analysis, Critical System/Digital Asset identification) before the system designer adopts the DID approach. The design and implementation processes were carried out under a computer Security Life Cycle Program and may vary between control and protection systems. In this paper, computer security design process and its implementation in the nuclear facility ICS Architecture is explained. A complete nuclear facility ICS computer security life cycle program and how DID approach is sequenced in this life cycle is described.

Synopsis ID: [56]

The Strategies and Policies for Physical and Cyber Security in Sudan: A Case Study on Sudan's Governmental Data Centers

Abdulrahman, M.[1], Ayoub, K.[2]

[1] Assistant Professor

[2] Engineer

Corresponding Speaker: M. Abdulrahman

Due to wide applications of information technology in nuclear industry, significant needs to secure the top sensitive data which follow from nuclear institutions have been risen. The risk on computer security can be divided into two parts which are the physical and cyber attacks, so it needs a special attention. In Sudan, there are no separate data centers for nuclear institutions; however, the Sudanese government hosts the data in secured central data centers to avoid any attack on sensitive information. The official records of National Information Center and Sudan center for Information Security show a significant improvement in security status in Sudan. This study illustrates the governmental policies and strategies of cyber and physical protection in the central data centers in Sudan along with up to date statistics of the number of attacks on these centers.

Synopsis ID: [142]

Differences between Defence in Depth for Computer Security and Physical Protection

StJohn-Green, M.[1]

[1] United Kingdom

Corresponding Speaker: M. StJohn-Green

Defence-in-depth is a well-known concept in physical security, embodied in the design of medieval castles with their concentric walls, and used today in many contemporary defensive physical security designs. The term is also used in computer security but, while the principles are the same, this paper will show that there are important distinctions in the way that the concept of defence-in-depth applies for the defence of networked digital technology. Physical defence-in- depth is designed such that the adversary will be delayed and detected at particular boundaries, offering the defender sufficient time to respond. This paper will consider the effect of blending a cyber-attack with a physical attack and show that some assumptions about defence-in-depth may not apply: does the nature of the blended attack vector offer the means to attack those security boundaries in a different sequence? Consider, for example, an insider introducing malicious code within the security perimeter to undermine physical protection. Second, should the defender have confidence that the attacker will be detected at key security boundaries? Consider, for example, the evidence of the effectiveness of current malware detection methods to detect cyber-attacks and the effect of a cyber-attack on physical protection mechanisms. If the attacker is not detected at particular boundaries, the notion of delaying the attacker has less relevance because the defender cannot rely on that time to muster his resources. This paper will show that the defender cannot make key assumptions about the sequence of a blended attack, and about detection and delay of the attacker at key security boundaries. Consequently, the paper will consider what should be the parameters for effective defence-in-depth for networked digital technologies, to defend against pure cyber-attacks and against blended attacks.

Synopsis ID: [240]

Cyber-Physical System Security

Long, A.[1], Gelfand, B.[1]

[1] Los Alamos National Laboratory, Department of Energy, United States of America

Corresponding Speaker: A. Long

Alia Long, Boris Gelfand Los Alamos National Laboratory Track classification: Computer Security A cyber-physical system is a network of coupled computing nodes sensing and controlling physical processes. Traditionally, cyber-physical refers to networked infrastructure and industrial control processes. We propose that all networked systems are cyber-physical in nature, especially when assessed for security risk. Major attacks have been made on controllers of physical processors at the scale of a targeted, nuclear material, processing plant and at the level of a distribution of in-home commodity items made to work together for a larger purpose. Understanding these systems and addressing issues requires an integrated, cross- domain approach.

Examples of these complex systems come in the form of aircraft control, autonomous vehicles, industrial control systems, and the internet of things. When considering the security of such systems, the complexity expands and simpler systems fall into the realm of historic cyber- physical systems. Networked devices which have any combination of physical I/O and computing power should approached be as an end-to-end, whole system with regards to security analysis. Cybersecurity, computer security, is no longer enough when a computer can have impact on the physical world and vice versa. Systems designed and built with multiple domain impacts must consider cross-domain security. A trend in hardware design is to use an off the shelf microprocessor or microcontroller with a standard interface, and which is increasingly powerful and flexible for

multipurpose use. For instance, a designer can know how to program a Microchip PICOR

and use the device in motor control, human interface, or network applications without the need to learn new hardware design, software interface, or coding technique in each application. While a particular design may not have all capabilities enabled, it also may not be designed to keep others from enabling a new capability in a design.

Defense in depth is a concept in both physical protection and cyber security which needs to cross realms. The entire path of data must be considered, discounting nothing as trivial, when even a flashing LED on a computer can give away information. It will always be challenging to balance convenience, trust, and cost/capability, but a clear process and informed operators are the first defense to any attack. Research and development of cyber-physical specific security techniques must

be a priority. Successful use of this approach will help secure against unauthorized removal of nuclear material during use, storage and transport and against the sabotage of nuclear material sustaining security/physical protection regimes. This paper supports an increase in the understanding of the interface between physical protection measures and systems and computer

security and considerations when developing security plans to include a threat-based, risk- informed approach. Findings will support enhancement of Nuclear Security Training and support centers increasing caliber of IAEA support to partner countries.

LA-UR-17-24002

Synopsis ID: [43]

Nuclear Security and Amended CPPNM Recommendations - Implementation Perspective

Qureshi, S.[1]

[1] Indian Institute of Technology Kanpur, India

Corresponding Speaker: S. Qureshi

Nuclear security has assumed utmost importance in the changed global scenario as occurrence of a malicious act involving nuclear or radioactive material is no longer a hypothetical threat. According to IAEA Incident and Trafficking Database (ITDB) Fact sheet 2016, there were 2889 confirmed incidents of illicit trafficking, thefts, losses and other unauthorized activities and events involving nuclear and radioactive material from 1993 till December 31, 2015 as reported by the participating states. Of these 2889 confirmed incidents, 454 incidents involved unauthorized possession of nuclear or radioactive material, 762 incidents involved thefts or losses and 1622 incidents involved other unauthorized activities and events [1]. The number of reported incidents from 2013 to 2015 is more than 30 and due to reporting time lag of 2 – 3 years, this number is likely to increase. ITDB scope covers all types of nuclear materials natural or artificial including scrap metal.

These confirmed incidents included 13 cases of highly enriched Uranium (HEU), 3 cases of Plutonium and 5 cases of Plutonium Beryllium neutron sources. Some of these cases involved attempts to sell or traffic these materials across international borders.

The incidents also included thefts or losses of radioactive sources not only from facilities but also during transportation and majority of these radioactive sources were used in industrial and medical applications. The industrial sources were related to construction and mining involving isotopes like Iridium-192, Caesium-137 and Americium-241. A significant proportion of incidents reported to ITDB related to sources used in diagnostic and radiotherapy.

The ITDB report is clear demonstration that illicit trafficking, thefts, losses and unauthorized activities and events involving nuclear and radioactive material continue to occur. The persistence of these incidents indicates a continuing nuclear security concern. In the light of these concerns the amended CPPNM version came into effect on 8 May 2016 expanding the previous convention to cover the protection of nuclear facilities and nuclear materials in domestic use, storage and transportation.

In support of the provisions of the amended CPPNM, the states are to develop nuclear security regime particularly regarding physical protection of nuclear material in facilities and during transportation. In developing the regime, IAEAs role is to actively work on the dissemination of the nuclear security recommendations contained in INFCIRC/225/Rev. 5 [2] through expert missions, workshops, and

training courses. IAEA has also committed to provide support to states through IPPAS missions so that states come to a common understanding in regulating, implementing and sustaining physical protection regime.

The key feature of these recommendations is that states establish, implement and maintain nuclear security regime. The overall objective of state's nuclear security regime is to protect persons, property, society and environment from malicious acts involving nuclear material and other radioactive material. The physical protection regime is an essential component of the state's nuclear security regime. The state's physical protection regime is intended for all nuclear material in use and storage and during transport and for all nuclear facilities. The state should ensure the protection of nuclear material and nuclear facilities against unauthorized removal and against sabotage.

Further, on international transport, the responsibility of a state for ensuring that nuclear material is adequately protected extends to the international transport until that responsibility is properly transferred to another state, as applicable.

On the front of legislative and regulatory framework state is responsible for establishing and maintaining a legislative and regulatory framework to govern physical protection. Further, according to the recommendations, the license holder should ensure control of, and be able to account for, all nuclear material at a nuclear facility.

However, the recommendations are silent on the role of licensee in case of unforeseen accident in a facility and who ensures the physical protection of nuclear and radioactive material in such circumstances is not clearly spelled out thus making physical protection of nuclear material vulnerable to thefts in such circumstances. Further, a state which has nuclear power programme may have nuclear regulatory mechanism in some form to assume supervisory role for physical protection of nuclear and radioactive material. However, a state that does not have nuclear power programme may not have a regulatory body and establishment of such a body which assumes regulatory role for physical protection of nuclear and radioactive materials is essential to ensure adequate protection as recommended. The paper will discuss these issues in detail along with the implications these have on the overall objective of ensuring the physical protection of nuclear and radioactive materials and nuclear facilities.

[1] ITDB 2016 Fact Sheet [2) INFCIRC/225/Rev. 5

Synopsis ID: [188]

Implementation of Amendment to the Convention on the Physical Protection of Nuclear Material and Nuclear Facilities in Ukraine: Lessons Learned

Klos, N.[1]

[1] Ministry of Energy and Coal Industry, Ukraine

Corresponding Speaker: N. Klos

In appreciation of its responsibility for the security of nuclear material and peaceful uses of nuclear energy Ukraine acceded to the Convention on the Physical Protection of Nuclear Material following its nuclear disarmament decision in 1993.

In 2000, the Parliament of Ukraine passed the Law On Physical Protection of Nuclear Facilities, Nuclear Material, Radioactive Waste and Other Sources of Ionizing Radiation. As we can see, already then Ukrainian experts believed threat existed in respect of nuclear material as well as of nuclear facilities, radioactive waste and other sources of ionizing radiation that could be used maliciously. Of course this approach to physical protection was to a large degree influenced by the experience of the disaster at Unit 4 of the Chernobyl NPP. Evolving threats to the public and the environment required a broader view of fissile materials requiring physical protection. Accession to the Amendment to the Physical Protection Convection (hereinafter the "Amendment") in 2005 was the next step towards the enhancement of Ukraine's physical protection regime. The Amendment was ratified on 3 September 2008; our state thereby reconfirmed its commitment to the principles of prevention and interruption of sabotage, theft or any other unauthorized removal of nuclear material, radioactive waste, other sources of ionizing radiation and to the enhancement of the nuclear non-proliferation regime.

Implementation of the Amendment into the national legislation occurred in 2009 through modifi- cation of main subject matter laws of Ukraine: on use of nuclear energy and radiation safety and on physical protection of nuclear facilities, nuclear material, radioactive waste and other sources of ionizing radiation.

Creation of a regulatory framework is a time-consuming and extended process involving experts in various sectors with various types of experience and knowledge. In addition, the speed of the review procedure is not the same for different regulations therefore some of them are passed earlier than others. In the meantime, government structure may change and new concepts related to new threats may be introduced. As the result, some legal discrepancies occur, which is the situation characteristic for all countries.

Ukraine is a unique nation considering the hostilities caused by the Russian aggression in its territory. After it had given up its world's second largest nuclear arsenal in 1993, Ukraine used nuclear power for peaceful purposes only. Accordingly, all physical protection systems were designed to operate in a time of peace. The design basis threat does provide for a possibility of "beyond design basis threats" – the ones that exceed design basis (such as an attack of armed forces of a foreign state). Although physical protection systems are designed with reference to a peace time, protection must be ensured under any circumstances. Ukraine aimed to achieve this by envisaging a possibility to respond to "beyond design basis threats."

Other lessons that may be learned from implementation of the Amendment in Ukraine include as follows:

Changes take place gradually. Accordingly, more time is needed to establish new views and to implement decisions based on these views.

Pace of change depends on the support and interest of the senior leaders of the state.

Specific requirements to physical protection help:

organize interaction between competent authorities and senior leaders; • raise the funds for creation and operation of physical protection systems; • formulate a systemic approach to the design and implementation of physical protection measures.

It is important to build a system to train qualified experts and to pass the relevant experience.

Difficulties of translation: nuclear security culture. Ukrainian, as well as many other languages use the same word "" for both "safety" and "security." The official Ukrainian translation of the Amendment ratified by a special law of Ukraine translates "nuclear security culture" as " " ("the culture of protectability"). This is a new term in our legislation so it was decided to provide its definition, which is as follows:

"Protectability of nuclear facilities, nuclear material, radioactive waste or other sources of ionising radiation means correspondence of the level of physical protection of nuclear facilities, nuclear material, radioactive waste and other sources of ionizing radiation with applicable laws."

1. If you need help, don't hesitate to ask it. IAEA provides assistance to the States on their requests. For example Ukraine hosts 5 IPPAS missions, which were very beneficial in all stages of creation State physical protection regime.

In the future, Ukraine will work on improvement of its existing regulatory framework on physical protection, settlement of existing legal discrepancies and building professional capacity in this area.

The ratification of the Amendment surely gave Ukraine a number of advantages, both for the enhancement of the national security and for the strengthening of the national physical protection regime.

Synopsis ID: [25]

Methodology for Upgrading Physical Protection Systems at Nuclear Facilities

Hassan, Z.[1]

[1] Egyptian Nuclear and Radiological Regulatory Authority (ENRRA), Egypt

Corresponding Speaker: Z. Hassan

The physical protection of nuclear facilities is a key part of the national nuclear security regime for States having such facilities. Those States are responsible for establishing, strengthening and sustaining physical protection regime and implementing the associated systems and measures to protect such facilities against theft, sabotage, or other malevolent attacks. Physical protection systems (PPS) should provide deterrence and a combination of detection, delay and response functions to protect against adversary completion of a malicious act. A PPS is consisted of equipment, procedures and personnel that integrated together to achieve the required protection. An effective PPS can be achieved using a systematic design approach that includes identifying the PPS objectives and requirements, designing systems and evaluating the design effectiveness to determine how well it satisfies the established requirements. Based on the evaluation results, the PPS design either implemented or redesigned to correct any deficiencies. After implementation, the PPS should be analyzed and evaluated periodically to ensure that the original protection objectives remain valid and that the system continues to meet them. Whenever the PPS is no longer able to defeat the anticipated threat, it has to be upgraded. Characterization of the ineffective PPS is the initial step of the upgrade process to establish a performance baseline of the system and identify its vulnerabilities. This will be followed by the system upgrade design and evaluation to address the identified vulnerabilities and improve the system performance.

The International Atomic Energy Agency (IAEA) offers assistance to Member-States in devel- oping, implementing and sustaining an effective physical protection regime. This includes the International Physical Protection Advisory Service (IPPAS) and physical protection systems upgrades as well.

Egypt acquired various nuclear facilities exclusively used for the peaceful applications and continuously concerned in enhancing and sustaining its physical protection regime that covers all existing nuclear applications especially nuclear facilities. In this context, Egypt has benefited from the IAEA activities to support its efforts in sustaining its physical protection regime, through having an IPPAS mission and upgrading PPS at some of its nuclear facilities in accordance with the international guidance. During the PPS upgrade process, a structured methodology was followed to determine the security requirements and best solutions to fulfil these requirements. The first step was the determination of the security problem and definition of the overall security needs in a document known as operational requirements Level-1 (OR-1). This document was developed based on a

systematic assessment of the problem and a best available solution in conjunction with the alternative options. OR-1 was followed by developing another document known as operational requirements Level-2 (OR-2) that addressed the individual security measures. OR-2 was a basis for the performance specification and assisted in deciding the most suitable system requirements. Derived from OR-1 and OR-2, a detailed system performance and technical specifications were identified in a document known as statement of work (SoW). This was followed by a bidding process and system installation and commissioning. This paper describes issues related to upgrading the PPS at nuclear facilities and outlines the approach for designing, developing and implementing upgraded PPS. In addition, the gained experience and learned lessons from PPS upgrading for some Egyptian facilities are briefly described.

References -IAEA, Nuclear Security Recommendations on the Physical Protection of Nuclear Material and Nuclear Facilities, INFCIRC/225/Revision 5, Nuclear Security Series No. 13, Vienna, Austria (2011). -IAEA, Physical Protection of Nuclear Material and Nuclear Facilities (Implementation of INFCIRC/225/Rev. 5), Draft Implementing Guide, Vienna, Austria (2015).

-IAEA, Project Support and Management Process for NSNS Projects: Information for Member- States, Vienna, Austria (2016). -IAEA, Handbook on the Physical Protection of Nuclear Material and Facilities, TECDOC-1276, Vienna, Austria (2002).

Synopsis ID: [115]

Sustainability of Physical Protection Equipment throughout the Lifecycle of a Nuclear Facility

Mahmood, R.[1], Kamal, S.[1]

[1] Pakistan Nuclear Regulatory Authority (PNRA), Pakistan

Corresponding Speaker: R. Mahmood

Sustainability of Physical Protection Equipment (PPE) throughout the lifecycle of a nuclear facility plays a pivotal role for ensuring physical protection regime. The sustainability process involves selection of appropriate equipment, procurement, installation, operation and repair & maintenance. The IAEA INFCIRC 225/Rev 5 duly recommends that "the State should establish a sustainability programme to ensure that its physical protection regime is sustained and effective in the long term by committing the necessary resources". The successful implementation of the physical protection regime depends on the operators, shippers and carriers, thus requiring them to establish sustainability programme by considering the following elements: • Equipment updating, maintenance, repair & calibration; • Performance testing & operational monitoring; • Configuration management of the PP Equipment and; • Resource allocation and operational cost analysis. A review study was conducted which reveals that the physical protection systems at a nuclear facility depends heavily on the choice of equipment and their installation to function either standalone or impeccable integration of various sensors from different locations. A good sustainability programme, hence, focuses on ensuring the operational and performance of the equipments to ensure that physical protection systems are available as required. The major constituents of such a sustainability regime of PPE are as following: • The first key task is to identify the need of PPE and its operational and performance objectives mapped to overall physical protection objectives; • Selection and installation of PPE is carried out through the rigorous project management process by following all stages from initiation to commissioning of PPE/systems and project closure. Overall objectives of PP are focused throughout the project phase. Standard operating procedures are identified during the project phase and implemented during the normal operation of PPE; • Formulation and implementation of repair and maintenance program and strategy including availability of resources for spare parts (Identification of resources and costs necessary to maintain the equipment, based on objectives and desired performance level) and repair work. This program covers both preventive and protective maintenance; • Comprehensive plan for operational and performance testing of the PPE/systems based on the industrial standards and acceptance criteria in line with regulatory requirements; • Performance of the PPE should be re-evaluated on periodic basis to ensure that all equipment/systems are working as their intended function. This paper will focus on the identification of important constituents for sustainable operation of Physical Protection Equipment (PPE)/systems and the role of NSSC for augmenting sustainability.

Synopsis ID: [204]

The United Kingdom's Experience in Developing and Delivering Physical Protection Workshops

Hobbs, C.[1], Salisbury, D.[2], Muti, A.[1]

[1] King's College London, United Kingdom

[2] CNS

Corresponding Speaker: C. Hobbs

This paper will outline the UK's experiences in developing and delivering a series of "Fundamentals of Physical Protection" workshops since the early 1990s, as part of the UK's Global Threat Reduction Programme (GTRP). Over the years, the workshop has brought together a wide range of international practitioners – from operators, regulators and government bodies to share their nuclear security experiences. The objectives and structure of the workshop will be outlined, followed by a short history of its implementation, before detailing a series of lessons learned.

The intensive six-day workshop provides a broad consideration of many aspects of physical protection. It has evolved to include topics outside of a traditional narrow physical protection course, such as security culture and nuclear regulation, with the goal of providing practitioners with a holistic understanding of nuclear security. It utilises subject matter experts drawn from academia, industry and government in its delivery in order to take both a conceptual and practical approach to physical protection, which is explored in different contexts. Practitioners are drawn from the UK's nuclear regulator, Office of Nuclear Regulation (ONR) and the Civil Nuclear Constabulary (CNC) which provides the armed response force at the UK's civil nuclear facilities. This was designed to enable UK best practices to be showcased drawing on practical examples. A key component of the workshop is a week-long table top exercise which integrates many key physical protection concepts: threat assessment, design basis threat, vulnerability assessment and red teaming, and physical protection upgrade planning. Participants also benefit from a day-long site visit to the Dungeness B Nuclear Power Plant where they are taken on a tour of the site and giving a series of briefings by nuclear security relevant personnel. This trip is designed to expose participants to the practical challenges and opportunities for applying physical protection principles to a working nuclear power plant.

The paper will argue that while the IAEA Nuclear Security Series of guidance documents provides a solid foundation upon which to base training and educational activities, their use must be carefully considered to ensure maximum impact. It will provide an overview of how both the contents and the teaching approaches of UK-led workshops have evolved in over 25 years of GTRP activity, and will focus on how current workshops use a range of modern teaching techniques to cement the security concepts contained within IAEA Guidance by showing how they translate into practice. Specifically the utility of

different educational and training tools for physical protection will be highlighted including the use of case studies, table top exercises involving hypothetical facilities, and site visits.

Synopsis ID: [265]

Practices of ISCN in Providing Effective Training Courses: Utilization of the Physical Protection Exercise Field

Matsuzawa, R.[1], Noro, N.[1], Nakamura, Y.[1]

[1] Integrated Support Center for Nuclear Nonproliferation and Nuclear Security (ISCN), Japan Atomic Energy Agency, Japan

Corresponding Speaker: R. Matsuzawa

Hands-on exercise is the one important method for effective human resource development in any field. This is also true in the capacity building support activities in the areas of nuclear security, or more specifically, physical protection of nuclear and other radioactive material and relevant facilities. Knowing the keen fact, the Integrated Support Center for Nuclear Nonproliferation and Nuclear Security (ISCN), the Center of Excellence (COE) or the nuclear security support center in Japan, has developed its Physical Protection Exercise Field as a training tool. This paper aims at sharing practices of ISCN to provide effective human resource development assistance, utilizing the Physical Protection Exercise Field (PP Exercise Field) in its training courses.

ISCN has put heavy focus in its nuclear security capacity building support activities on physical protection of nuclear material and facilities, since its establishment under the Japan Atomic Energy Agency (JAEA) in December 2010. Learning from US experience, the PP Exercise Field was designed and introduced to ISCN. In order to design, implement and further develop its Exercise Field, the Center has coordinated numbers of meetings with and visits to the US Department of Energy's National Nuclear Security Administration (DOE/NNSA) and Sandia National Laboratories (SNL), that have long experience of providing training courses in the field of physical protection of nuclear material and facilities. In the first part of this paper, the initial establishment of the Field will be briefly described.

The PP Exercise Field has been utilized by ISCN, while complementing the limitation of other teaching tools. For achieving effective learning by course participants, ISCN applies interactive lectures between participants, subgroup exercises, and more hands-on exercises using training tools such as the PP Exercise Field and other. Although interactive lectures and group exercises are useful to facilitate the understandings on principles and concepts, in-class activities on its own have insufficiency of not-being able to see and experience how actually the concepts and physical protection elements or equipment are implemented and performed at a facility. Equipped with major physical protection devices including intrusion detection sensors, contraband detection equipment, fences and barriers, entry control systems, cameras and a mock central alarm station, the Exercise Field enables the

training course participants to actually observe and test the physical protection elements. Also, another unique training tool of ISCN, the Virtual Reality (VR) System, allows participants virtually walk through a hypothetical nuclear power plant, learn how physical protection measures are implemented at a plant, and even re-design a physical protection system at a virtual facility. The two training tools complements each other; while the VR System virtually realizes what is difficult to demonstrate in the real world, PP Exercise Field provides more practical experience accomplished only by using actual physical protection elements.

Considering the characteristics of different teaching methods and training tools, ISCN has designed and implemented training course curricula and materials, in order to better meet the needs of the region and partner countries. Strategies on how to use the training tool is essential to achieve effective capacity building, according to the course goals, background of the course participants and the contents of the course materials. The capacity building of its own instructors is another key. Also, the PP Exercise Field has kept being improved with new technologies and equipment installed based on the feedbacks from stakeholders and course participants. In its 6-year experience of conducting total 83 courses in the area of nuclear security until April 2017, ISCN has followed the principle of needs-oriented and effective capacity building. This paper will share ISCN's practices on how it has utilized the Exercise Field in its training courses such as a regional training course on comprehensive process of designing and evaluating physical protection system and others on various topics on nuclear security.

The practices shared in this paper could benefit other countries to operate or newly establish its own training center. ISCN also has keen interests in further learning from practices of other COEs in the world. Based on its experiences and lessons from other COEs, the Center will continuously develop the Physical Protection Exercise Field and other training tools along with teaching skills to fully utilize the tools. Efforts, together with different COEs and initiatives, to mutually build up capacity as training centers should contribute to the world with enhanced nuclear security.

Synopsis ID: [267]

Training and Advanced Training of Nuclear Security Specialists in the Russian Federation

Kuskov, A.[1]

[1] Global Nuclear Security and Safety Institute, Russian Federation

Corresponding Speaker: A. Kuskov

Ensuring nuclear security at nuclear sites of the Russian Federation is one of the main strategic priorities and is considered as a prerequisite for the successful operation of the entire nuclear industry. The State Atomic Energy Corporation Rosatom on a regular basis strives for effective physical protection of nuclear materials and facilities as well as implements improvements in this area including that associated with personnel training. In order to improve the reliability of security systems, Rosatom uses the systems with top-class technical and organizational solutions as well as carries out their continuous improvement. Rosatom regularly evaluates the effectiveness and assesses vulnerability of security systems when exploring and testing the latest technological solutions. Annual audits, followed by the necessary corrective measures, further increase the overall nuclear security level at Russian nuclear industry sites. This year, in order to enhance expertise and proficiency of nuclear security personnel, Rosatom imitated activities on organization of training on all aspects of nuclear security at to-be-created Rosatom "Technical Academy". Such an approach will allow training in a more effective manner. In the near future, training of specialists from countries embarking on national nuclear power programs will start on the basis of the Rosatom "Technical Academy". Training will be conducted in all areas related to the creation and development of nuclear infrastructure of the newcomers. Training courses on nuclear security will be conducted at facilities of the Rosatom Institute for Global Nuclear Safety and Security, which is the IAEA center of the excellence in the field of nuclear security.

Synopsis ID: [231]

Human Capacity Building in Nuclear Security

Crawford, C.[1], Williams, A.[2]

[1] Oak Ridge National Laboratory, Department of Energy, United States of America

[2] Sandia National Laboratories, Department of Energy, United States of America

Corresponding Speaker: C. Crawford

The increasing prominence of the nuclear security discipline has resulted in an increased emphasis on capacity building in relevant skills and experiences in states with nuclear and radiologi- cal material responsibilities. Recent high-level events—like the International Atomic Energy Agency's (IAEA) 2016 International Conference on Nuclear Security, the entering into force of the Amendment to the Convention on the Physical Protection of Nuclear Material, and the Nuclear Security Summits—demonstrate the importance of developing and sustaining efforts to prepare the professionals (across a range of disciplines) to support all necessary nuclear and radiological material security-related requirements. Taken together, there is a clear need to develop the next generational of nuclear security professionals.

One recent response has been the emergence of educational programs in the Nuclear Security domain with universities across the globe offering varying levels of nuclear security curriculum. Noting this trend in nuclear security courses, in 2010 the IAEA established the International Nuclear Security Education Network (INSEN) for the purpose of enhancing global nuclear security by developing, sharing and promoting excellence in nuclear security education. To date, over 50 countries participate in this network, representing over 150 universities, institutes, agencies, etc. Further, INSEN has established suggested guidelines on nuclear security curricula, going so far as to lay out a recommended Master's Degree set of courses in Nuclear Security—recommendations that eventually resulted in the IAEA's Nuclear Security Series No. 12 (Educational Programme in Nuclear Security). The IAEA has, at the same time, expanded their nuclear security outreach by facilitating the establishment of Nuclear Security Support Centers (NSSC) , connecting research institutions in the nuclear industry to further their development of next generation nuclear security professionals. Other efforts in human capacity building for nuclear security include various internship programs across the nuclear domain which provide professional, academic and real-world experience in nuclear security.

Despite current levels of success in generating nuclear security professionals, what has not overtly occurred to date is an analysis of the need for nuclear security professionals within the nuclear domain, the requisite academic knowledge required to meet those needs and the types of coordinated programs necessary to provide this knowledge. There is currently no system for monitoring the

matriculation of students through the needed nuclear security curriculum, coordination of internships with academic requirements or the insertion of nuclear security graduates into the workforce—let alone through the early stages of their careers and professional development. While specific implementation will require country-specific discussions, the authors posit that a systematic approach to establishing a Human Capacity Building program in Nuclear Security is necessary to ensure operationally relevant capabilities are coming out of our academic institutions, supplying the next-generation professionals necessary to accomplish the intended global security needs in the 21st century.

Synopsis ID: [200]

Capacity Building for the Physical Protection Systems Strengthening of BATAN's Nuclear Facilities

Hasan, Y.[1], Purnomo, I.[1], Jumadiono, J.[1]

[1] National Nuclear Energy Agency of Indonesia (BATAN), Jakarta, Indonesia

Corresponding Speaker: Y. Hasan

To build the capability for the physical protection systems (PPS) strengthening of its nuclear material and nuclear facilities, National Nuclear Energy Agency of Indonesia (BATAN), in cooperation with the experts of Sandia National Laboratory and Pacific Northwest National Laboratory of the US Department of Energy, has conducted a series of workshops on performance testing and contingency plan in the period of 2014-2016. The activities consist of a gap analysis in 2014, performance testings 2015-2016, and contingency plan 2016, and involved some security, safety, and reactor operation personels and the police.

The workshop objectives on the gap analysis conducted in September 2014 are to understand the recommended physical protection requirements found in INFCIRC/225/Rev.5, conduct a gap analysis on elements of PPS against the security recommendations documented in INF-CIRC/225/Rev.5, and determine whether regulatory changes will recommend or require associated modifications of PPS at the BATAN's Serpong Nuclear Research Center. The workshop also provided an overview of the key physical protection concepts provided in this document, and explained the differences and rationale behind the changes from Rev.4 to Rev.5. The topics covered during the workshop included protection recommendations for materials in use, storage, and during transport; recommendations for protecting nuclear material against sabotage; use of a performance based approach for PPS; elements of a physical protection regime relative to State responsibilities; and license holder responsibilities.

After understanding the recommended requirements, the participants conducted a site gap analysis to evaluate existing regulations and PPS against the recommendations contained in INFCIRC/225/Rev.5, with the objective is to determine whether INFCIRC/225/Rev.5 recom-mendations will require associated modifications of PPS at the site. The participants were asked to determine what type of information needs to be gathered in order to conduct an assessment; to gather information from the respective sources; to assess the site perimeter, limited access area perimeter, entry control points, and protected areas; to use check-lists to determine compliance or gaps; and to develop a draft summary of the assessment results reflecting strengths and weaknesses found during the assessment.

The workshops on performance testing conducted in April, July, and August 2015, and April 2016 are designed to provide a practical understanding of performance testing of all three elements of a PPS: detection, delay and response. The goal of performance testing is to test people, procedures and equipment to determine if the various elements of a PPS are effective in defeating the threat. The workshops are designed as a follow-up to the gap analysis workshop conducted in September 2014. The goal of the workshop is for participants to understand the purpose and importance of performance testing and gain practical experience conducting different types of performance tests on the PPS in accordance with INFCIRC/225/Rev.5 recommendations. The performance testing exercises are directed at eventually informing the decision making process as the sites evaluate potential upgrades related to implementation of INFCIRC/225/Rev.5. The activities comprised of classroom training and field exercises. The field exercises helped the participants how to conduct performance testing of people, procedures and equipment related to access control and prohibited articles detection – searches/inspections; detection – step test specific sensors in the reactor facility and test camera coverage; response – conduct time motion studies in support of timely response determination; delay – evaluate delay at various security area boundaries The workshop on contingency plan conducted in September 2016 provided the participants with an introductory understanding of the recommended requirements for security contingency plans, the predefined set of actions for response to unauthorized acts indicative of attempted unauthorized removal or sabotage to a nuclear facility and is designed to counter such acts. GA Siwabessy reactor facility at Serpong Nuclear Research Center as the basis for this activity. The participants were personnel representing the guard force, police and other physical security, operations, and safety personnel that have the role in responding to a security incident at the site.

The purpose of the whole workshops is to provide the personnel with the knowledge and the ability to take performance testing of physical protection elements, which then to be able to evaluate and up-grade the PPS. Performance testing needs to be done periodically by the physical protection management in each nuclear facility to raise awareness for officers related to operational of PPS of nuclear material and nuclear facilities. Performance testing is also to convince BAPETEN (regulatory body) that BATAN as the operator has implemented best practices on the PPS as recommended by INFCIRC/225/Rev.5. With these activities, BATAN expects to ensure the people nearby the nuclear facilities that the security management has been carried out apropriately by applying the IAEA nuclear security recommendation and BAPETEN regulation.

Synopsis ID: [107]

Challenges in Establishing Effective Nuclear Security Culture

Kohli, A.[1]

[1] Department of Atomic Energy, India

Corresponding Speaker: A. Kohli

It is important to establish a strong physical protection system to ensure the security of facilities and nuclear materials in transport and to combat illicit trafficking and the inadvertent movement of radioactive material. But a strong physical protection system without appropriate human behaviour will not serve any purpose. Culture encompasses those traditions and habits which have worked in the past and people in that area tend to normally follow those. Culture also reflects the way people look at their environment and fellow beings in the society. An organisation with a strong culture will share the same core values and a high degree of commitment to those values. The way safety and security is valued by the staff and leadership, given priority and integrated into its way of working reflects the real commitment to safety and security. Weaknesses in safety or security culture are the main reasons for occurrences of the accidents which have happened. It is important for a society to ensure proper compliance of specified procedures and proper response to various events happening around them. Thus, having a sound safety and security culture is one of the fundamental requirement for an organisation dealing with nuclear materials. A strong nuclear security culture can result in a significant increase in the effectiveness of the security of radioactive material and associated facilities. However, following are some of the challenges faced in establishment and maintenance of an effective nuclear security culture particularly in the case of developing countries.

When the nuclear facilities and technologies are not home grown, and are imported there may be sometimes lesser appreciation of complexities and issues involved despite extensive training imparted to some of the staff as the lessons learnt are not from the home country and the situations prevalent may be different.

Strong nuclear security culture cannot be simply ensured when general security culture prevailing in that country itself is low. However, when general security culture in other strategic facilities is strong then it may not be out of place to establish and expect a strong nuclear security culture also.

Retaining and ensuring availability of manpower with adequate skills can become a challenge. On the other hand, organisations where the staff have long tenures in the same role and there are not much

opportunities for rotation of staff also can pose a different kind of challenge. Motivating such employees becomes difficult.

Security of nuclear materials which need to be transported over long distances and fall under different controlling authorities poses another challenge. The accompanying staff performing the duties may have to face different unfamiliar environments.

Since the number of security related events are necessarily far and few, some sort of lethargy is bound to set in. It becomes difficult to retain the message that nuclear threat is real and nuclear security is important. What is being attempted by authorities is to prevent sometimes a single specific security event with disastrous consequences. Learning lesson from actual happening of such an event can be very costly.

When the commercial viability of the facility is not on strong footing, it poses another major challenge. Maintaining security management system may become a financial load. It can result in reduction in staff strength. The message that security is responsibility of all including those involved in meeting production targets and not just security personnel sometimes may get lost.

When there are other security issues prevailing such as terrorist infested or areas with civil unrest, that can have effect on security culture. This may lead to some of the staff falling prey to bad elements increasing danger of insider threat. Poverty is another factor which may have a compounding effect. Such staff will be more vulnerable in getting in to traps set by malicious elements.

Synopsis ID: [147]

The Regulator's Tools to Support the Operator's Security Culture

Speicher, C.[1]

[1] Ministry of the Environment, Climate Protection and the Energy Sector, Baden-Württemberg, Germany

Corresponding Speaker: C. Speicher

This paper deals with various ways, tools and tricks how the regulator could effectively support the operator's efforts to foster a robust security culture within his organization. It is widely understood and frequently communicated that a well fostered security culture is crucial for any safe and secure operation of any part of critical infrastructure. These confessions are somehow honourable but rather useless without a concrete plan how to characterize the current state of such a sub-species of the overall organizational culture. Then, based on the results and findings of such a characterization, a tailored action plan to continuously improve this state should be implemented. Therefore, first of all both regulator and operator should provide and tailor tools to characterize the current state of the security culture and thus by appropriate means and quality assured procedures. One pitfall should be avoided from the beginning already: to blunder into the trap of prejudices and complacency. Whereas a self-assessment procedure is an internal tool for any organization and should not be influenced massively by external key players such as the regular, the latter one is in charge to keep an eye on the progress of the operator and how he performs with his self-assessment campaign. This means that the regulator can (and should) support the operator's campaign from the beginning, which usually means that he should define a proper starting point, i.e. give the initial impulse to decide to launch a self-assessment campaign. How such a campaign can be successfully planned, done in practice and improve the security culture state is described in detail in the draft of the IAEA technical guidance for NSC Self-Assessment (NST 026) which will be published and distributed soon. This draft however is already applicable as an "out-of-the-box" tool, it just has to be adapted to the respective national organizational needs. "Before the campaign is after the campaign" should be communicated by the regulator and therefore by the top management of the operator as well, as singular and isolated "light-house" projects are maybe a perfect starting point but if not followed by a continuous improvement process (PDCA circle) the sustainable success would be at risk. To summarize some generic proposals within this paper, some of the following tools of the regulator should be taken into account:

Giving the initial impulse to the operator to launch a self-assessment campaign,

Developing an appropriate and tailored self-assessment plan,

Evaluating the results and help to derive an action-plan,

Monitoring the progress of the action plan,

Appreciating the effectiveness of the action plan,

Specifying a subsequent self-assessment campaign,

Offering help to create tools to raise the awareness level of the staff,

Offering realistic examples (e.g. taken from the IAEA ITDB) why awareness and vigilance is crucial for an effective security culture,

Organizing regional or national workshops on NSC or applying for IAEA workshops on NSC,

Offering participation in national or international conferences and workshops which are focused on NSC.

It should be also addressed here that these proposals are not confined to the nuclear industry and respective applications but could be useful to minimize risks for any critical infrastructure,

e.g. by mitigating possible insider threats.

Synopsis ID: [109]

Physical Protection Regime-Universalization of the Convention on the Physical Protection of Nuclear Material and its 2005 Amendment

Udum, S.[1]

[1] Hacettepe University, Turkey

Corresponding Speaker: S. Udum

Global governance of the physical protection of nuclear material in use, storage and transport is evolving. Governance of an issue for cooperative problem-solving can be of several types. These arrangements and activities created by states and other actors are motivated toward resolving conflicts, serving common purposes and overcoming inefficiencies in decision-making. They include international law (treaties, conventions, UNSC resolutions), international organizations, international regimes and soft law (norms). International regimes focus on a specific issue on which actors have similar interests. They develop, maintain and strengthen rules, norms and decision-making procedures. What upholds a regime is its norm(s). They set a standard on the behavior of actors. Usually a dramatic event or strong leadership (with coercion or consent) initiates international cooperation, treaty, organization and paves the way for a regime. As members start benefitting from it, they work towards maintaining and strengthening it. The codes of behavior then define a community and a social identity for the members. In international arena, members of such community also benefit from compliance behavior and they "social awards", such as a rise in status and prestige. The pertinent example to this is the international nuclear nonproliferation regime, where the underlying context of the issue is traditional war, that is, actors are states per se. Nuclear security or physical protection of nuclear material in use, storage and transport involves malicious acts emanating from non-state actors. Thus, the context is asymmetric war. The pieces of the international regime on nuclear security are still developing. When the question becomes the universalization of the Convention on the Physical Protection of Nuclear Material and its 2005 Amendment, and the development of an understanding of the INFCIRC 225/Rev.5, one needs to look at the process, as the word "universalization" implies. It shows the expectation towards a growing number of states to endorse it. The process requires either strong leadership or an urgent/dramatic event. In this case, an event of "nuclear terrorism." The leadership came from the United States, under Obama administration in the form of Nuclear Security Summits. The pieces of the regime are the International Convention on the Suppression of Acts Against Nuclear Terrorism, CPPNM and 2005 Amendment, SUA Convention and 2005 Protocol, UNSCR 1540 and 1373, Global Initiative to Combat Nuclear Terrorism, IAEA, INSEN and WINS. What is missing for the development of the regime and the universalization of CPPNM is that of its norm. By definition, it takes some time. To shorten this time, states can engage in several activities: First, leadership is still necessary and more high-level conferences and meetings like the NSS,

would be productive and will signal continuing commitment to the nuclear security targets. Second, raising awareness is essential. The aim is to prevent that dramatic event, that is a terrorist attack with the use of nuclear or radiological material. Public awareness through media and education are powerful instruments. They have been in use, but they need to become widespread by effective communication techniques. The movie industry have produced several films and vice episodes. Education activities go on under WINS and the member states of INSEN. What is also essential, according to the INFCIRC 225/Rev.5 is cooperation between organizations, bureaucracies and individuals. That requires the development of the norm of nuclear security and nuclear security culture. These include terms that fall into the domain of Sociology, hence we need to work with social scientists. Security culture, according to the INFCIRC, means that a credible threat exists, that preserving nuclear security and the role of the individual thereof are important. Therefore, the state, organizations, managers in organizations and individuals should work together to establish and maintain an effective nuclear security culture. The mode of this cooperation depends on the bureaucratic culture of a state, that is, whether there is a top-down or bottom-up approach, the effectiveness and strength of bureaucracies, and security culture in general. As a result of in-depth research and analysis on these sociological processes, we can see the path for the development of a nuclear security culture in individual states. Personnel education and contingency planning are good starters to educate the public sector.

Synopsis ID: [277]

Building Robust Nuclear Security Culture in Nuclear Research Centres

Kutuvan, J.[1], Taly, Y.[1],Rajdeep, R.[1]

[1] Bhabha Atomic Research Centre, India

Corresponding Speaker: J. Kutuvan

Nuclear security threat is a major concern for all countries. The risks associated with nuclear security incidents could be disastrous: they may have a serious impact on human health and the environment; they also may have serious political and economical penalties. These threats could arise from the hands of an outsider or an insider of a nuclear facility. As the insiders often have good knowledge of the security measures and their weaknesses, the security measures, such as physical security systems alone, may not be sufficient to prevent malicious activity. Therefore, utmost care has to be taken in recruiting the manpower and necessary surveillance measures are to taken to minimise the insider threat. State of the art physical protection systems have to be installed to take care of the outsiders' threat.

Good security culture can protect the organisation from the insiders, as wells as that from outsiders. IAEA Nuclear Security Series No. 7 titled, "Nuclear Security Culture: Implementing Guide" defines Nuclear Security Culture as the assembly of characteristics, attitudes and behaviour of individuals, organisations and institutions, which serve as a means to support and enhance nuclear security. Security culture ensures that individuals remain vigilant and are aware of what is happening in their organisation. It introduces a questioning attitude among individuals, which may help to detect an insider threat.

Nuclear safety culture is an established concept in nuclear facilities. However, security culture is a recent concept. Both are intended to reduce the risk from nuclear materials and facilities. However, in some cases, they differ in their approaches and attitudes. Security culture focuses on deliberate acts intended to do harm, whereas safety culture focuses on the effects of human or mechanical error. Safety emphasises on transparency, where as security emphasises on confidentiality. Both cultures need to co-exist in nuclear facilities to meet safety and security requirements.

Unlike nuclear power plants or fuel cycle facilities, a nuclear research centre will have a variety of activities. The activity also may change with time. A research centre will have diverse categories of visitors, ranging from students, researchers and faculty members from universities to various users of radioisotopes, which could give a different threat perception to nuclear research centres. Good physical protection system, combined with a robust nuclear security culture, is necessary to address these threats. The authors' experiences in building a robust security culture are described in the article.

Synopsis ID: [298]

Potential Weaknesses in the Cyber Systems of High-Security Physical Protection Systems

Clem, J.[1]

[1] Sandia National Laboratories, Department of Energy, United States of America

Corresponding Speaker: J. Clem

The nuclear security community relies on physical protection systems (PPS) under the presumption they are isolated, operate as expected, and are not targets for adversary subversion. Key concerns identified by an expert committee reporting to the United States Congress include (cyber) "interactions and dependencies among security countermeasures," and "the adequacy of attack scenarios used to design, update, and test the security systems."[1] To address these concerns, the same committee recommended that the National Nuclear Security Administration adopt a total systems approach to "characterize the interactions and dependencies of security countermeasures. . . "[2] The committee also concluded that it is essential to understand the adversary, i.e., their objectives and perspectives on the security system itself.[3]

Indeed, given the incorporation of digital information technologies in a multitude of components and subsystems that make up modern PPS, and given the global availability of cyber attack tools (including custom exploit development), attack scenarios targeting theft or sabotage of nuclear assets now must consider cyber exploitation. But the PPS stakeholder community has been slow to address this need. In the authors' experience, a worrisome number of stakeholders presume their PPS and associated network(s) are isolated and not exposed or reachable by an adversary through cyber means. Yet attackers have compromised cyber-based components in similar systems, including those used to manage critical infrastructure and other important cyber systems that govern processes and hardware in the physical world.[4] Even once stakeholders acknowledge the general threat posed by cybersecurity vulnerabilities, they still do not know what credible cyber attack pathways might be available to an adversary (where vulnerabilities are discoverable, reachable, and exploitable). Unfortunately, current methods and tools used by the nuclear security community (e.g., physical security simulations) do not provide enough fidelity to validate the achievability of hypothesized cyber-enabled physical attacks available to adversaries.

Specifically, current methods fail to enumerate and demonstrate exploitability of technical cyber vulnerabilities in high-consequence PPS. Thus, decision makers lack sufficient understanding and demonstrable evidence of potential cyber threat impacts on PPS performance.

This paper describes the results of a multiyear R&D effort undertaken by researchers at Sandia National Labs who investigated potential weaknesses in the cyber systems of a representative high-

security PPS. It discusses the fundamental design of PPS, key measures of performance, and general cybersecurity threats to PPS. It follows with a description of three attacks including attack vector, defender assumptions around the system's security, relative difficulty, and consequences. [1] Committee on Risk-Based Approaches for Securing the DOE Nuclear Weapons Complex, National Research Council, Understanding and Managing Risk Security Systems for the DOE Nuclear Weapons Complex – Abbreviated Version, The National Academies Press, Washington DC (2011) [1]

[2] Ibid.

[3] Ibid.

[4] See, for example, the article titled "The Real Story of Stuxnet", Kushner, David, IEEE Spectrum, February 26, 2013.

Synopsis ID: [256]

Bridging the Gap between Cyber-Physical Protection System Attacks and Hazards: STPA-SafeSec-Attack Graph Approach

Findrik, M.[1], Friedberg, I.[1], Schmittner, C.[1], Smith, P.[1], Piatkowska, E.[1], Waedt, K.[2] , Kuskov, A.[2] , Spirito, C.[3]

[1] Austrian Institute of Technology

[2] AREVA

[3] Idaho National Laboratory, Department of Energy, United States of America

Corresponding Speaker: M. Findrik

A Physical Protection System (PPS) is used to protect nuclear materials within a nuclear power plant (NPP) from theft, robbery, illegal transfer, and to ensure secure access to different areas of a nuclear facility. Modern physical access control and surveillance systems rely increasingly on ICT technology, with the use of access card readers, RFIDs, biometric readers, and IP cameras used for perimeter monitoring to name only a few of the technologies. However, a PPS does not only protect nuclear materials; it also guards the digital assets in the plant from unauthorized access and tampering. Therefore, a PPS prevents potential cyber incidents that start with a physical intrusion. Access to a digital asset in a low-security environment (digital and physical) can ease access to higher-level security assets, potentially leading to theft of nuclear materials or disruptions to the normal operations of a NPP, depending on the attacker's goal. Therefore, a circular dependency exists between the need for physical protection, to prevent unauthorized access to the NPP, and its digital assets, and digital protection to ensure the intended operation of an ICT infrastructure that enables physical protection. Figure 1 shows an integrated approach for analysing the security of cyber-physical systems, by connecting the attack analysis steps together with impact analysis. In order to untangle these dependencies, and to understand the complex vulnerability landscape which enables multi-stage attacks, using digital and physical attack vectors, we propose a novel analysis approach that is based on the STPA-SafeSec methodology for effect (hazard) analysis, and attack graph technique [4] for attack analysis. The goal of the presented methodology is the identification of the most critical paths an attacker may take to cause hazardous events. The attack graph technique is used to cover not only Industrial Control Systems (ICS), but it also covers physical protection systems. It includes application of the Mean-Time-To-Compromise (MTTC) metric [3] as a measurement of difficulty for the attacker to preform individual step in the attack graph and move the system into a hazardous state. On the other hand, STPA-SafeSec [1] is a new methodology that

integrates safety analysis and security analysis into one concise framework. STPA-SafeSec allows elicitation of control actions that can trigger safety functions or cause hazardous events. In contrast to traditional hazard analysis techniques, it is not based on the classical fault-error-failure chain, but instead focuses on hazards that are caused through the incorrect or insecure interactions of different subsystems. The presented methodology is not limited to the identification of information flows that carry critical control messages and measurements through ICT networks. Instead, it enables the identification of attacks that leverage vulnerabilities in the PPS (either in the digital assets or more traditional flaws in the design) to gain physical access to the critical ICT infrastructure and subsequently cause hazardous operation of the NPP. In this work, we demonstrate our methods by applying them to a control loop of an open-pool reactor cooling system. Once the critical control actions in the control loops have been identified, hazard scenarios are derived that highlight how these control actions that could cause hazardous system states can be triggered. The potential attack vectors are described using the compromise graph, which shows how different cyber-physical domain attacks can cause safety events (e.g., an emergency shutdown due to over the limit coolant temperature). In particular, we explore cyber-attacks that exploit emerging vulnerabilities of digitalized PPS (e.g., by blocking alarms from smart fences or by freezing the video of IP cameras) to gain physical access to the operational ICT network. The presented methodology is designed to detect these complex attack paths and subsequently aid the design of more secure PPS and ultimately NPPs.

Synopsis ID: [275]

Enhancing Security of Physical Protection Systems through Software Behavioral Whitelisting

Khan, A.[1], Bhattacharjee, A.[1], Patil, P.[1]

[1] Bhabha Atomic Research Centre, India

Corresponding Speaker: A. Khan

Modern Physical Protection Systems (PPS) rely on complex sensor elements, software and configuration data for surveillance. Most of the systems employ COTS devices and software over a commodity hardware. The security issues with commodity computing systems and OS remain a vulnerable spot with large surface area for cyber-attack on PPS. However, it is seen that this factor is not given due importance as the focus remains on functional aspects of PPS. It is imperative that computer based systems used for physical protection, nuclear safety, and nuclear material accountancy and control should be protected against compromise (e.g. cyber attack, manipulation or falsification) consistent with the threat assessment or design basis threat. In fact, the IAEA guide on Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/REVISION 5) recommends configuration management of a facility's physical protection system, including computer systems and software. It demands ensuring that changes to these characteristics are properly developed, assessed, approved, issued, implemented, verified, recorded and incorporated into the facility documentation. It is required that computer based systems used for physical protection, nuclear safety, and nuclear material accountancy and control should be protected against compromise against cyber-attack consistent with the threat assessment or design basis threat. Most of the software components use the services of the underlying OS and vulnerabilities of information flow from secure to non-secure components can be induced by a malware infected component and thereby breaching the confidentiality and privacy requirements of PPS. This may happen due to large number of system calls exposed to user-space; which remains a problem as it expands the kernel attack surface. Recent designs in Linux OS kernel provides system call filtering, Namespace based containment approach and controlling capability for all privileged operation. This paper presents the technique of application behavior whitelisting by using application specific profiles, Linux namespaces and capability learning and it's implementation. The application behavior whitelisting has two modes – a) Learning Mode and b) Enforcing Mode. In Learning Mode, user generates the behavior profiles by running the desired application. In Enforcing Mode user, can enforce the profiles on the applications. If application behavior gets modified at runtime due to a malware infestation, it is captured and reported in audit log. As a part of user defined behavior policies, it supports Linux Namespace based resource limiting, network bandwidth control, system call filtering, capability based least privilege execution of application, file system controls – like whitelisting or

blacklisting or creation of application specific private directories and many more. The implemented system is tested in the laboratory.

Synopsis ID: [233]

Authenticated Sensor Interface Device for Securing Sensors and Data Transmission

Poland, R.[1], Deroller, N.[1]

[1] Savannah River National Laboratory, Department of Energy, United States of America

Corresponding Speaker: R. Poland

The paper will discuss the features of Savannah River National Laboratory's (SRNL) Authenticated Sensor Interface Device (ASID) which provide the ability to authenticate data from critical sensors and other data streams, share that data among a number of parties, and protect the sensor and each party's network from outside cyber attack or cyber attack from other parties receiving the data. In addition, the paper will discuss the development of the prototype to date as well as the future plans for the ASID. As industrial sensor data is increasingly transmitted over networks which are ultimately connected to the internet the likelihood that this data, critical to the protection and operation of nuclear and other facilities, will suffer a successful cyber attack has greatly increased. The risk of unreliable data, either through manipulation or denial of service, being relied upon for physical security systems poses a tremendous security risk. Additionally, unreliable data due to a cyber attack on industrial control systems poses unacceptable safety and operational risks. The risk of unreliable sensor data must be mitigated to ensure the safety, security, and reliability of nuclear and other critical infrastructure facilities throughout the world. The ASID, fully implemented, can be a key component in the protection of critical infrastructure from malicious cyber attacks. The ASID's modular concept allows for interfacing to numerous sensor types including digital protocols as well as analog sensors with voltage, milliamp, and temperature outputs. The sensor signal is authenticated and encrypted by the primary embedded controller, then communicated to each party's transmission module where additional private encryption may be applied to the data stream. An integral and key feature of the ASID is the data diode functions that ensure no communication flows backward to the sensor interface module which ensures that both the sensor and every network is protected from cyber attack.

Synopsis ID: [284]

Cybersecurity & Physical Protection: How Cyber Attacks Can Influence the Reliability and Integrity of Facility PPS & Communications

Nickerson, C.[1], Fabro, M.[2]

[1] Idaho National Laboratory, Department of Energy, United States of America

[2] Lofty Perch

Corresponding Speaker: M. Fabro

Nuclear and radiological facilities are digitizing elements of security and operational systems in order to improve performance, effectiveness and efficiency while reducing cost of ownership. These digital elements have greatly increased the interconnectivity between traditionally disparate systems such as components in physical protection systems (PPS). The migration to digital technology, along with the increased interconnectivity, has introduced new vulnerabilities. These vulnerabilities, traditionally unobserved in PPS, present a new landscape of opportunity for threat actors having cyberattacks in their portfolio of capability. Improving the cybersecurity of these interconnected systems is a challenge that nuclear and radiological facilities are now assessing. Regulators and operators are seeking to reduce the risks and impacts of a cyberattack by analyzing where their systems can be compromised.

The purpose of this paper is to identify network architectures and communication protocols commonly used at nuclear and radiological facilities and to analyze their vulnerabilities and how they could become compromised. The research, on that involves consequence-driven use cases, demonstrates how these vulnerabilities could be exploited to facilitate unauthorized access to information and/or nuclear material (NM). The goal of this paper is to empower regulators and operators with a working example of an evaluation process that can lead to an accurate understanding of their digital system attack surface and a realistic view of their risk profile.

A key element of this research is based upon the observation that a cyber-enabled adversary seeks to:

Leverage misconfigurations in network architecture and devices; Exploit errors in coding; and Manipulate how devices communicate in order to gain unauthorized access to a system. Once inside, the adversary pivots within the network or compromises additional devices in order to achieve their ultimate goals.

The paper evaluates common practices in network and protocol procedures of physical protection systems utilizing this threat profile. For example, physical protection systems tend to have flat

networks. However, flat networks do not usually have robust 'defense in depth' capabilities and enable free lateral movements by a cyber threat.

The paper evaluates pros and cons to these typical examples and provides suggestions on how to implement security countermeasure and best practices to enhance the PPS architecture and reduce risk. The paper also uses a working example to examine the impacts of a cyberattack during a traditional theft scenario and measures system performance of the PPS as a function of time.

Synopsis ID: [82]

The U.S. Department of Energy's Use of Protective Force Standards to Ensure a Timely and Effective Response to Security Threats

Curry, G.[1], Brooks, M.[1], Faiver, R.[1]

[1] U.S. Department of Energy, United States of America

Corresponding Speaker: G. Curry

Abstract. Annex I to the CPPNM states that Category I material should be stored in a protected area that is under surveillance by guards who are in close communication with appropriate response forces with specific measures to be employed with the objective for the detection and prevention of any assault, unauthorized access or unauthorized removal of material. The U.S. Department of Energy (DOE) utilizes Protective Forces (PF) to provide the physical protection of interests under DOE's purview ranging from facilities, buildings, Government property, and employees to national security interests such as classified information, special nuclear material (SNM), and nuclear weapons. DOE utilizes a graded approach for the protection of the lowest level of government property, with increasing layers of security, to the most critical assets. DOE requires the establishment and maintenance of a PF program, as an integral element of its defense-in-depth strategy, to detect and prevent malevolent acts against DOE security interests. The PF program includes the development of written plans, post orders, general orders, and procedures covering PF routine, emergency and administrative duties; tactical deployment, and other operational requirements to allow maximum concentration of resources in a tactical posture. Consistent with NSS-13, which requires physical protection be comprised of a designed mixture of hardware (security devices), procedures (including the organization of guards and the performance of their duties) and facility design (including layout), the DOE PF is a critical element to provide assurances for safeguarding against loss, theft, diversion, unauthorized access, misuse, or sabotage of nuclear material that could adversely affect national security and the health and safety of employees, the public, and the environment in accordance with the DOE Design Basis Threat policy.

The DOE PF must be knowledgeable and skilled in site and/or mission-specific protection strategies; tactical response options, actions, and times; and other applicable response requirements as delineated in site security and contingency response plans. DOE prescribes PF medical, physical readiness, firearms and training standards as a means of ensuring the requisite level of demonstrated knowledge, skills and abilities (KSAs). DOE PF with access to nuclear weapons, nuclear test devices, complete nuclear assemblies, Category I and II quantities of SNM; or with access to credible roll-up to Category I or II must obtain and maintain the most stringent trustworthyand reliability, as well as

training and qualification standards based upon Job Analysis/Mission Essential Task List (JA/METL).

Accordingly, the DOE PF training and qualification program is based on a valid and complete set of JA/METL, with identified levels of skills and knowledge needed to perform the essential functions prescribed in applicable security policy. KSAs necessary to competently perform the tasks associated with assigned PF duties must be identified based upon the JA/METL applicable for each job assignment. PF personnel must demonstrate familiarity with, and knowledge of, the responsibilities identified in the JA/METL for their assignment and must demonstrate proficiency in the skills and abilities necessary to perform required and assigned job tasks.

Synopsis ID: [177]

How FOF Exercise Helped Us Building Joint Training Programme

Perc, R.[1]

[1] Ministry of Interior, Police, Slovenia

Corresponding Speaker: R. Perc

How FOF Exercise Helped us Building Joint Training Programme (graded approach gives results, increase cooperation and efficiency)

Nuclear power plant (NPP) Krško is located in the south part of Slovenia, near the town of Krško. From 1977 onwards, the cooperation and coordination between NPP and Police Directorate Krsko (regional police directorate, in charge of organisation of off-site response forces) has been on a high professional level.

In 2011 reorganization of Police in Slovenia occurred and some units within the police on regional level, previously linked to NPP security on 24/7 basis, were moved to new Police Directorate HQ in Novo mesto (36 km away from NPP – as the previous was 3 km away). All stakeholder involved in the site security and off-site response forces (which is the police) were facing with a need to review documents and procedures to adopt adequately to new situation. Furthermore, an idea to test the response organisation with exercises was introduced – force on force exercise (hereinafter FOF) was the best option and stakeholder decided to use graded approach instead of launching a full scale FOF for the first time. Unannounced FOF was launched by night in 2014 with a simulated attack to the perimeter and planned one with larger police unit intervention within the perimeter in 2015.

State competent authorities' officials were present at the events as observers. Follow up activities included interviews, analyses of communication, coordination, cooperation, analyses of recorded video and voice communications, observations, recommendations and proposals from official observers etc. Results were presented in the following months to authorised personnel on local, regional and state level. Seven different areas with fourteen proposals were identified for improvements and upgrades. Overall experience gave some surprising information, which was used in following months to improve overall security regime on many different levels.

Among others, a need has emerged to build a joint training programme for security guards (on-site) and police (off-site) with some safety topics but mainly with security topics, to introduce each other's equipment, procedures and basic tactics with objective to understand what to expect when facing real threat situation and provide better coordination among on-site and off-site forces. One of the most interesting topic to be covered was familiarisation with the area, especially perimeter, entry

procedures etc. that has not been in a prime focus of the off-site forces before (but has been identified as possible seatback after FOF analyses). The training programme development is continuous operation of many entities: the NPP, the police at local, regional and state level, the Nuclear Safety Administration, the Ministry of Interior, the Civil Protection and Disaster Relief Administration etc.

The scope of the programme is to prepare simple, robust, not to extensive, flexible but comprehensive training to allow as many participants as possible to go through the programme to increase overall cooperation, coordination and communication (CCC) among response forces (on-site and off-site). The experience was lesson learned how to increase efficiency – thanks to the valuable feedback of the FOF, which has been a "wakeup call on-time".

Synopsis ID: [213]

Outcomes-Based Training and Education for Protective Forces

Parker, J.[1]

[1] National Nuclear Security Administration, Department of Energy, United States of America

Corresponding Speaker: J. Parker

Outcomes Based Training & Education (OBT&E) is an established, principle-based approach to planning and executing outcomes-based performance that deliberately promotes the development of individual initiative, collective agility, and, most importantly, enhanced leader confidence through the development of mission-specific skills and professional competence. Since 2007, in order to more effectively counter 21st-century dynamic threat conditions, military organizations have purposefully implemented this training methodology to significantly enhance unit mission training and institutional leader development programs.

OBT&E should not be confused with institutional course design (instructional). OBT&E is focused on recurring, mission-focused performance training at the site (unit) level. While formal instruction provides a framework for instructors to impart new knowledge and understanding in their trainees, training is the approach by which qualified professionals improve through deliberate practice, based on individual and team assessments.

Tactical effectiveness is a product of 1) an individual and/or unit's ability to understand the components of any given system (e.g., weapon system, personal equipment, vehicles, tactics & techniques, etc.), and 2) the ability to utilize/adapt/apply the skills necessary to quickly resolve a tactical situation. This basic "equation" served as a foundation for constructing the sequence and combination of activities that were executed during the workshop, successfully demonstrating to the student participants a logical approach for designing and executing training that inherently allows for the progressive assessment and development of subordinate. General concepts for leaders and instructors are to:

Maximize understanding of equipment/tools and their capabilities Develop mastery in mission essential skills Build trust and confidence within the team Earn trust and confidence of the organization Reward accountability, initiative, and expertise

Threshold training is a concept by which leaders design training activities that allow movement of performance from rote replication to judgment-based application within the same training period. Productive learning and development happens just at the threshold of failure, with discomfort but not discouragement. Keeping all individuals collectively, regardless of experience and skill, too far to the left of the threshold with rote or administrative compliance is boring and participants do only the minimum needed to do to pass the test. Pushing participants too far, too soon to the right of the

spectrum for their experience and expertise level is chaotic and discouraging. Properly designed learning activities, especially in the field or on ranges, permit cadre to adjust conditions for individual learner needs without requiring the entire group to work at the pace of the slowest learners, and without overwhelming participants.

Where an individual or team is performing on the scale, determines whether the threshold of failure generally moves to the right on both scales, remains stagnant or moves backward. Continually assessing student performance and confidence provides instructors with the information needed to determine the appropriate time to move to the next activity. This approach is far more effective than rigidly following a pre-defined schedule of events.

Synopsis ID: [102]

An Industry-Led Governance Framework for Demonstrating Strong Security

Umayam, M.[1], Rauhut, K.[1], Howsley, R.[2] , Barrett, J.[3]

[1] Stimson Center, United States of America

[2] World Institute for Nuclear Security (WINS)

[3] Canadian Nuclear Association, Canada

Corresponding Speaker: M. Umayam

With the entry into force of the Convention on the Physical Protection of Nuclear Material and Nuclear Facilities (CPP), the international community has successfully extended the legal bedrock for physical security to civilian nuclear facilities. The newly added Fundamental Principles not only include concrete, measurable actions like establishing national legislation and a competent regulatory authority, but also cover concepts that are scalable depending on the State's resources. For instance, the Fundamental Principles call for States to ensure that all organizations involved in physical security give "due priority" to a strong and enduring security culture. Although the responsibility to implement and sustain the physical protection regime remains under national authority, the Fundamental Principles also recognize the role of the licensee (e.g., operators or shippers) who ultimately is responsible for implementing physical protection.

While it is a laudable milestone to invoke such concepts as security culture in a legally binding instrument, it raises questions about its effective implementation: how would industry operationalize and demonstrate to the State that this has been achieved based on "reasonable and practicable" terms? Is it possible to agree to an industry-wide metric for security culture and other elements under the Fundamental Principles such that a level of uniformity can be achieved in the way these elements are addressed across all organizations, while still allowing for operational flexibility?

This paper presents a case for the development of a nuclear security governance template that could serve as a framework for demonstrating compliance with some of the CPP Fundamental Principles. The paper argues that good corporate governance supports key elements of physical protection including security culture. It also emphasizes that good corporate governance cannot be externally imposed by a State. Rather, it must be internalized and prioritized within an organization as an essential element of operations. Thus, an industry-developed template for good governance would help executive-level managers continually evaluate and prioritize physical protection in their nuclear facilities by way of institutionalizing board-level assessments of company security policies including:

clearly defining managerial accountability for nuclear security; establishing meaningful performance metrics for security procedures including emergency management; measuring worker perceptions of culture; and other criteria for demonstrating quality management.

The paper will cover some of the key elements that should be incorporated in the proposed governance template. Specifically, it posits that the template should incorporate not only existing guidelines and resources, but also include industry input to account for the on-the-ground realities executive leaders face when running a facility and maintaining a business. Nuclear industry operators serve as the front line to nuclear security and would inevitably be responsible for establishing and demonstrating the Fundamental Principles. Engaging industry, potentially through the Nuclear Industry Steering Group for Nuclear Security, to develop such a template would allow industry stakeholders to weigh in on what is reasonable and practicable given their unique risk situations.

Voluntary adoption of this template by industry leaders could be used to demonstrate to their respective national regulatory authorities – and in turn the larger international community – that they have given "due priority" to the elements under the CPP Fundamental Principles in order to help sustain their State's physical protection regime.

This paper builds on the Stimson-WINS paper presented at the IAEA 2016 Nuclear Security Conference in Vienna, "Industry's Potential Role in Implementing the CPPNM Amendment and Improving Nuclear Security". Please see: https://www.stimson.org/content/industry%E2%80%99s-potential-role-implementing-cppnm-amendment-and-improving-nuclear-security.

Synopsis ID: [58]

Physical Systems and Regulatory Oversight for the Protection and Operation of the Nigeria Research Reactor-1

Ewa, I.[1]

[1] Amadu Bello University Teaching; Centre for Energy Research and Training, Nigeria

Corresponding Speaker: I. Ewa

The Nigeria Research Reactor-1 operated by the Centre for Energy Research and Training, Ahmadu Bello Univetsity Zaria under the authorization of the Nigeria Atomic Energy Commission is a 31 kW tank-pool type with 90% enriched uranium (UAl4)fuel. The length of the fuel element clad in the aluminium alloy is 248 mm. A total of 347 of these fuel elements make up the highly enriched uranium core of the reactor. Application of a defence-in-depth concept against unauthorized removal ensures that the core within the reactor is well shielded under a de-ionized pool water contained in a re-enforced concrete stainless-steel-lined tank of diameter 2.7 m and 6.5 m deep. NIRR-1 became citical on the 3rd of February 2004 with a thermal neutron flux of 10 x 10E12 cm E-2s E-1 at full power. An assuring indicator of the existence of the core in place is always guaranteed by the emission of Cerenkov radiation under the pool water during operation. The reactor has been exploited over a decade for the socio-economic development of Nigeria in the areas of training and capacity building on physical protection and management of nuclear materials. A Final Safety Analysis Report initially referenced CERT/NIRR-1 having undergone several reviews, documents special protection strategies for the facility and its ancillary nuclear materials. A consolidated and well secured Waste Management Facility acts as a secured repository for spent and irradiated nuclear materials. The regulatory oversight of the facility is under the strict supervision of the Nigeria Nuclear Regulatory Authority (NNRA). The NNRA ensures that the facility operates within its operational limit and conditions, authorized licensing regime and that its ancillary materials are adequately accounted for through enhanced physical protection measures. Safeguards and physical protection infrastructural systems installed are constantly reviewed by the reactor safety committee thus ensuring the safety of both the facility and its associated nuclear materials. The reactor is installed in a protected area within an enclosed zone with limited access. The whole area is constantly patrolled as outlined in the Security Plan. The Security Plan assures a 24/7 surveillance on the facility by well trained guard-force on nuclear security culture, assisted by an armed Nigeria Police Force network. A central alarm system activates itself each time there is an intrusion either by an unauthorised opening of the reactor hall door or external incursions to specific exclusion zones. Complementing these efforts is a robust play-back Close Circuit Television (CCTV) monitoring and computer logging program. The CCTV output is a daily recording and documentation of events within and around the inner perimeter walls of the facility including more importantly all activities surrounding and overlooking the core in the

reactor hall. A graded approach towards the physical protection of both the facility and nuclear materials is applied where and when necessary by both the guards and the armed personnel protecting the facility during daily surveillance. Well established Emergency Response Programs (ERP) provide adequate measures to counter sabotage and terrorists attacks. Implemented human reliability programs assure internal in-house vetting, trustworthiness and information management on facts and data relevant to ERP solutions of vital importance. A two-person rule is usually adopted for on-the-spot assessment of the accuracy of records during nuclear material auditing and balancing. This assures the Reactor Safety Committee (RSC) which is an independent body from the operation team of the validity of the records provided by the operators during inspections. The facility's outer physical protection regime is consolidated with a three-series perimeter fencing wall with access control monitoring achieved through staff/visitor screening at the three admission gates whenever one passes each consecutive gate. Routine physical protection drills enable on-site and off-site guard responders to be alert on their protection responsibilities against any malicious act perceived to arise either from an insider or outsider threat. In conclusion, it should be noted that issues of security and safety of the facility and nuclear materials as recommended in INFCIRC/225/Revision 5 are always on the front burner of the RSC and has been the strength supporting the successful operation of the NIRR-1 research reactor for thirteen years without any loss of nuclear materials nor the facility being subjected to neither sabotage nor malicious attacks.

Synopsis ID: [21]

Performance Testing Nuclear Security

Rosano, R.[1]

[1] EXCEL Services, United States of America

Corresponding Speaker: R. Rosano

The expectations for nuclear security programs are spelled out in State regulations, or outlined in the objectives statement of the utility. The means of achieving these expectations are described in volumes of guidance published by the State, industry groups, or the utility itself, often calling upon a broad library of extant literature from other sectors and sources.

For the most part, these expectations, regulations, and guidance documents describe the systems, equipment, training, and staffing required to fulfill the basic goals for security at a nuclear facility– to achieve compliance with the specific details of the requirements.

Compliance inspectors can use checklists and procedures to focus on whether the security organization installed the appropriate equipment, conducted the appropriate training, and satisfied the promise of the requirements. But the ability of the program to survive the stress of an actual attack is a more difficult matter to judge.

This paper will address performance testing of the security program, a complex and integrated response element that includes equipment and systems, the ability of these systems to support the response team, and the security organization itself to perform the right tasks, at the right time, and with sufficient force to counter an adversary attack.

Preparation

When the performance test begins, events will transpire in quick succession, so failure to prepare for observing and recording the events will make evaluation of the results impossible. It is assumed that the security organization is already trained in their assigned duties, but the observers, exercise controllers, managers who will be expected to analyze the data must also be trained; even visitors and dignitaries whose presence could impact the conduct of the exercise must understand their roles.

Safety training is also critical in this process to avoid injuries or equipment damage during the exercise. The facility's actual security measures must remain in place throughout the exercise –while a shadow force participates in it – so special steps must also be taken to reduce the potential for confusion between the "real" force and the "shadow" force, and to ensure that all observers and visitors are aware of the duplicate forces.

Places to conduct effective observation, forms that are designed to simplify the capture of results while action proceeds, and effective communication between participants and observers for clock management and unanticipated stoppages must all be considered prior to the initiation of the exercise.

Clock Management

Real events proceed without stoppages, and experience has shown that many adversary attack scenarios may complete their action in under ten minutes. However, "exercise time" moves more slowly, includes anticipated and unanticipated stoppages, and must be recorded as if the clock continued to move, otherwise the data evaluation will not reflect real events.

Real-time Recording of Events

Increments of time should be established that are manageable within the structure of the exercise. As the mock adversary attacks the site and the "shadow" force protects it, observers and controllers assigned to each team must be able to track movement and time in an integrated manner. This requires communication between the teams to ensure that the clocks are moving in sync.

Artificialities

Most actual attacks involve the destruction of equipment, which should be avoided during exercises. However, preservation of the equipment – for example, physical barriers – requires that the mock adversary penetrate go around the barrier, taking more time than the true adversary would require. Similarly, the use of small or large explosives, smoke bombs, radio frequency jamming equipment, and the like would not be allowed during an exercise. To ensure the validity of the data, all potential artificialities should be anticipated prior to initiation of the exercise and recorded to minimize the impact on the data.

Evaluating the Results

Based on planning, training, and preparation for clock management and artificialities, the forms completed by the observers and controllers, along with narrative input from participants, program managers, and even visitors should be collected as soon as possible after the exercise. It is critical to debrief the results while immediate recall can still contribute the sometimes-obscure details witnessed during the exercise.

Summary

Compliance with governing expectations and relevant guidance can establish a security program, but only a well-planned performance testing process can prove that the security program can defend the facility.

Synopsis ID: [252]

Preparation for the Implementation of the Convention on Physical Protection of Nuclear Material and Its Amendment in Senegal

Faye, N.[1], Tall, M.[1]

[1] Autorite Senegalaise de Raioprotection et de Surete Nucleaire, Senegal

Corresponding Speaker: N. Faye

Even though Senegal is not a nuclear country for the time being, it has pledged to support the efforts of the international community for the peaceful use of nuclear energy, to enhance the level of safety and security in the conduct of all activities involving the use of nuclear material or other radioactive sources and to combat proliferation. By ratifying the CPPNM in 2003, Senegal undertakes to ensure that the implementation of the Physical Protection, while respecting its responsibility, is based on the recommendations of the INFCIRC / 225 of the International Atomic Energy Agency (IAEA). Following its commitment to strengthening the international nuclear security regime, Senegal adopted the law 2017-21 of 5 April 2017 authorizing the President of the Republic to ratify the Amendment to the CPPNM. The aim of this article is to show how Senegal is preparing for the implementation of this legally binding instrument considered as an important tool to strengthen and complement the multilateral nuclear non-proliferation regime.

In addition, it will be a good experience as Senegal intended to get research reactors soon. The inspections carried out by the Senegalese Radiation Protection and Nuclear Safety Authority (ARSN) since its establishment in 2011 have shown the existence of radioactive sources of all categories and of small quantities of nuclear material originating either from shielding of certain sources or abandoned at sites. It was therefore imperative to make the necessary arrangements for the physical protection of these materials and for securing the sources of high categories. So, considering the Fundamental Principle A, which gives primary responsibility to the State for the development, implementation, and maintenance of a system of physical protection on the territory, Senegal has undertaken to reform its legal framework to meet its obligations. The paper will show the legal and regulatory measures taken in the new comprehensive nuclear law we have elaborated, to meet the three objectives of the Convention to establish and maintain effective physical protection of nuclear materials, to preventing and combating offenses against such materials and facilities and to facilitate cooperation among States Parties. So, the rules related to the twelve fundamental principles of physical protection have been introduced in this law and will be reflected in the implementing regulations to: guard against any unauthorized removal of materials, including during transport; to implement rapid measures to locate and recover missing nuclear material or stolen; to guard against possible sabotage of nuclear installations; and to mitigate or minimize the radiological consequences of sabotage. The paper will

point out mainly the new offenses incriminated in our domestic laws (new nuclear law and the revised Penal Code) regarding use or transfer of nuclear material without authorization required, transport, shipment or movement of nuclear material to or from a State without proper authorization, offenses related to terrorist bombings, nuclear or radioactive materials and nuclear installations, threats of harm to persons by the use of nuclear material in the event of a death threat, threats to commit an act directed against a nuclear installation, etc. Finally, the initiatives taken for coordinated and effective national and regional efforts, those with the assistance of the IAEA and in bilateral cooperation (with the United States of the America, the European Union and Mauritania) will be also highlighted in particular about the implementation of the national INSSP plan to ensure the effective security of nuclear material and radioactive sources and human resources development. References: Law No. 2004-17 of 15 June 2004 on the Protection against Ionizing Radiation Law No 2009-14 on nuclear Security and Radiation protection Decree No. 2010-893 of 30 June 2010 on the organization and functioning of the Radiation Protection and Nuclear Safety Law 2017-21 of 5 April 2017 authorizing the President of the Republic to ratify the Amendment to the CPPNM. Law amending the law No 65-60 of 21 July 1965 on the Penal Code Protocols with Customs, Gendarmery, Forces Army Protocol with Mauritania

Synopsis ID: [269]

Practical Experiences of Combined Nuclear Security and Safety Culture Self-Assessments in NPPs

Solymosi, M.[1], Horvath, K.[2]

[1] National University of Public Service, Hungary

[2] International Atomic Energy Agency

Corresponding Speaker: M. Solymosi

Although the scope of use of atomic energy is different all over the world, but the enhancement of the safety and security of applications is a global requirement.

Nuclear safety and security are sharing the same objective, to protect people, society and environment from the harmful consequences of a nuclear and/or radiological event. While some safety issues have no security implications and vice-versa, in most cases they are not mutually exclusive and have to be managed in an integrated manner. (IAEA 2016)

Probably the most relevant risk to the safe and secure operation of an Organization is the human component; namely, their own staff. Thus, in addition to continuous development of technical solutions can protect us so far the culture for safety and security become a major point. The common goal of the concept of nuclear safety and security culture is to reduce these risks. On the other hand, international guidances are divided about the process and concept and the national regulations are not uniformalized about the combination of the assessment of nuclear safety and security culture.

Nuclear safety and the culture for nuclear safety is essentially accepted for decades. Safety culture is regularly assessed by nuclear operators itself and by many domestic and international organizations like the International Atomic Energy Agency (IAEA) Operational Safety Review Team (OSART), Assessment of Safety Culture in Organizations Team (ASCOT), World Association of Nuclear Operators (WANO).

The necessity of security and security culture was emphasized on each Nuclear Security Summit. While the first summit in 2010 Washington focused on fissile materials, the second in 2012 Seoul and the third in 2014 Hague made it explicit, that (from security approach) radioactive sources should have a status equal to other items at the top of the nuclear security agenda. (Khripunov 2014)

The paper analyzes the possibility to combine safety and security culture assessments, assessing, among other things, the integrity of management, regulations and the control of sensitive information.

The authors summarize the basic knowledge about the combined content and also presents the advantages and disadvantages of the combination of the assessment of nuclear safety and security culture. Based on personal experience during the combined nuclear safety and security culture self-

assessment in Paks NPP at 2015, and Bruce Power NPP in Canada at 2016 the author present a good practice how the facilities can apply a toolset and assess and enhance their own (culture for) safety and security, including the component of nuclear safety and security culture, the theoretical background of safety and security and the culture of them, the considerations which must be taken into account regarding the combination of culture assessments of nuclear facilities; the methods of the self-assessment, a recommendation about the self-assessment and enhancement process Finally, the paper will conclude that the assessment is not just a single effort to fulfill the requirements of the regulations or international recommendations; it is a continuous process, where the line between the process of the assessment and the enhancement is very precarious.

Synopsis ID: [246]

A System-Theoretic Approach to Overcoming Cultural & Organizational Barriers to Nuclear

Williams, A.[1]

[1] Sandia National Laboratories, Department of Energy, United States of America

Corresponding Speaker: A. Williams

If the same physical protection system (PPS) is applied to identical nuclear facilities in two different countries, traditional nuclear security analysis techniques conclude that PPS effectiveness is the same—despite the highly probable different in experienced security performance. In fact, a 2010 National Academy of Science report entitled 'Understanding and Managing Risk in Security Systems for the DOE Nuclear Weapons Complex'—which reviewed common security analysis techniques—concluded that most current risk-based 'methodologies cannot address cultural or organizational barriers to improved security.' Though recent (and widespread) efforts to raise the profile of nuclear security culture have generated a useful framework for addressing some of these barriers, current nuclear security analysis techniques struggle to include these insights—described by one expert in a 2014 review of the International Atomic Energy Agency's nuclear security culture framework as 'not yet [having] introduced guidelines on assessing the human factor in detection, delay and response'. This suggests a need to move away from the dualistic framework where physical protection system performance nuclear security culture are disparately analyzed and toward a new paradigm that incorporates both social and technological influences on security for nuclear facilities. Borrowing from advances in system and engineered safety in the nuclear, aerospace, automotive and medical industries, a recent study has developed a complex, socio-technical system model and system-theoretic approach for analyzing nuclear security. In this approach, defining nuclear facilities as systems composed of interrelated social and technological components that maintain dynamic equilibrium through information and control feedback loops provides a rigorous framework to identify how cultural and organizational factors influence the vulnerability of nuclear facilities. Explicitly identifying causal mechanisms between cultural and organizational influence (e.g., the 'human factor') and physical protection system performance (e.g., detection, delay and response) results in a complex, socio-technical system model of nuclear security that better aligns with the complexities of reality. Further, a system-theoretic approach combines the concepts of interdependence, hierarchy and emergence to describe how the information and control feedback loops interact with these causal mechanisms to influence (un)desired levels of security performance. This paper demonstrates the ability of this system-theoretic approach to evaluate the security of international spent nuclear fuel (SNF) transportation. Though limited in number, past experiences (e.g., the 1996 shipment of highly enriched uranium SNF from a research facility in Bogota to the Colombian coast for shipment back to the U.S.) and the predicted significant increase in international SNF transportation (e.g., SNF 'take-

back' agreements being offered by nuclear fuel suppliers to support the increased global demand for nuclear power) support the need for security analysis capable of integrating cultural and organizational influences on nuclear security. Decades of experience in SNF transportation safety analysis based on probabilistic hazard estimates forms the theoretical bases for common international security guidance and best practice documents that struggle to account for the expanding complexities of securing SNF during global transit. More specifically, security for this transborder, multi-modal distributed process must have the capacity to include such non- traditional security influences as ensuring consistent security across countries with varying resources and adequately shifting security responsibilities among federal and local organizations along a transportation route. By using the international SNF transportation as the demonstration case, the benefits of a systemtheoretic approach to security analysis indicates that explicitly incorporating causal mechanisms between social and technological components can mitigate such 'non-traditional' issues as an increasing number of SNF cask transfers between transportation modes (e.g., road to rail to water) and an increasing number of geopolitical or maritime borders crossed by SNF casks. Despite the increasingly dynamic security environment, the complex, socio-technical system model and associated analysis technique described in the paper provide a framework for overcoming the cultural and organizational barriers to improving security.

Synopsis ID: [160]

Qualitative Assessment of Nuclear Security Culture in a Public and a Private Radioactive Source Using Hospital

Islam, M.[1], Ahmed, M.[2]

[1] Department of Nuclear Engineering; University of Dhaka; Bangladesh.

[2] Scientific Officer, Center for Research Reactor, AERE, Bangladesh Atomic Energy Commission (BAEC), Bangladesh

Corresponding Speaker: M. Ahmed

In Bangladesh, different radioactive materials are used in hospitals for diagnostic and treatment purposes. Bangladesh, being a party to all the conventions and treaties related to safety and security of nuclear and radioactive materials, is firmly committed to provide adequate security to these nuclear and radioactive materials and their associated facilities. Nuclear Security Culture (NSC) is widely recognized and accepted tool for enhancing the nuclear security regime. Assessment of NSC is very important to identify the employees' beliefs, attitudes, personal behavior, leadership, and management system of an organization. This facilitates establishing and maintaining a robust and sustainable nuclear security regime. In response, a NSC assessment was performed at the radiotherapy department of a public medical college and hospital. A qualitative assessment was done according to the IAEA NSC model and its self-assessment methodology. , Different sets of culture indicators were selected by the self-assessment team. At first a survey was conducted among the staff of different levels for obtaining the security related baseline information about the facilities' overall management system towards prioritizing the nuclear security. Based on the survey result, an interview guide was made to conduct the interview for identifying areas of improvement and maintaining good practices. The interview was focused on identifying the leadership and personal behavior characteristics from the top level manager to the security personnel. From the survey result, a good response was observed from top manager on visible security policy, clear roles and responsibilities, determination of staff trustworthiness, professional conduct, adherence to procedure, vigilance, believes and attitudes. Also top manager had given an average response on performance management, basic security awareness training, work management e.g. planned work, feedback process, and self assessment. But a poor level of response was found from the top manager on work environment e.g. periodically visiting manned security posts, availability of nuclear security training program, contingency plan, information security e.g. cyber threat. Mid-level managers had expressed unsatisfactory opinion on work environment, training, and qualification and quality assurance. For example, in response of a statement like "The security significance of various rules and procedures is clearly adequately explained to me", the average answering level was 3.33 out of total scale 7 which is exhibited in Figure 1. On the other hand, technical operators had showed contradictory views on

work management and information security, operation, and maintenance, change management, feedback process and contingency plan and drills. Lack of proper training and education on nuclear security was also observed from the overall survey result.

Figure1: A Response of Management Level People

From the semi-structured and unstructured interviews, it had become possible to explore more information about the existing security culture level of the entire workforce of the radiotherapy facility. The results of the interview were mainly interpreted into three categories: longstanding, changing, and emerging issues. From the interview, it was observed that overall leadership and personal behaviors are acceptable where the nuclear security issue is considered as a changing issue. Some behaviors that support the nuclear security can be considered as longstanding. In this study, quality assessment of NSC using the same cultural indicators between a public and a private hospital will be carried out. The same method and structure will be followed for the case of a private hospital.

Synopsis ID: [280]

An Integrated Approach for Design and Implementation of Physical Protection System Elements for Nuclear Facilities

Sinha, V.[1], Thakur, A.[1], Kumar, A.[1], Sharma, A.[1], Kumar, R.[2]

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

[2] Dept. of Atomic Energy, India

Corresponding Speaker: V. Sinha

Physical Protection System (PPS) is an integral part of all Nuclear Facilities (NF). All modern NF, intrinsically by design, are distributed in nature as they handle different process stages of the NF. The NF, including all its geographically strewn processes are correspondingly protected by appropriate PPS elements. The PPS involves people, procedures and equipment spread across a Nuclear Facility.

It is important to get a Common Operating Picture (COP) using these distributed PPS elements in order to effectively and efficiently analyse the safety and security aspects of the NF. The design approach in integrating the PPS elements distributed across a Nuclear Facility essentially starts with classification of the systems. In order to effectively analyse the dynamic scenarios arising out of the day to day facility operations, the PPS systems can primarily be classified as of three types depending upon the functionality: 1) Protective: Detection & Analysis Elements 2) Preventive: Delay Elementsand 3) Reactive: Response Elements. The Protective elements essentially cover Intrusion Detection, Video Surveillance System, Area Monitoring, Contraband Detection etc. The Preventive elements include delay elements like Access Barrier System (automated/ manual), multiple access controls, double fencing etc.The Response elements essentially consist of the equipped response forces.The routine guard forces form a part of all these three elements.

The distributed and functionally independent PPS elements are connected over an encrypted constant data rate redundant communication media to a central monitoring & control station, which hosts the COP.Going by the availability of network hardware, IP based systems is the most obvious choice to integrate these spatially distributed elements, however this hardware selection again comes with its own challenges viz confidentiality, integrity, authenticity etc in order to avoid any intrusions into the system. This COP gives us an insight overview of the PPS System in a Nuclear Facility. The diverse and distributed elements provide an in depth picture essential for balanced protection of the NF. The COP helps us in a real-time analysis of situations in case of any nuclear security event. Such a centralized data repository of sensors, events and data also helps in carrying out Vulnerability Analysis of the PPS as a whole. The data repository also provides a unified platform to analyse attributes viz Insider threat, compliance with program standards etc and carry out post event analysis to bridge in the gaps in the PPS. A centralized feed of surveillance video helps in

effective video analytics and monitoring. Such an integrated approach is also helpful in effective scenario generations and simulation studies to keep the PPS updated to counter the ever emerging threats. The COP is characterized by a series of geo-tagged images which map the events to the points of occurrence in real time. Such an integrated approach to PPS helps in a better understanding of the system elements, a quick revisiting of the system status is easy to use, easy to scale, quick to analyse & easy to reconfigure to fit the desired responses. The paper discusses ways to efficiently introduce redundancy and diversity in the PPS.

Synopsis ID: [220]

Physical Protection Measures and Systems for Nuclear Materials in Uganda

Oboo, M.[1]

[1] Atomic Energy Council, Uganda

Corresponding Speaker: M. Oboo

Nuclear materials refers to uranium, plutonium and thorium in any form. These materials can be used by interested persons for nuclear terrorism acts with the intention to cause harm to their targets or to cause public fear. Thus the safety and security of these materials must be embraced by every state through ensuring that proper physical protection systems and measures are put in place.

Uganda is currently conducting uranium explorations in many parts of the country where many targets have been discovered and there are Phosphate and copper mining industries where remarkable traces of uranium are expected and yet these facilities have not setup physical protection systems and measures. The country is also bordered by Democratic Republic of Congo (DRC) where there is uranium mining and abandoned nuclear reactor where sabotage of these facilities can be a threat to Uganda since our border points are porous and have limited detection equipment and trained personnel. It should also be noted that there were reported incidences of stolen radioactive sources at Mulago National Referral Hospital in Kampala and in Kasese Cobalt Company Limited (KCCL) and have not been recovered up to now. This clearly shows that Uganda needs to do more to have feasible physical protection systems and measures to be put in place especially as the country is in the high gear preparations to ensure that there is a developed nuclear power plant in the country by 2031.

My paper presents the key human and physical aspects to be considered in each of the five areas of Access authorization, Access control, detection, delay, assessment and response that should be included in the design of the physical protection measures and systems by the concerned facilities and the country at large and provided they are considered and implemented, am confident that they will greatly help to improve the existing physical protection measures and systems and therefore minimum the opportunity of the adversary using nuclear materials for their various malicious actions.

In conclusion am indebted to say our country needs to adopt the suggestions and ideas in this paper to build robust physical protection measures and systems to ensure proper safety and security measures are put in place to ensure that the people and the environment are protected from the dangers of ionizing radiations that can a raise from the misuse of nuclear materials.

Synopsis ID: [243]

Verifying Operational Effectiveness of Nuclear Security Systems

Leach, J.[1], Nickerson, C.[2], Vieth, T.[1], Lee, D.[1]

[1] Sandia National Laboratories, Department of Energy, United States of America

[2] Idaho National Laboratory, Department of Energy, United States of America

Corresponding Speaker: J. Leach

Nuclear security and measurement systems are designed and implemented to prevent malicious acts involving nuclear and other radioactive material. As the hardware and software associated with these systems evolve, they have become heavily reliant upon network-based data, communication, and control pathways. If security professionals fail to properly address these pathways, an increased potential for remote exploits exist. The current threat has demonstrated evolving capabilities and technical sophistication to include the use of cyber attacks against nuclear security systems. The need for the Competent Authority and other participants in the threat assessment process to consider cyber capabilities for both insider and outsider threats is so important that it is distinctly identified in NSS-10, Development, Use and Maintenance of the Design Basis threat. As part of the licensing and evaluation process, security professionals must demonstrate the effectiveness of the protection system to protect against malicious threats. To accomplish this, gaps between physical and cyber elements and how these elements may be susceptible to external or internal exploits must be identified so that mitigation measures can be instituted. Gaps resulting in risk can typically be classified into one or more of the following areas: [U+F0B7] Physical exposure [U+F0B7] Persistent vulnerabilities [U+F0B7] Lack of skill and awareness, and [U+F0B7] Division of responsibilities For nuclear facilities in the pre-commissioning phase or in the process of retrofitting their systems, comprehensive site assessment testing can potentially address many physical and cyber concerns. Site acceptance testing is the inspection, dynamic testing, and qualification of systems or major system components verifying that the equipment or system meets or exceeds predefined operational requirements. A site acceptance test is an important step in the security system lifecycle process and provides a systematic evaluation of the security system. Threats to cyber-based nuclear security and measurement systems can come from numerous sources, including hostile governments, terrorist groups, disgruntled employees, and malicious intruders. Using a formal site acceptance testing for new or upgraded nuclear security systems provide process-related risk reduction. This paper will address the four areas of risk for a nuclear security system and describe how implementing a site acceptance test prior to commissioning a nuclear facility ensures a systematic evaluation of the security system against physical and cyber threats.

Synopsis ID: [264]

Complementarity between Physical Protection System and Nuclear Security

Chetaine, A.[1]

[1] University Mohammed V, Morocco

Corresponding Speaker: A. Chetaine

A physical protection system is the integration of people, procedures, and equipment used to protect assets or facilities against theft, sabotage, or other malicious human attacks. The PPS functions are detection, delay and response.

As Defined by the IAEA, Nuclear security is: The Prevention and Detection of, and Response to, theft sabotage unauthorized access illegal transfer theft , Sabotage , Unauthorized access, Illegal transfer or other malicious acts involving nuclear material, other radioactive substances or their associated other radioactive substances or their associated facilities. These objectives can be achieved with equipment, methods and human behavior that we can trust.

The objectives of the nuclear security and physical protection system is to protect nuclear facility or nuclear material against threats and terrorist. The equipment is not sufficient it must be completed with nuclear security and nuclear security culture to achieve this objectives.

The PPS and nuclear security can achieve the protection of nuclear facility and nuclear material if they complete each other's and fill the gaps.

Synopsis ID: [226]

Security Risks posed by Nuclear and Other Radioactive Materials at a Research Reactor Complex

Ek, D.[1], Potter, C.[1]

[1] Sandia National laboratories, Department of Energy, United States of America

[2] Sandia National Laboratories, Department of Energy, United States of America

Corresponding Speaker: D. Ek

Research Reactor is a general term to represent a wide variety of non-power reactors, critical assemblies, and the other co-located and associated facilities that undertake a variety of research and commercial activities on the same complex. As a vital part of the reactor operations, and that of the other co-located and associated facilities, there are a variety of radioactive materials found on the complex. The combination of nuclear and other radioactive materials pose a nuclear security risk, as has been outlined in numerous international instruments and Nuclear Security Series documents; however, the risks posed by some of these materials may be overlooked when assigning security priorities. In fact, the level of security risk posed by the research reactor complex is typically represented solely by the enrichment of uranium of the reactor fuel or by the power level of the reactor–in spite of the fact that there may be many high activity nuclear and other radioactive materials located on the complex.

This paper will discuss the security risks posed by inventory of nuclear and other radioactive materials on research reactor complexes, the reasons why a more balanced perspective of security based on the combined risks of all materials and facilities on the complex is prudent, and research currently underway to investigate this.

Synopsis ID: [254]

Nuclear Security Infrastructure Training for New Nuclear Power Programs

Kryuchenkov, V.[1], Artisiuk, V.[1], Labyntseva, M.[1]

[1] Rosatom, Russian Federation

Corresponding Speaker: V. Kryuchenkov

Building the capacity of nuclear operators and regulators, to develop, implement, and sustain a nuclear security and physical protection regime is a key requirement for a State embarking a new nuclear power and/ or nuclear research program. Promotion of Russian peaceful nuclear technologies to nuclear newcomer States requires, in particular, education and training in the area of nuclear security and physical protection. These training activities are based on the CPPNMA requirements, IAEA nuclear security recommendations and Rosatom good practices in physical protection of nuclear material and nuclear facilities.

State Atomic Energy Corporation Rosatom, being responsible vendor of several new nuclear facilities in newcomer countries, supports education and training in all 19 nuclear infrastructure development issues. Rosatom Central Institute for Continuing Education and Training (Rosatom-CICE&T) developed training materials for all these important nuclear infrastructure development issues including nuclear security in close cooperation with the Rosatom Departments of Physical Protection and International Cooperation, and the Rosenergoatom Concern, responsible for ensur- ing nuclear and radiation safety at all stages of the NPPs life cycle: siting, design, construction, operation, and decommissioning of NPPs. These training materials are dedicated to workshops, seminars and training courses for the personnel of Nuclear Energy Programme Implementing Organization (NEPIO), national operator and regulatory bodies of countries embarking nuclear power programmes.

In 2008-2015 Rosatom-CICE&T has developed training curricula and conducted international training courses and seminars on the nuclear security culture, NMAC, security of nuclear material in transport and practical training of instructors on these topics. In 2016 we launched training materials for the course “Development of a Nuclear Security Systems and Measures for the Implementation of a National Nuclear Power Programme” used for nuclear security infrastructure training of representatives five newcomer States. Training materials for this course were accepted by the IAEA as the basis for such International Training Course. A pilot event for eight newcomer countries was held in Obninsk, Russia, in October 2016, and next one is planned for September 2017 in St. Petersburg. In 2017 we started development of materials for a training course on nuclear security infrastructure of a nuclear facility at all phases of its lifetime and training seminar on computer security at nuclear facilities, both focused on needs of nuclear newcomers.

Key words: capacity building for nuclear security, nuclear newcomer State, nuclear security and physical protection training.

Synopsis ID: [211]

Training Quality Analysis for Protective Forces

Parker, J.[1]

[1] National Nuclear Security Administration, Department of Energy, United States of America

Corresponding Speaker: J. Parker

The Office of Defense Nuclear Security (DNS) completed a Training Quality Analysis (TQA) of protective force training at all National Nuclear Security Administration (NNSA) sites. The objectives of the TQA were to 1) determine optimal student time engagement (i.e. time spent actually working on improving task performance) during off-post training in order to maximize performance improvement, 2) identify and improve instructor leadership characteristics, and 3) seek opportunities to standardize documentation and processes.

After analyzing the TQA data internally, DNS assembled the protective force training managers from all NNSA sites and the National Training Center (NTC) to review the results and determine how to use the information to improve performance. During this phase, the participants learned about leadership characteristics and student outcomes, discussed time engaged, decided on a standardized approach for training plan documentation, discussed the linkage between Enterprise Mission Essential Task List (EMETL) needs and training, discussed how Outcomes-Based Training and Education fits into this analysis, and ultimately determined a path forward to improve protective force training and mission performance across NNSA. Enhancing Instructor Transformational Leadership Characteristics

The TQA team used correlational statistical analysis to determine relationships among instructor leadership characteristics and student outcomes using the Full Range of Leadership Model created by Bernard Bass (1985). This model categorizes leader/instructor actions into transformational leadership, transactional leadership, and passive-avoidant behavior styles. This concept provides the framework for defining the overall spectrum of leadership, from the most effective to the least effective.

Transformation leadership includes idealized influence (attributed and behavioral), intellectual stimulation, inspirational motivation, and individualized consideration. Transactional leadership includes contingent reward and management-by-exception (active and passive). The model also includes laissez-faire or the absence of leadership. Student outcomes include extra effort by the student, perceptions of instructor effectiveness, and satisfaction with the instructor.

The combined TQA team agreed that educating instructors on transformational leadership characteristics and their relationship with student outcomes will, indeed, enhance mission performance. By doing so, instructors can create training events with these characteristics in mind and thereby improve student performance at the end of each training day.

Improving the Utilization of Off-Post Training Time

During data-collection visits, the team observed training and captured the amount of time students either actively participated (physically), participated in a discussion, listened to a lecture, prepared for training, or were not engaged (e.g., on break, eating lunch, or waiting in line). The results showed that students were typically engaged 77% of the training day; however, percentages of active physical participation and listening to a lecture were almost equal. In other words, students spent almost the same amount of time listening to a PowerPoint presentation as they did actually practicing a task. The goal is to spend more time actively engaged and less time in lectures or waiting in line.

The TQA Team agreed that students should spend more time actively (physically) engaged and participating in discussions during off-post training rather than sitting in lectures or preparing for training. Furthermore, instructors should give the students instruction on the task to the best of their abilities and then structure training with a focus on "deliberate practice" so performance actually improves, which will improve mission performance under both routine and response conditions.

Standardizing Training Documentation

The TQA team discussed standard items that should be included in a training schedule/plan for a specific training day. It was necessary to agree upon a basic, standardized approach for training documentation that includes the following key elements:

Objectives • Standard to achieve • Achievement goal • Student numbers • Instructor numbers

Resources • Timeline/Outline • Additional training criteria

In the end, this approach focuses heavily on planning and preparation for training by instructors. This ensures available resources (e.g., time, personnel, ammunition) are utilized in a manner that maximizes return on investment. Ultimately, student performance in mission related tasks will improve using this training approach.

Synopsis ID: [59]

Perspectives for the Use of 3D Interactive Environment in Physical Protection Education and Training

Cherkashyn, D.[1]

[1] Institute for Security and Safety at the Brandenburg University of Applied Sciences, Germany

Corresponding Speaker: D. Cherkashyn

Despite facts that the First International Training Course on the Physical Protection of Nuclear Facilities and Materials was performed in 1979 in US and First Educational Program in Physical Protection was started in 1997 in MEPhI, RF, even today places where you could receive extensive training or graduate with diploma in this field can be counted on the fingers of one hand. The attention been paid to the issues of different areas in Physical Protection was raised for the last fifteen years, but with the larger number of States are willing to embark on Nuclear Energy or other nuclear applications, we can observe a lack of education capabilities in the nuclear security field. Even worse that in the area of nuclear technologies education, where future nuclear professionals usually don't have any introduction to security aspects of their job, basics of nuclear security culture and receive such information only after taking their position at the company, if ever receive. Usually shortage of the funding for overseas training for specialists from third countries and thought schedule of available training facilities, which are only few in the world, leave thousands of security related staff without initial or follow-up trainings, even though many of them work on Nuclear Facilities with Category I of Nuclear Materials or with highly dangerous Radioactive Materials. While the main problem of educational programs and trainings is a lack of practice for students with security system components, of security exercises and drills is issues to use real facility to perform such activity, and of security culture and awareness programs is natural apathy and resistance to such knowledges for future or actual nuclear facility staff, most part of those problems could be resolved with usage of state-of-the-art gamification technologies and virtual environments for immersive or non-immersive virtual reality utilization. Developed 3D interactive environments in the Institute for Security and Safety at the Brandenburg University of Applied Sciences are demonstrating possibility to give students insight into the world of security systems and their equipment as one big complex rather than number of separate components. "Serious games" approach also very attractive to perform awareness training and scenario simulation for security culture training. This paper describes two examples of the 3D models with different levels of interactivity, which are suitable for wide range education and training purposes as an inspection of Physical Protection Systems, Operation of Physical Protection Systems, Security Procedures Approbation, Performance Testing of Equipment, Security Exercises for individual security role or a group exercises including emergency training can be used with conventional monitors and input devices or with modern VR headsets for deeper insight. Internet connection allows participating in such

training sessions from any point of the World, which creates opportunities for distinguished experts from different countries to share with their valuable knowledge and experience without leaving their job. Such activities could be also interesting for non-technical experts of different position levels, who are researching in policy sciences or have decision-making power. Why would we not bring the training facility to participants instead of bringing participants to the training facility?

Synopsis ID: [230]

Training for Nuclear Facility Sabotage Analysis

Hale, R.[1]

[1] Oak Ridge National Laboratory, Department of Energy, United States of America

Corresponding Speaker: R. Hale

Radiological sabotage is defined as any deliberate act directed against a nuclear facility or nuclear material in use, storage or transport which could directly or indirectly endanger the health and safety of personnel, the public or the environment by exposure to radiation or release of radioactive substances. ORNL and SNL are engaged with NNSA to provide training on evaluating sabotage threats/vulnerabilities/consequences to nuclear facilities as part of series of training opportunities offered by DOE NNSA. The training is designed to meet the needs of partner States seeking to plan and implement security measures to protect facilities against sabotage of nuclear and radiological materials consistent with relevant international legal and guidance documents, including both international standards as well as US NRC/DOE perspectives. The training analysis makes use of existing/available nuclear facility documentation and covers the triad of threat/vulnerability/risk associated with sabotage for multi-focused audiences that include:

Regulators, (2) Licensee's (3) nuclear facility operational staff, and (4) Onsite and offsite protective force personnel. A description of the methodology for developing this training along with the a discussion of how the content material is "layered" and "branched" to allow rapid tailoring to meet audience needs is provided in this paper.

Synopsis ID: [198]

Training of New Security Inspectors - The Swedish Program from a Participant's Point Of View

Löfstström Johnsson, T.[1]

[1] Swedish Radiation Safety Authority, Sweden

Corresponding Speaker: T. Löfstström Johnsson

Training of new security inspectors - The Swedish program from a participant´s point of view The Swedish radiation safety authority is a values-driven and process-oriented organisation with an extensive training program for new co-workers and inspectors. The presentation contains an overview of the training program from a participant's point of view. The participant (the presenter) is a fire protection engineer that during the last year have done a transition from working with the oil and gas industry into the role as a security inspector in an authority, a journey that have given many new insights.

The Swedish programme for all new co-workers contains:

To work in a authority, formal requirements and the governmental system

Swedish Radiation Safety Authority – a modern values-driven organisation with three core values; Reliability, Integrity and Openness

Swedish Radiation Safety Authority – a process-oriented organisation The training program for inspectors contains:

The inspection processes in depth: to prepare, conduct and finally report the results of an inspection

How to interpret prescriptive and performance-based legislation

Legal requirements, especially the balance between the Swedish act on public access to information vs. the need for confidentiality

How to formulate an inspection report: injunctions, suggestions and acknowledgement of best practice

Interviewing methods

Communication and presentation techniques

Media training, all inspectors are supposed to be able to handle questions from media

Safety & security culture

Mandatory participation as observers in inspections The individual training program aspects:

Mentorship

The varying grade of knowledge about legal requirements and the role as a representative for the government

Individual background, education and experience from other jobs

Nomenclature – the transition from one industry to another

In addition to the oversight of the training program the presentation also contain a few personal experiences and take home messages:

Old truths are still valid - take responsibility for your own training and development

How to find the right mentor and what to do if you don't, because you won´t. The key is to use several persons and learn from different parts of the organisation.

Dare to ask, dare to be questioned and dare to say that you don´t know. If everyone keep this in mind, the learning process can be a benefit for both the trainee, the mentor and the organisation!

No training program will suite everyone due to different backgrounds and education. Use organisational core values to make the training program generic and then the make individual adjustments.

Synopsis ID: [101]

Nuclear Security Culture as a Tool to Address Insider Threat

Khripunov, I.[1], Speicher, C.[2]

[1] University of Georgia, United States of America

[2] Ministry of the Environment, Climate Protection and the Energy Sector, Baden-Württemberg, Germany

Corresponding Speaker: I. Khripunov

Nuclear facilities, organizations, and regulatory agencies have a compelling interest in developing effective methodologies to help mitigate potential insider threat. The IAEA defines an "insider" as one or more individuals with authorized access to nuclear facilities or nuclear material in transport who could attempt unauthorized removal or sabotage, or who could aid an external adversary to do so. The IAEA implementing guide "Preventive and Protective Measures Against Insider Threat" (NSS N◦8) has multiple references to the role of nuclear security culture (NSC) in addressing insider threat but does not provide any specifics in this regard. This paper attempts to fill in this gap and develop step-by-step guidance for using the evolving NSC methodology to perform this vital function. The IAEA NSC model has 30 characteristics of culture while the Draft Technical Guidance for NSC Self-Assessment lists over 300 culture indicators to illustrate the meaning of each characteristic. At least several of them are directly linked to the key widely used practices designed to prevent insiders from committing malicious acts and mitigating their possible consequences. For example, Human Reliability Program is covered by NSC characteristic "Continual determination of staff trustworthiness; Mitigation of Occupational Strain by "Work environment"; Compliance with IAEA Proposed Preventive and Protective Measures by "Adherence to procedures"; and Improved Observation Skills by "Vigilance" which includes observation and reporting. Culture indicators associated with these characteristics would enable management to self-reflect to determine existing weaknesses and strengths or launch, if deemed necessary, a full-scope self-assessment focusing on insider threat as the main theme. A follow-up NSC enhancement plan will prioritize, among other tasks, improving relevant management systems, targeted training curricula, awareness raising and reliable communication systems in a comprehensive effort to promote a robust culture with special emphasis on dealing with insider threat. Regularly held NSC self-assessments held at regular intervals will enable management to determine whether its follow-up plans yield desired results and what adjustments need to be made under the next plan. This cycle of IAEA recommended assessment and enhancement of security culture will keep insider risks under continuous scrutiny in a NSC general context rather than implementing separate and often disconnected initiatives in this regard. In addition, involving a considerable portion of the workforce in surveys, interviews and focus groups as methods of self-assessment can be a valuable and sustainable learning experience in addition to conventional classroom training format. Continuous focus on NSC as well as organization-wide

dissemination and discussion of self-assessment reports can deter potential insiders from implementing their plans. The proposed approach is just one possible way to cope with the insider risk but it has several important advantages which will be discussed in this paper.

Synopsis ID: [111]

Vision-Based Hand Motion Recognition for Insider Sabotage Detection Using Deep Learning

Chen, S.[1], Demachi, K.[1]

[1] The University of Tokyo, Japan

Corresponding Speaker: S. Chen

Introduction

Recently, the threat to nuclear security by sabotage is increased. In addition, when considering the sabotage, due attention should be paid to insider since they could take advantage of their access authority and knowledge, to bypass dedicated physical protection elements or other provisions. IAEA indicated that the physical protection system (PPS) of a nuclear facility should be integrated and effective against both sabotage and unauthorized removal. The primary PPS functions are detection, delay and response. It is noticeable that if detection failed, delay and response would become invalid. In this case, detection of insiders sabotage is necessary and should be enhanced. Hand motion has high contribution to human activity and a significant portion of maintenance behaviors and malicious behaviors can be detected through hand motion.

Conventional research of abnormal behavior detection commonly use static image analysis and learn features from normal pattern. However, it's difficult to distinguish malicious behaviors from ordinary maintenance behavior by static image analysis since some frames of these two types of motions may share some similarity. In order to solve this problem, time-series data analysis will be used in our research. Compared with static image analysis, time-series data analysis can detect more scenes, more detail information and time variation information. In addition, data compression can be proceeded and amount of computations can be reduced by feature extraction. Machine learning is frequently used to analyze time-series data. Moreover, research has shown the value of using Deep Learning for feature learning, and it can be applied in recognition of different patterns of motion.

Methodology

Fingertips position can be used to detect hand motion and recognize hand gesture. The fingertips calculation algorithm in this research based on RGB and depth image analysis. The hand motion detection system consists of four main components: RGB and depth data acquisition, hand region classification, fingers segmentation and fingers identification. Stretched fingers pixels and bend fingers pixels of both left and right hands were classified as different parts based RGB and depth

image. Fingers were identified by using K-means clustering algorithm. This system was developed by using Visual Studio 2015 with C# as programming language.

To distinguish malicious behavior and ordinary maintenance behavior, different malicious motion should be classified into different patterns. Deep Learning is considered as a useful method for pattern recognition and was implemented in this research. In current experiment, we assumed five malicious motions for behavior detection as follows:

Cutting motion (by using scissor, etc.);

Patting motion (control panel, etc.);

Turning motion (switch, etc.);

Grasping motion (tools);

Pushing motion (buttons).

Malicious motions with different persons in different distance and angle to camera were captured as trainset. By training Deep Neural Network using this trainset, these five malicious motions can be classified into different pattern.

Results

Positions of each fingertip can be captured by the real-time detection system we developed with the frame rate of 22fps.

All five assumed malicious motions can be detected from the testing time series data and distinguished from ordinary normal motions by using trained Deep Neural Network. Detection accuracy is shown as below:

Cutting Motion:100%;

Putting Motion:100%;

Turning Motion:92.47%;

Grasping Motion:96.23%;

Pushing Motion:84.25%.

Conclusion

In this research, a fingertips calculation algorithm was proposed and a real-time hand motion detection system was developed. In addition, assumed insider malicious motions can be classified into different patterns and detected using Deep Neural Network.

For future work, hand motion detection technology will be improved and Deep Neural Network will be implemented for the detection of sign of malicious insider sabotage. Furthermore, the prediction of detected features for earlier response will be taken into consideration.

Synopsis ID: [241]

Approaches and Modeling Techniques to Determine System Effectiveness against Insider Collusion

Snell, M.[1], Gibbs, P.[2], Scharmer, C.[1]

[1] Sandia National Laboratories, Department of Energy, United States of America

[2] Oak Ridge National Labs, Department of Energy, United States of America

Corresponding Speaker: M. Snell

Modeling the effectiveness of nuclear security systems against collusion that involves multiple insiders or insiders with outsiders has always been challenging. Historically techniques used by U.S. Department of Energy facilities for vulnerability analysis have approached colluding threat analysis primarily through modeling "super" insiders that combine attributes of two colluding insiders and by protecting key protection elements that are needed to defeat outsiders. While these approaches are certainly effective, they focus on only a subset of insider protection programs, thereby potentially resulting in protection that may be less effective than it could be or too costly or both. At the same time, these approaches are not readily extended to cover insiders who have access to cyber systems who can enable physical attacks by other insiders or outsiders. This paper discusses a number of evaluation methods for addressing colluding insider threats that, to our knowledge, have not received as much emphasis as they might merit. Two methods relate to building detailed process models for carrying out organizational activities or for representing fuel cycle activities involving nuclear material. Once constructed, such models help the analyst identify places in those processes where insider attacks may be more successful, whether these are part of the "super" insider scenario or not. Another described method relates to the novel applications of compartmentalization, either of insider knowledge, access, or authority to make collusion more difficult. The paper will also discuss how to use importance measures, reliability analysis, and other mathematical techniques to identify key protection elements and to evaluate where best to add system redundancies. Using these methods the authors outline options for creating new tools for security system designers and engineers to evaluate current and proposed designs against collusion. Finally the paper discusses how these techniques can support cyber/physical protection and how they align with, and extend, the methods developed by the International Atomic Energy Agency (IAEA) Nuclear Security Assessment Methodologies (NUSAM) Coordinated Research Project.

Synopsis ID: [148]

Introduction and Implementation of Physical Protection Measures including Trustworthiness Program at Tokai Reprocessing Facilities

Nakamura, H.[1], Kitao, T.[1], Kimura, T.[1], Yamazaki, K.[1], Iida, T.[1], Tasaki, T.[1]

[1] Japan Atomic Energy Agency, Japan

Corresponding Speaker: H. Nakamura

After the Great East Japan Earthquake followed by the accident of Fukushima Daiichi Nuclear Power Station in 2011, Japan learned a lesson that the blackout could cause the event of severe accident. To develop effective security measures based on the lesson learned from such crisis and to meet the IAEA security guideline (INFCIRC/225/Rev.5), Nuclear Regulation Authority (NRA) in Japan made a partial amendment of the regulations concerning the reprocessing activity in 2012. The regulation includes many additional important security measures, for example, introduction of limited access area, strengthened of the information control, cyber security measures, secondary central alarm station (SAS) and the new definition, "vital area" which is the areas in inner area where the equipment that supply AC power, remove decay heat and generate hydrogen are located, could cause unintended radiation release by the loss of those functions when sabotage occurs. JAEA Tokai reprocessing plant that have more than 20 facilities including several facilities classified as Category I, have implemented all of those security measures by the end of March 2014. Those new measures help us to keep high degree of security level for all the facilities in Tokai reprocessing plant and contributed to our planned operations, such as the vitrification of high active liquid waste solution and the conversion of Pu solution to MOX powder to reduce the potential risk of the plant. On the other hand, the trustworthiness program was newly introduced in 2016, based on the trustworthiness policy determined by NRA. The implementing entity of the program is JAEA for Tokai reprocessing plant, and is required for both the persons afford unescorted access to Category I and II, Central Alarm Station (CAS)/SAS, and the persons afford access to the sensitive information. Those who are involved this program will be judged before engaging the work whether they might act as insider to cause or assist radiological sabotage or unauthorized removal of nuclear material, or leak sensitive information. In this program, the personal information such as individual carrier, overseas travel history, criminal record, bankruptcy record and the relationship with organized crime groups etc., will be confirmed. Also the submission of the individual application based on the NRA public notice, personal interview, aptitude test and other necessary methods will be implemented for the clearance. The program is expected as a measure against insider at nuclear reactors for power generation and reprocessing facilities, and is expected to be enforced around the summer of 2017. In Tokai reprocessing plant, the trustworthiness program will be launched just after the NRA authorization,

and over 1000 employees need to be judged within a year. As well as the establishment of security measures, the promoting nuclear security culture for all employees and executive managers is a big challenge. JAEA have implemented the periodical education and training dedicated for the nuclear security culture in accordance with the annual plan with a goal in the beginning of every fiscal year. In addition to the periodical security education program, Tokai reprocessing plant have introduced many activities, such as the review of related manuals, the case study education of security events done by a small group, patrolling the site by the head of the plant and putting up the security culture poster and so on. Finally, an exercise with the response force against security events about intrusion and unauthorized removal of nuclear material by insider was first conducted in 2016 that contributed to a very productive discussion with all employees, guards, NRA and local police. Since the feedback and improvements are very important, we introduced PDCA (Plan, Do, Check, Action) cycle approach to the security that helps us to keep the high security level in the facility. This paper presents introduction and implementation with effectiveness of security measures in the Tokai reprocessing facilities in accordance with IAEA INFCIRC225/Rev.5 and the future security measures applied to the reprocessing facilities are discussed.

Synopsis ID: [28]

Intrusion Detection Measures against Insider Threats at Al-Tuwitha Nuclear Site

Saihood, A.[1], Al-Bakhat, Y. [1], Al-Hamadani, H.[1]

[1] Ministry of Science and Technology, Iraq

Corresponding Speaker: A. Saihood

Given the size of the terrorist threats facing the country at present, especially the threats related to the security of vital facilities, it was necessary to develop solutions and prepare studies that ensure the insurance coverage of these facilities at the human and material levels. Treason is a state of mind that makes man easy prey to the temptation of enemy agents and difficult to detect unless it takes an external physical appearance is the activity or action of the traitor such as espionage and sabotage, and because the difficulty of detecting treachery before achieving its appearance and the impossibility of avoiding the consequences of severe before it is a serious threat to security within the state. Therefore, all the means and procedures used so far to investigate and verify people's intentions do not give definite results in this regard. However, by taking care of the continuous investigations and their follow-up and re-investigation, the establishment of the risk in that respect. We have taken into consideration in this paper the type of risks that can affect on the site of Al-Tuwitha from the inside and risks associated with the behavior of individuals this paper is not intended to present a proposed physical security system. In the introduction the description of Al-Tuwitha nuclear site and the most important sites inside the site were discussed, In addition to the above, they and the magnitude of the risks that result from malicious acts have addressed it to give a description of the insiders may be potential to be on the site and the threats that may be obtained. The main responsibilities of the nuclear security team at the site were also addressed to the external and internal threats under consideration, In addition, the most important procedures were followed by the nuclear security teams and committees, including the site protection force, which represents preventive measures, protection measures and contingency plan that can be applied in the event of a terrorist incident or internal threat. This paper aims to describe the intrusion detection measures against insider threats at Al-Tuwitha nuclear site through studying potential threats inside the site. The procedures for securing the facilities depend on the efficiency of the security and security apparatus in carrying out these procedures. Therefore, everyone who deals with security work must stand on the bases and rules of insurance of enterprises, their nature and risks and the procedures followed which is Compatible with the IAEA

Synopsis ID: [283]

Nuclear Security of Regulatory Authority

Janjić, V.[1], Lucic, V.[1] , Avramović, I.[1]

[1] Serbian Radiation Protection and Nuclear Safety Agency, Serbia

Corresponding Speaker: V. Janjić

Constant growing threat to nuclear and radioactive material requires complete dedication to security principals from all stakeholders in nuclear industry. Main goal of nuclear security is protection of nuclear and other radioactive material and related facilities where mentioned material is present. Regulatory body, although not in direct possession of nuclear or radioactive material, is in close connection with institutions and facilities where mentioned material is stored and used. As an institution responsible, among other things, for issuing and reviewing licenses to operators and for keeping records of nuclear material and radiation sources under regulatory control, regulatory body have an information that could be used for potential malicious acts against both, material and facilities. In that light security and physical protection of regulatory authority should also be included in overall state nuclear security regime.

Nuclear security system at the regulatory authority should be established following two concepts: protection of premises, documents and information in possession and compliance with the principals of nuclear security culture and trustworthiness program. Security system should be built to prevent potential adversary from obtaining any information that could help him to perform malicious act, and also to prevent any unintentional leakage of information from personnel.

Regulatory authority usually have an information about nuclear and radiological facilities, their functional properties, security systems and also information about type, quantity and location of nuclear and other radioactive material. All those information, both in digital or hardcopy, should be considered as classified and need to be protected with proper physical protection system. Additional measures of cyber security for handling digital information, need to be implemented due to growing threat of cyber-criminal.

Trustworthiness program for personnel need to be established. All employees should be subject to background check before employment and regularly reviewed afterwards. Well defined procedures for handling restricted documents and information should be established and consequently, issuing clearance levels for all employees, based on their position and responsibilities within organization. Nuclear security culture should be strongly promoted in organization on all levels. Employees should be familiar with all internal procedures regarding security and compliance with those procedures should be regularly evaluated. Additional attention and education should be devoted to employees which professional duties are not directly related to nuclear and radiological activities, such as lawyers, administration and human resources personnel.

Regulatory authority have an important role in overall state nuclear program and therefore it could be potential target for malicious act, or to give an adversary a key to access nuclear or radiological facilities. States nuclear security regime can be considered as effective only if covers all aspects of nuclear and radiological activities in the country and if includes all relevant organizations.

Synopsis ID: [192]

Considerations for Deploying a Security Information and Event Management System supporting Physical Protection Systems in Nuclear Facilities

Cowie, A.[1]

[1] Australian Nuclear Science and Technology Organisation (ANSTO), Australia

Corresponding Speaker: A. Cowie

This paper presents an overview of the considerations required when deploying a managed Security Information and Event Management System (SIEM) to monitor computer-based Instrumentation and Control (I&C) systems that are crucial to the availability and operation of a Physical Protection System (PPS) that enables a Nuclear Facility to achieve its Physical Protection objectives. Due to this linkage, these I&C systems would fall within the scope of a facility's Sensitive Digital Assets (SDA). The protection of computer-based systems, including those used for Physical Protection, is recommended by the International Atomic Energy Agencies (IAEA) Nuclear Security Series No. 13 (NSS13) - Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5)1[2]. A compromised Physical Protection System may result in a facility's inability to meet its Physical Protection objectives. For instance, an SDA within a Security Alarm System (SAS), which provides a detection an informs a response function, could be compromised by an adversary in such a way that they are able to intercept and modify a data stream which prevents the system from indicating to an onsite response force that it is in alarm. Another adversary may seek to compromise the confidentiality of an Electronic Access Control System (EACS) SDA, which provides the physical protection functions of deterrence, detection, and delay. The Sensitive Information this SDA may store, process, or communicate, could be used in the process of granting access into a protected area (such as a badge number, PIN code, or an individual's biometric data). If the confidentiality of this information is compromised, an adversary may be able to replay the same information to gain unauthorised access into areas that contain safety-critical nuclear I&C systems. In either case, the adversary has had a material impact on the facility's Defence in Depth. Such a malicious act could contribute to the ability of an accompanying physical attack element to cause the unauthorised removal of nuclear material or sabotage of a nuclear facility through a reduced ability to meet its physical security objectives. Therefore, computer security measures for Physical Protection System SDAs need to be applied with the knowledge that their availability, integrity, and confidentiality are intrinsically linked to a facilities ability to achieve its nuclear security objectives. Such an SDA may be defined as "security-critical". Nuclear Security Series No. 17 (NSS17)[2] suggests an approach where a higher level of computer security protection is provided to

critical systems to maintain their integrity. This is coupled with strict data flow requirements for systems of a higher security level. At the highest level where data flow is still permitted, the example security levels within NSS17 would permit only unidirectional outbound communication to protect the integrity of the SDAs within the higher security level. NSS17's constrained data flow model is inadequate for a Physical Protection System. A facility must also be concerned about the confidentiality of the information used as part of the authentication process. This causes difficulties when connecting the Physical Protection System to a Cyber Security Operations Centre (CSOC) monitored SIEM. This paper details a prototype SIEM built upon an open-source toolset able to process, alert, and analyse example network protocols and events used within a Physical Protection System. This mock environment is then used to understand the data flow requirements between a physical protection system and a CSOC, analyse their functions in support of a facilities nuclear security objectives and identify their classes of sensitive information and their susceptibility to compromise. The analysis demonstrates that the CSOC and Physical Protection System, while being closely related, require protection methodologies for their Sensitive Information. While the two systems logically share the same security level, they should be separated between different security zones with additional controls applied to allow monitoring of the Physical Protection System, while preserving the confidentiality of the sensitive authentication information. The paper concludes that proper security architecture requires an analysis of each system and how the sensitive information it stores, processes, and communicates, contributes to a function within the facility. This information determines the security level of the system and only then can an appropriate security zone be defined to preserve common need-to-know and need-to-access restrictions for sensitive information.

Synopsis ID: [297]

Planning & Executing an International Transport of Category I Nuclear Materials – the UK Delivering Specialist Nuclear Services with Pride

Whittard, B.[1]

[1] International Nuclear Services Ltd, United Kingdom

Corresponding Speaker: B. Whittard

Regarded as the world leader in the maritime transport of specialist nuclear materials (SNM), International Nuclear Services (INS), together with the Civil Nuclear Constabulary's Strategic Escort Group (CNC), have worked closely with the British Government and the UK's independent competent authority, the Office for Nuclear Regulation, to successfully plan and execute a number of Category I transports of SNM by sea in support of commitments made at the Nuclear Security Summit.

Each of the above organisations have played an important role and contributed to successfully plan, permission and execute these shipments; ensuring each transport is completed with effective yet proportionate security arrangements that are in line with both domestic UK regulations and international obligations. This paper will describe the work that each organisation undertook to complete these specialist transports, to help support global threat reduction, and reveal some of

the challenges encountered in delivering these highly sensitive shipments to make the world a safer and more secure place.

In doing so, the paper will explain how the UK is committed to helping States deliver their commitments made at the Nuclear Security Summit and how it supports wider global threat reductions initiatives. It will discuss the intergovernmental relationships established and the subsequent agreements made in line with the Convention for the Physical Protection of Nuclear Material (CPPNM) to allow for these shipments to proceed, and describe how information and communications concerning these international transports are managed between Governments to ensure the right balance between transparency and security is struck.

It will describe how INS and their partners at the CNC prepare, execute and review each shipment and give an insight into how INS, as a world leader in the transport of SNM, delivers these unique transports in accordance with UK regulations and international recommendations developed by the International Atomic Energy Agency (IAEA). The paper will also cover the specialist emergency response and resilience arrangements that INS and CNC put in place to ensure these shipments are delivered to highest safety and security standards for its customers, stakeholders and the public.

Finally, it will explain how the Office for Nuclear Regulation, with the support of the Military of Defence, provides independent oversight of these arrangements to ensure they are completed in accordance with UK legislation and describe how they achieve their mission to provide efficient and effective regulation of the UK's nuclear industry, holding it to account on behalf of the public. In summary, it is hoped this paper will serve to further improve awareness around the measures and challenges faced when planning and executing an international transport of Category I SNM and help share UK experience with its international partners.

Synopsis ID: [222]

A Performance Based Approach for the Security of Nuclear Materials in Transport or "Answer the Threat Not the Prescription"

Tertrais, C.[1], Forest, Y.[1], Ropital, R.[1], Faudonnier, D.[1]

[1] Department for Nuclear Security, France

Corresponding Speaker: C. Tertrais

Background :
Having a large nuclear industry imposes France to have a robust physical protection regime for the security of nuclear material, their facilities and their transport as well as a strong nuclear security authority. In this regard France reviewed its regulation and its Designed Basis Threat (DBT) from 2009 to 2011. However, to adapt to the current threat, adjustments are to be made. It mainly consists in focusing more on a performance based approach rather than to rather rely on compliance with very prescriptive requirements. Prescriptions exist and are to remain. However, the main purpose of the proposed evolution is to make sure security measures are designed to answer the evolving threats.

An evolving and hard hitting threat

The international context has changed and the threat has very much evolved this last decade with the multiplication of terrorists attacks worldwide. Adequate level of protection of nuclear material, their facilities and their transports are, in this context essential. For the French nuclear security authority, this objective can be reached in particular through a nuclear security regime that :

relies on a strong training and exercises policy that is adequately controlled;

focusses on performance achievements instead on "only" aiming at compliance with detailed prescription; includes a stronger nuclear security culture.

In this regard, the nuclear security authority has renewed its general approach on nuclear transports. The current regulatory framework is under revision and is expected in 2019-2010. New requirements are been tested and progressively implemented. Higher standard for operators and an improved authority oversight start been processed in order to enhance accordingly the security of all the phases of nuclear transports. "Answer the threat effectively and do not only answer the prescription", this is the presentation France proposes to share and to elaborate at the November 2017 security conference in Vienna.

Synopsis ID: [181]

Vulnerability Assessment for Sabotage during Nuclear Transport in Germany

Doehler, M.[1], Bruecher, W.[1]

[1] Gesellschaft für Anlagen- und Reaktorsicherheit gGmbH, Germany

Corresponding Speaker: M. Doehler

In Germany the regulations for physical protection of nuclear transports are revised periodically. The latest revision of the regulations concerning the DBT and the requirements for the physical protection of nuclear transports had major effects with respect to sabotage. Within the licensing procedure of transports of nuclear material in Germany one licensing requirement is a suitable physical protection system including measures against unauthorized removal as well as against sabotage. The revised DBT implies sabotage scenarios and therefore a new categorization scheme based on an assessment of potential radiological consequences as well as new requirements to implement adequate physical protection measures for sabotage were introduced.

In IAEA NSS No. 13 it is recommended to not only determine the physical protection requirements to prevent unauthorized removal of nuclear material during transport but also to take into account the potential radiological consequences of sabotage of a shipment of nuclear material and additional protective measures in those cases where the need for protection against sabotage warrants them. A sequence of considerations in determining the physical protection measures applicable to a shipment, taking into account all of the potential risks is given in IAEA NSS No. 26-G. In the flowchart it says that after the characterization regarding theft one should consider whether a sabotage could result in unacceptable radiological consequences for material of Cat. I or II. In the German regulations a graded approach is also applied for Cat. I, II and III. The categorization procedure itself corresponds to the one suggested in IAEA NSS No. 26-G.

The change of the regulations results in relevant changes of the physical protection measures applied by the shipper/carrier/license holder. During the licensing process a vulnerability assessment has to be carried out to proof that sabotage could not result in unacceptable radiological consequences. This is reviewed by the licensing authority, usually supported by a TSO assessing the physical protection measures.

The presentation will provide an overview of the new German approach for considering sabotage to nuclear material transport within the licensing process compared to the IAEA recommendations. Furthermore, the challenges resulting from the new regulation and the experience from licensing procedures will be discussed (e.g. identifying suitable measures to reduce the radiological consequences to an acceptable level and assessing the performance of these measures).

Synopsis ID: [88]

Regulating the Transport of UOC in Australia

Botha, M.[1], Bayer, S.[1]

[1] Australian Safeguards and Non-Proliferation Office, Australia

Corresponding Speaker: M. Botha

The transport of uranium ore concentrates (UOC) from the production plant to its final destination can involve many parties including mines, carriers (road, rail and shipping), ports, stevedores and first responders. In Australia, the Australian Safeguards and Non-Proliferation Office (ASNO) is responsible for regulating the security of uranium in use, storage and transport under the Nuclear Non-Proliferation (Safeguards) Act 1987 while transport safety is subject to separate State jurisdictions. ASNO recently concluded a review of the regulatory requirements contained in transport permits issued under the Safeguards Act. The review drew on the recently published IAEA guidance document Nuclear Security in the Uranium Extraction Industry 1 and the outcomes of a UOC Transport Working Group. The long transport distances involved in Australia presents challenges such as unsealed roads, necessity to use interim storage, availability of communications and timeliness of response to incidents. International shipping must address piracy, denial of access and shortage of available cargo liners willing to take Class 7 dangerous goods and the constraints imposed by port authorities. Most of Australia's UOC exports are currently done through Adelaide in the State of South Australia. The government of South Australia recently established a UOC Transport Working Group of industry, state and federal government and first responder representatives for the identification, coordination, monitoring and execution of initiatives directed toward maintaining the safety and security of UOC. The working group conducted a SWOT analysis of the current transport arrangements and has identified key action items. These include providing best practice guidance for Transport Plan content, determining standards and obligations for incident responses, Industry expertise to establish specific training for first responders. The aim of the permit review was to address all the above mentioned issues and also to achieve a more functional permit layout, by separating pre-transport, during-transport and incidental storage requirements. The review also refined a scalable threat model in which transporters are required to establish a system of planned interim measures that collectively address changes in threat levels and their associated risks. From the review, ASNO produced a number of template permits and compliance codes that cover the various stages of transport including road/rail transport, sea transport and stevedoring. These permits specify requirements for physical protection, inventory control and emergency response for transporting UOC and for the content of transport security plans. The paper will outline Australia's policies and regulatory requirements for the transport of UOC and elaborate some of the more significant changes to requirements arising from the review. The paper will also outline the benefits of industry and government stakeholders working together to improve security and other governance arrangements for

UOC. 1 INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security in the Uranium Extraction Industry, IAEA-TDL-003, Vienna (2016).

Synopsis ID: [260]

Training on Security during Transport of Nuclear and Other Radioactive Materials

Pope, R.[1], Liu, Y.[1], Shuler, J.[2]

[1] Argonne National Laboratory, Department of Energy, United States of America

[2] U.S. Department of Energy, United States of America

Corresponding Speaker: R. Pope

Shippers and carriers (operators) of nuclear and other radioactive materials, along with regulators and other entities involved in such shipments, are responsible for ensuring that a sound security culture exists for such shipments. These entities also must ensure that the transport security system they use for shipments is adequate and follows appropriate regulatory principles. For each shipment, the transport security system needs to satisfy the security requirements imposed by international conventions and agreements and by the responsible regulatory bodies of each country transited by the shipment. For example, the development and operation of the nuclear material transport security system must be consistent with the categorization of the material being shipped and must embody all relevant security provisions set forth in the Convention on Physical Protection of Nuclear Material (CPPNM), the amendment to the CPPPNM, INFCIRC/225/Rev. 5, and any relevant international modal and State regulations. Many of these documents specify that all entities involved in the transport of nuclear material, as well as other radioactive materials, must be properly trained to fulfill their specific assigned functions. These entities include consignors (i.e., shippers); carriers; consignees (i.e., receivers); and escort, guard, and emergency responder personnel. For international shipments, involved entities also may include border crossing and customs personnel. This requirement has been satisfied, in part, through an effort undertaken at Argonne National Laboratory to provide detailed training and hands[U+2010]on experience for individuals involved in transporting nuclear and other radioactive materials. The training focuses on (1) raising awareness and strengthening security during the transport of nuclear and other radioactive materials and (2) gaining experience in training personnel so that lessonslearned can be used to enhance the training experience. This training effort is supported by the U.S. Department of Energy's (DOE's) Packaging Certification Program within the Office of Packaging and Transportation, Office of Environmental Management (EM). These training courses have focused on transport security requirements; promotion and sharing of good practices; and their effective application through a sound, structured, and comprehensive security culture. The training has matured from its initial one[U+2010]week pilot in 2013, which addressed both international and domestic transport security: a single course was held in 2014, focusing on international transport security; two courses were held in 2015 and 2016, each dealing with U.S. domestic transport security; and currently, a course is scheduled for September 2017, dealing with international transport security. The transport security course is part of the curriculum of the

Graduate Certificate in Nuclear Packaging program, inaugurated in 2015 at the University of Nevada, Reno. The goal of this training effort is to improve the ability of the participant to deny those with malicious intent from stealing, diverting, or attacking shipments of nuclear and other radioactive materials. Those trained have come from North America, Europe, and Asia. Participants have included representatives from regulators; consignors, carriers, consignees, and shipping brokers; and state/regional inspection, escort, enforcement, and response personnel. The courses have included lectures, discussions, and exercises that are comprehensively directed toward: • Understanding why transport security is needed, its fundamental security principles, and definitions; • Overviewing both the security requirements and recommendations of international and U.S. domestic transport, and guidance from international and U.S. governmental organizations;

Developing transport security systems that follow the graded approach specified by regulations;

Developing transport security plans (TSPs) that satisfy regulatory security requirements; • Participating in hands[U+2010]on and field exercises involving TSPs, readiness review, and corrective actions; and • Monitoring and tracking a mock shipment with "staged incidents" through a field exercise by using the ARG[U+2010]US remote monitoring systems. Lecturers of the training courses have included experts from involved organizations, both domestic (the

Nuclear Regulatory Commission [NRC], the U.S. DOE, and the U.S. Federal Bureau of Investigation [FBI]) and international (the International Atomic Energy Agency [IAEA], the World Institute for Nuclear Security [WINS], and the World Nuclear Transport Institute [WNTI]). The breadth of experience and knowledge developed through these training courses has also contributed significantly to two WINS Best Practice Guides focused on transport security and the WINS Academy training module on Transport Security Management. This paper will review and highlight the lessons learned from the training courses held from 2013 to 2016, how the lessons learned have been used to improve the training and to enhance the table[U+2010]top exercises in the 2017 international security course, as well as how this knowledge and experience base could be used to leverage future transport security educational efforts worldwide to support capacity building.

Synopsis ID: [62]

Benchmarking Security Standards and Knowledge Innovations of Physical Protection of Nuclear Materials and Facilities: Organization Absorptive Capacity Perspectives

Hossain, M.[1]

[1] Bangladesh Atomic Energy Commission, Bangladesh

Corresponding Speaker: M. Hossain

The need for adequate physical protection of nuclear materials and facilities has emerged as a strategic imperative that is increasingly tied to benchmarking its security standards and knowledge innovations into the organization. In the light of this, CPPNM, and IAEA have developed convention, recommendations for physical protection standards for nuclear materials and facilitated to assist member states in implementing a comprehensive physical protection regime. Individual states assure physical protection through establishing and operating a physical protection oversight system. However, despite the clear benefit of protection, there is currently lack in many organizations establishing standards of physical protection. Hence, the benchmarking of these physical protection standards raises the issues of absorptive capacity of an organization. These gaps are the prime motivators for this work. Therefore, this study aims to benchmarking these physical protection standards and knowledge innovations into organization. The conceptual model of benchmarking process of security standards and knowledge innovations of physical protection of nuclear materials and facilities in organization grounded upon contextual theories of organizational absorptive capacity, and benchmarking principle 1. Through benchmarking relevant nuclear organizations can best understand the progression of physical protection and mitigate the consequences by reference to external perspectives of security standards and knowledge innovations from stakeholders. Hence, the essence of benchmarking of physical protection standards and knowledge innovations is to develop these external perspectives, and to search for innovation levels and practices that will provide a competitive edge to the nuclear organizations. Finally, this paper offers a useful framework to assess the organizational absorptive capacity as system and knowledge frames context that impact on the sustainable physical protection standards and knowledge innovations in organization. Theoretical Framework: Based on the theoretical proposition, this study offers a new conceptual model of benchmarking as shown in Figure 1. Organizational absorptive capacity is the ability of an organization to absorb, assimilate, and establish new standards, knowledge innovations through its prior related infrastructures [2]. In this context, the related infrastructure refers to organizational prior internal knowledge frames and systems standards efficacy. [Figure 1 here] Organizational absorptive capacity is widely understood to enhance an organization's innovative capabilities [3]. The organizational absorptive capacity broadly conceptualizes as absorptive system and knowledge

frames context. The figure shows the five central elements of organizational absorptive capacity as the process of benchmarking:

Computer system security goals setting are defined as outcomes, events, or processes and are viewed as internal psychological representations of desired states [4]. Organizations should set CSS goals in relation to integrity, confidentiality and authenticity of data through the organizations' computer systems; (2) Physical protection systems standards efficacy reflects the perceptual measures of comprehensiveness, flexibility, and enforcement of organization to support sustainable physical protection systems and value creation. Nuclear organization can potentially accelerate sustainable physical protection systems by establishing required sustainable physical protection systems and laws; (3) Knowledge integration focuses on how people act and interact to generate knowledge regarding a specific innovations as a resource for individual and collective ends [5]; (4) Knowledge opportunism reflects capacity of scanning the environment for emerging technologies/innovations and respond proactively to exploit, avoid, or ignore potential opportunities and threats. (5) Policy knowledge constitutes a capability developed in particular contexts and depends on collective understandings regarding a specific technology process in organization. The policy process is inextricably linked to organizational knowledge [3,4], and the processes that policies are developed, implemented, and used depend on how policy knowledge is constructed [6]. Research method, data, and analyses: Final study intends to adopt a survey method and secondary data sources. The assessment of the research model will be analyzed using Partial Least Squares (PLS), PLS-Graph version 3 or higher. Results and impacts This research is expected to extend and enrich the extant literature on benchmarking process and absorptive capacity of security standards and knowledge innovations of physical protection of nuclear materials and facilities in organization, thereby providing important new insights into innovations assimilation within organization. Finally, the expected outcomes of this paper are then used as a stimulus for action, which is intended to mitigate the consequences of both inside and outside threats and improve the organization's relative position by assimilating and sustaining the physical protection standards and knowledge innovations within organization. References: 1. Camp, C 'Benchmarking: The search for best practices that lead to superior performance - part 1 to 5' Quality Progress (January-May 1989) 2. Cohen, W. M., and Levinthal, D. A. Absorptive capacity: a new perspective on learning and innovation. Administrative Science Quarterly, 35, 1, 1990, 128–142 3. Liang, H., Saraf, N., Hu, Q., and Xue, Y. Assimilation of enterprise systems: the effect of institutional pressures and the mediating role of top management. MIS Quarterly, 31, 1, 2007, 59–87 4. Perkering, I. and Chambers, S. " Competitive benchmarking: progress and future development" Computer-Integrated Manufacturing Systems, Butterworth-Heinemann Ltd., 1991

Synopsis ID: [214]

Exploring the Possibility of Forensic Investigations on Steam Turbine Governing Systems

Altschaffel, R.[1], Hildebrandt, M.[1], Kiltz, S.[1], Dittmann,J.[1]

[1] Otto-von-Guericke-University of Magdeburg, Germany

Corresponding Speaker: M. Hildebrandt

Steam turbines form an important part of any power plant. They perform the task of generating electric power by using the steam pressure generated by the reactor itself. In general, steam turbines consist of a shaft connected to a number of blades. These blades form blade rows and are formed so that the connected shaft revolves once steam pressure is pushing against these blade rows. In order to improve flow characteristics inside the turbine a number of static diffusers and bends might be connected upstream. Turbines need a constant stream of steam with specific temperature and pressure. To ensure these conditions steam turbine governing is used. Steam turbine governing relies on valves controlled by industrial automation. Errors or incidents in this governing can influence the specific parameters and led to reduced efficiency, breakdown or direct damage to the involved components.

In this work we discuss the industrial automation used in steam turbine governing system and show possible exemplary attacks on such systems. In the context of this work these attacks will be modeled according to the established basic attacks (read, spoof/create, interrupt, modify, steal/remove). When an attack or an error is detected it is necessary to reconstruct what has happened. This might be an integral part of the contingency plan and to reduce further threats. Investigation might be needed to prove guilt or innocence of the involved parties. Especially in the later case it is necessary that such a reconstruction adheres to scientific and well-proven principles. These principles are referred to as a forensic process. A forensic process requires the used traces to be authentic (originating from the subject of the investigation), integer (unaltered by external influences or during the course of the investigation) and well documented. We will discuss the possibilities of a forensic investigation performed on steam turbine governing system in order to reconstruct course of events that led to an incident. This requires the identification of data streams, the means to gather and analyze these and a thorough analysis on the forensic soundness of these traces. While functional safety is an often discussed topic in this domain and is therefore well researched it is often unclear if an incident arises from an error and an attack. Hence an investigation should follow the same principles.

As a foundation for this work we use a simulation of a steam turbine governing system using the Siemens SIMIT v9.0 simulation framework. The simulation environment provides a simulated flow of steam with variable pressure and temperatures which are measured by simulated sensors (employing a 3-way redundancy for each measurement location). Our Siemens S7 1516F-based

I&C system controls the steam flow to maintain steady 1500 rpm of the turbine in order to ensure the constant output of a 50 Hz alternating current of the attached generator. The sensor readings and control messages to valves are logged via a central historian system. This particular system is the focus of our investigation in this paper. Based on simulated attacks on sensor readings, control messages and the log messages to the historian, we analyze the possibility of tampering with potential evidence. We will discuss potential traces and countermeasures for protecting the integrity and authenticity of the logged data with respect to the specific threat assessment in NPP.

Synopsis ID: [247]

Trustworthy Design Architecture (TDA): Cyber-Physical System

Choi, S.[1]

[1] Sandia National Laboratories, Department of Energy, United States of America

Corresponding Speaker: S. Choi

Conventional cyber defenses require continual maintenance: virus, firmware, and software updates; costly functional impact tests; and dedicated staff within a security operations center. The conventional defenses require access to external sources for the latest updates. The whitelisted system, however, is ideally a system that can sustain itself freed from external inputs. Cyber- physical systems (CPS), have the following unique traits: digital commands are physically observable and verifiable; possible combinations of commands are limited and finite. These CPS traits, combined with a trust anchor to secure an unclonable digital identity (i.e., digitally unclonable function [DUF] – Patent #62/175,753; CodeSeal, physically unclonable function [PUF]), offers an excellent opportunity to explore defenses built on whitelisting approach called "Trustworthy Design Architecture (TDA)." There exist significant research challenges in defining what are the physically verifiable whitelists as well as the criteria for cyber-physical traits that can be used as the unclonable identity. One goal of the project is to identify a set of physical and/or digital characteristics that can uniquely identify an endpoint. The measurements must have the properties of being reliable, reproducible, and trustworthy. Given that adversaries naturally evolve with any defense, the adversary will have the goal of disrupting or spoofing this process. To protect against such disruptions, we provide a unique system engineering technique, when applied to CPSs (e.g., nuclear processing facilities, critical infrastructures), that will sustain a secure operational state without ever needing external information or active inputs from cybersecurity subject-matter experts (i.e., virus updates, IDS scans, patch management, vulnerability updates). We do this by eliminating system dependencies on external sources for protection. Instead, all internal communication is actively sealed and protected with integrity, authenticity and assurance checks that only cyber identities bound to physical component can deliver. As CPSs continue to advance (i.e., IoTs, drones, ICSs), resilient-maintenance free solutions are needed to neutralize/reduce cyber risks. TDA is a conceptual systems engineering framework (Submitted for IEEE, 2017 ICCST Conference publication) specifically designed to address cyber-physical systems that can potentially be maintained and operated without the persistent need or demand for vulnerability or security patch updates.

Synopsis ID: [30]

Physical Protection of Nuclear Materials and Nuclear Facilities; Nigerian Nuclear Fuel Conversion the Progress Made

Onoja, R.[1]

[1] Ahmadu Bello University, Nigeria

Corresponding Speaker: R. Onoja

The threats from terrorist attacks are in the increase and the nature of attack keeps changing. This has been a concern to all states with Nuclear Materials as well as Facilities.

.Nuclear Security Summits (NSS) were convened in 2010, 2012, 2014 and 2016 to address the security of nuclear and radiological materials, specifically, to stop nuclear and radiological materials

from reaching non-state actors so as to avert potential sabotage on nuclear facilities through stringent physical protection systems. Nigeria has five (5) Nuclear Energy Centres of which Centre for Energy Research and Training (CERT) Ahmadu Bello University Zaria is one. CERT has two facilities having nuclear and radiological materials, the Waste Management Facility (WMF) and the Research Reactor Facility (NIRR-1). Orphans and spent sources are kept and managed in the WMF. CERT has been operating its nuclear reactor which currently runs on HEU fuel. The reactor which was critical in 2004 is currently undergoing conversion to LEU. Since commissioned, certain physical protection measures have been put in place but then there are quite numbers of challenges. However , this presentation shall address this issue as well as on the journey so far on the preparation for the conversion process in Nigeria and experience gained.

Synopsis ID: [113]

Best Physical Protection Practices at Spanish Nuclear Power Plants

Pérez-Baez, A.[1], Lardiez, P.[1], Calvín, M.[1]

[1] Consejo de Seguridad Nuclear (CSN), Spain

Corresponding Speaker: A. Perez-Baez

In Spain there are 8 nuclear reactors in 6 sites, all of them PWR and BWR designs, belonging to private companies and built during the 70´s and 80´s. The Nuclear Safety Council (CSN) is an independent nuclear regulator who controls and oversights the safety and security in these facilities. The CSN issued a Security Order in 2006 in which Ministry of Interior –also Competent Authority in Security- and Operators took part in the development of that rule. That means, nuclear power plants started to improve their physical protection system before it was required. During this 11 years, CSN has been performing annual security inspections and has been getting information from the findings and best practices observed in the Spanish nuclear facilities. This continuous evaluations and the good attitude of operators in order to better their physical protection systems have achieved a high level in this field. Nuclear Plants have gone further than it has required, in other words, there is a good security culture set up. This paper shows, without giving names and sensible details, some examples of the best practices accomplished by the Spanish Nuclear Power Plants in different areas of nuclear security: • Regarding physical barriers, the CSN security regulation requires categorizing the site in 3 areas: Owner Control Area (OCA), Protected Area (PA) and Vital Areas. The PA must have double fence with intrusion detection systems and TV cameras. There is a nuclear operator which accomplishing that requirement, has installed another double fence with sensors and cameras, of course is larger because is in between the OCS and PA.

Regarding Intrusion Detection Systems, there is a large variety of sensors and technology and operators have more than it is required following the Defense in Depht philosophy. But there is no doubt that the vehicle entrance to the PA is something a weak point. In order to detect people hidden in big trucks two operator have using a Heartbeat Sensor, this is a sort of wires connected to several parts of the vehicle and could read that movement. • The control access of materials is sometimes difficult, especially during refueling periods when there are a lot of vehicles getting into the PA, nuclear operators have sniffing dog to detect explosives hidden in any part of the truck.

Responding in case of threat must be very quick, there are some operators who have electric motorcycles in the site, and so guards can patrol and arrive to several places very fast. • Training and exercises is one of the key factors to minimize the human error and also to be successful in this strategic area. There is a close and very good relationship between Police Forces and Nuclear Security Guards, so Police often come to the facilities to perform joined exercises, and guards also go the Police

facilities to be trained. There is a very good connection. • Security management is probably one of the best important security functions. There are several best practices about this issue. One of them is the Annual Security Problems ad Resolutions Report. The operators are tracking all the failures in any of the components or equipment of the physical protection systems, and afterwards they can perform statistics and evaluation, so they can get very useful trends, conclusions and effective performance information. • Security Culture is one of those indicators which can tell how well a nuclear facility works. There are several examples about it: you can wall down in the nuclear sites and have a look to the Access Control processes seeing all the workers obeying the rules and passing through the portal detectors, using their badges, swiping their cards, guards performing their responsibilities, searching the vehicles, patrolling the site and the managers always involved and encouraging the staff.

Synopsis ID: [149]

A Comprehensive Study on the Physical Protection of BAEC TRIGA Research Reactor and Status of Nuclear Material Accountancy and Control in the Facility

Shohag, M.[1]

[1] BAEC, Bangladesh

Corresponding Speaker: M. Shohag

BAEC TRIGA Research Reactor (BTRR) is the only research reactor in Bangladesh. The reactor has been used in various fields of research and utilization, such as, neutron activation analysis (NAA), neutron radiography, neutron scattering experiments, radioisotopes production, manpower training, education, etc. since its commissioning. It is a tank type research reactor and achieved its first criticality in the morning of September 14, 1986. With the vision for the safe and secure operation of the research reactor facility, the state has a strong policy, planning and implementation in the field of physical protection as well as material accountancy and control. Present physical protection of the facility has been designed and implemented based on the probable threat assessment following the guidelines of International Atomic Energy Agency (IAEA). The state's security regime addressed the protection of persons, property, society and the environment from any malicious act. The paper highlights on the current threat assessment, detection, delay & response elements and features of the existing physical protection system, safety & security culture, good practices and weakness of the facility as well as nuclear material accountancy and control procedures. A detailed strength (S), weakness (W), Opportunity (O) and Threat (T) analysis matrix has been developed and depicted in this literature. The paper also describes about the implementation of defense in depth design, contingency and emergency planning and computer security for protecting confidential information. It also discuss about the state of the art technology and procedures used in the facility. Beside these Bangladesh establishes an independent and sole competent authority named Bangladesh Atomic Energy Regulatory Authority (BAERA) which is responsible for the implementation of the legislative and regulatory framework, and is provided with adequate authority, competence and financial and human resources to fulfil its assigned responsibilities. The regulatory authority formulates all the rules and regulations to have a strong physical protection regime in the country following IAEA guidelines. A brief description is included about the activities of the regulatory body for proper implementation and ensuring physical protection of the facility. Manpower development through training on physical protection and material accountancy & control is one of the key parameters for ensuring security of the facility and develop state's security regime. The future plan and needs are described in brief considering facility need, human resource development, quality assurance and others. International cooperation is very much needed to implement the future plan for upgrading the physical protection system & procedures in the facility to ensure secure and safe

operation of the research reactor. Bangladesh is committed for peaceful uses of nuclear energy. The Government also has firm commitment for implementation of nuclear power program in the country. In the light of the vision of the country it has signed all International Treaties/Agreements/Protocols in this connection. All the confidential reports and agreed information submit routinely and timely to the IAEA through authentic established channel. Bangladesh has entered into the IAEA's Integrated Safeguards (IS) system on 01 January 2007 based on the declaration in completeness and correctness of safeguards and additional protocol reports of Bangladesh. This is the commitment to the international community for peaceful uses of nuclear energy.

Synopsis ID: [219]

Nuclear Security during the Decommissioning of NPPs

Rduch, A.[1]

[1] GRS GmbH, Germany

Corresponding Speaker: A. Rduch

The German regulations governing the security of nuclear power plants (NPPs) are highly specific regarding the nuclear security of NPPs in operation. On the basis of the general nuclear security objectives and special nuclear security objectives for individual types of installations, nuclear security requirements were derived and nuclear security measures specified to fulfil these requirements. For the nuclear security of NPPs that are in decommissioning and being dismantled, the regulations refer only to the specifications made for NPPs in operation.

Since the decision to phase out the use of nuclear power for electricity production, there have been many simultaneous decommissioning projects at the same time or several overlapping ones within a short period of time. To guarantee a sufficiently high and also uniform level of nuclear security in the different licensing proceedings which are carried out under the responsibility of different authorities, a standardised method was agreed on.

Compared with the level of nuclear security applied to NPPs in operation a graded approach for the determination of the necessary level of nuclear security and for typical stages of the remaining hazard potential is possible and expedient. Using a standardised systematic approach, these stages are analysed specifically for each installation.

The systematic nuclear security analysis is nuclear-security-objectives-oriented and based on fundamental nuclear security requirements: 19 fundamental so-called nuclear security functions that have been defined for NPPs in operating mode. As concerns decommissioning and dismantling, it was extrapolated whether and under what conditions reduced nuclear security requirements are permissible. This depends amongst other things on the safety and security systems that are still needed, the structures to be protected, the possible impacts that are still relevant, the effectiveness of countermeasures, and the reliability of substituting and compensating measures. In the presentation, the 19 fundamental nuclear security requirements are shown and their relevance in connection with decommissioning and dismantling is assessed with regard to whether they have to be applied unrestricted or whether restricted application is possible under plant-specific aspects or only after an analysis and demonstration that the nuclear security objectives are fulfilled. For reduced nuclear security requirements it is then possible to adapt the deterministic specifications of nuclear security measures made for NPPS in operation. When modifying individual nuclear security measures, it is always the entire nuclear security concept that has to be considered; hence a systematic analysis has to be carried out as a basis.

Deficits of a physical protection system revealed during a periodic systematic analysis of the nuclear security status that could not be rectified until decommissioning are also subject for a nuclear-security-objectives-oriented approach. Criteria for decision are e. g. the security relevance of the backfitting measures and the time needed for their implementation in relation to the reduction of the hazard potential. The presentation gives typical examples of graded backfitting measures, compensating measures or essential measures to be additionally installed.

Synopsis ID: [174]

Lessons Learned Regarding Physical Protection System at VVR-S Nuclear Research from IFIN-HH to Implement Preparatory Measure for Loading HEU and LEU Nuclear Spent Nuclear Fuel Assemblies, Loading Activities and Shipments by Road and Air from Romania to Russian Federation

Dragusin, M.[1], Repanovici, S.[2]

[1] National Institute for R&D in Physics and Nuclear Engineering-Horia Hulubei-IFIN-HH, Romania

[2] National Commission for Nuclear Activities Control, Romania

Corresponding Speaker: M. Dragusin

The nuclear research reactor VVR-S from National Institute for Research and Development in Physics and Nuclear Engineering-Horia Hulubei-IFIN-HH was in operation from 1957 until 1997. The spent nuclear fuel assemblies (SNFA) resulted from this period LEU type EK-10 and HEU type S-36 were repatriated in the Russian Federation used multi modal shipment road-air road (IFIN-HH Magurele-Henry Coanda Otopeni Airport by road, Airport Otopeni-Bucharest-Airport KoltsovO-Ekaterinburg-Russian Federation by air and from KoltsovO airport to Radiochemical factory MAyak by road. Nuclear Safety Report for loading the SNFA in the transportation casks, nuclear security plan for loading area, security plan for transportation, plan for intervention in the nuclear and radiological emergency situation as well as for other threats (nuclear terrorism). The paper will highlighted the lessons learned from preparatory activities in the IFIN-HH until sending responsibilities and nuclear materials to reprezenatives from Mayak Factory from the Russain Federation on Koltsovo Airport Ekaterinburg.

Synopsis ID: [242]

Purpose and Content of Contingency Plans

Natha, R.[1]

[1] Sandia National Laboratories, Department of Energy, United States of America

Corresponding Speaker: R. Natha

Nuclear Security Series 13 (NSS-13) emphasizes the use and implementation of contingency plans as a fundamental principle in maintaining a State's nuclear security regime. This recommendation has been implemented in numerous countries, while others continue to struggle to define the components of a contingency plan. Per NSS-13, a contingency plan is "Predefined sets of actions for response to unauthorized acts indicative of attempted unauthorized removal or sabotage, including threats thereof, designed to effectively counter such acts." Contingency plan components can vary significantly due to regulatory requirements and/or site specifications. NSS-13 provides recommendations for using contingency plans however the draft implementing guide of NSS-13 currently does not provide a sample template for a contingency plan. In large part, this can be attributed to differences of opinion about the content requirements and breadth of contingency plans from nuclear security subject matter experts. Additionally, NSS-13 implies that contingency plans and emergency plans need to be integrated. It is important to note that contingency plans should focus on security-related events while emergency plans focus on safety-related events. With this interpretation, it is important to consider the physical security implications associated with contingency plans. Current nuclear and radioactive material recommendation documents, combined with a performance-based approach, could serve as foundation for contingency plan templates. The contingency plan should cover various information about the site and response measures. Sections in the contingency plan may include site information, layout, characteristics, vulnerable materials and facilities, and physical protection measures. Additionally, it is important to consider the on- and off-site response measures that are currently in place to support any malicious events. Emphasis should be placed on response teams (i.e., hazardous material), Nuclear Material Accountancy & Control, fire and medical response, and other offsite agencies. The involvement of additional agencies should occur as regulators deem their participation necessary as part of an integrated response strategy. The contingency plan can have a significant amount of information related to the site, so it is critical to consider information security, thereby ensuring the document's protection. A plan for information security must be in place and active before beginning any work on contingency plans, which ensures that only appropriate personnel are able to access certain components of the plan. Contingency plans are emphasized in NSS-13, specifically in revision 5 of the document. Coordination between the operator and regulator is key in determining the contents of contingency plans, addressing the needs of the operators while abiding by the State's laws and regulations. Contingency plan requirements should be flexible in order to effectively counter the threat at the facility.

Synopsis ID: [255]

Implementing a Nuclear Security Program in Argentina - A Policy at National Level

Terrado, C.[1]

[1] Nucleoelectrica Argentina, Argentina

Corresponding Speaker: C. Terrado

Argentina has an important nuclear program, started in 1950 with the creation of the National Atomic Energy Commission. At that time main activities were research and development oriented and, in time, after years of sustainable governmental support the nuclear field became an important technological cluster. Nowadays the integrated nuclear area has 3 nuclear power plants, 7 research reactors built in the country and 5 in foreign nations, 1 small modular reactor of Argentine design under construction, 3 atomic centers and factories that produce: fuel elements, heavy water and irradiation sources. Several facilities are spread over the whole national territory and radioactive sources are used in many medicine centers and industries.

Initially, all activities were concentrated in the National Atomic Energy Commission, but since 1994 the regulation has been in charge of the Nuclear Regulatory Authority, an independent governmental institution, while the operation and maintenance of the nuclear power plants is in the hands of Nucleoelectrica Argentina SA. Safety and security culture has always been a great concern for nuclear workers and authorities; the country has an excellent performance in these areas. Argentina has an active participation in every regional and international security meeting and organization, the CPPNM Amendment was signed in November 2011.

Argentina is a big country, with the 8th largest territory in the world, a land area of 1,068,302 square miles or 2,791,810 square kilometers, long borders on land, rivers and sea, a population of around 43 million people and vast areas with low density of population. These characteristics increase the difficulties for the detection of nuclear material or radioactive sources out of regulatory control, illicit trafficking or other security events.

Furthermore, Argentina is a federal country; it has 24 provinces with different governmental authorities, laws, agencies and security forces that take action when a security event occurs. The coordination among personnel and institutions that would need to be trained to respond or participate in these kind of emergencies constitutes a significant challenge.

Over the last years nuclear security concerns rose because of the increasing threat of international terrorism; in that sense Argentina is working to strength all measures and procedures to diminish vulnerabilities and risk.

In this regard during the present year a specific inter-ministerial committee started a process to implement a Nuclear Security Program at the national level. It will allow the coordination among the different national institutions that have participation through a security event.

With the new governmental period in 2015, the Under Secretary of Nuclear Energy was created, which coordinates policies and activities in the nuclear area and is in charge of the implementation of this security program.

The implementation of the Nuclear Security Program will be finished at the end of this year and will establish, among others, these main issues:

Responsibilities of each participating institution

Procedures to follow among institutions for threats assessment

Coordination and upgrade of procedures to follow in case of a nuclear/radioactive emergency

Responsibilities and coordination for mitigation activities

Health services coordination and availability

Maintenance and improvement of the program through periodic evaluation through tests and exercises

Responsibilities with the regional and international communication and cooperation The paper will present:

Description and explanation of the main issues developed under the program.

The methodology applied to implement the Nuclear Security Program at the National Level.

The difficulties detected to deal with so many different organizations at national and provincial level in interior and border scenarios.

The specific issues considered because of the different actors involved, scientific, medical, security forces, media people, each of them with particular background, knowledge, language and behavior.

The difficulties found in consolidating emergency team integration.

The experiences collected and the results obtained from the work performed.

Synopsis ID: [144]

Emergency Response Contingency Measures to Respond to Unauthorized Removal of Radiological/Nuclear Material in a Nuclear Security Event

Maurer, R.[1], Buntman, S.[1], Butler, J.[1]

[1] Department of Energy, United States of America

Corresponding Speaker: R. Maurer

In a Nuclear Security Event involving the unauthorized removal of radioactive material, the radioactive material could be used in a criminal act or nuclear/radiological terrorism. Radiological or nuclear material out of regulatory control is of great concern throughout the world, and significant international cooperation has been focused on securing borders from trans-national shipments of illicit materials, especially radiological materials. From the technology perspective, these efforts have provided radiation portal monitors and trained personnel to detect, interdict, adjudicate, and recover illicit radioactive material being smuggled through international gateways such as shipping ports, land borders (pedestrian, vehicle and train conveyances), and airports. A Nuclear Security Event may be initiated by a security force or law enforcement response to a security alarm or a physical barrier penetration; but it can quickly turn into a radiological incident with national and international consequences.

Radiological emergency response operations to search for, locate, identify, and recover illicit radioactive material can be complex, requiring technical cooperation between Competent Authority technical specialists and law enforcement security experts. Trained experts with specialized radiation detection and radioactive material identification instruments are required to conduct these emergency response operations. Countries may become overwhelmed and require supplemental assistance from the international community. International assistance is available through the International Atomic Energy Agency (IAEA) Response and Assistance Network (RANET), bilateral/multilateral cooperation agreements, regional partnerships, and international agencies to support Contingency Planning and Preparedness for Response to Nuclear Security Events (IAEA Nuclear Security Series No. 13, Fundamental Principle K). This assistance can aid in ensuring the public is safe and the radioactive material subject to unauthorized removal is recovered and secured.

The U.S. Department of Energy/National Nuclear Security Administration's (DOE/NNSA) Office of Nuclear Incident Policy and Cooperation works with international partners to provide technical advice, analysis and interpretation of radiological data, medical consultation for radiation injuries, and emergency response capabilities to assist with the safe and secure recovery of radiological/nuclear

material in a Nuclear Security Event. From these efforts, DOE/NNSA has experience linking Security Contingency Plans to Emergency Response Plans and will share the experiences and lessons learned.

Synopsis ID: [32]

Preparedness, Readiness and Interoperability of Contingency Forces to Counter an Incident of Nuclear Security

Romao, C.[1]

[1] System for the Protection of the Brazilian Nuclear Program, Brazil

Corresponding Speaker: C. Romao

The purpose of this work is to demonstrate the importance of jointly training the operator Response Forces and the State Contingency Forces that are assigned to prevent theft of nuclear material or prevent sabotage of nuclear facilities. Preparedness, Readiness and Interoperability are training attributes of any security forces. For the effectiveness of this kind of training, it must be taken into account that Response Forces and State Contingency Forces must be ready to be employed according to a minimal standard of performance, against a Design Basis Threat (DBT) in any time and in any moment. If the capabilities of the adversary are superior to the Operator Response Force, this Force must be immediately able to be reinforced by a State Contingency Force in order to defeat the threat. On the other hand the State Contingency Force must be in a condition to promptly support the operator Response Force once it is clear that the threat has superior capabilities and may cause unacceptable radiological consequences with its actions. This operation requires a previous division of responsibility between the State and the operator to define the capabilities the State should dispense in order to complement the nuclear facility security. The division of responsibility should happen once a DBT is developed by the State. This agreement will trigger a joint reinforcement operation between the operator Response Force and the State Contingency Force. The paper will show that this reinforcement should happen appropriately without delays and without harming the war principles of "unity of command" and "unity of effort". Principles of war are concepts that support the organization, training and employment of Forces. Both forces should fight the threat using the same doctrine of employment, bearing in mind that interoperability is most achieved when the "simplicity" war principle is the basis of this joint action. The Amended Convention on Physical Protection of Nuclear Material of July 2005 mentions the Fundamental Principle "K" which deals Contingency 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 holder. The research discuss the implementation of a Contingency Plan regulating actions based on realistic training with focus on a credible scenario and integrated and complemented by a State Contingency Plan. This integration is feasible if a common Preparedness and Evaluation System is established in the State, with focus on arrangements and protocols among competent authorities and operators, culminating the training with a Force on Force exercise. This exercise should use the threat characteristics resulted from a State DBT development. The research also emphasizes the importance of a State Nuclear Security Training Program to build the desired capabilities of Response and State

Contingency Forces. The Program is related to Preparedness, which involves Contingency Planning, organizing, training, equipping, exercising, evaluating and corrective actions to be taken. The Program should describe training objectives to be achieved, the training cycle in a year, the drills and exercises, a common evaluating system and the training budget available in each fiscal year. This Program should be followed by the State Contingency Force and all Operator Response Forces. This will provide the State and the operator an assurance of the level of the Readiness of each Force.

Key Words: Preparedness, Contingency Forces, Interoperability

Synopsis ID: [128]

When Protection Measures Fail – Health Physics Support of Medical Response

Sugarman, S.[1]

[1] Oak Ridge Institute for Science and Education, United States of America

Corresponding Speaker: S. Sugarman

When measures being used to safeguard radioactive sources fail there is potential for people to receive medically significant radiation doses. Responding to these situations can become quite complicated and it can be easy to lose sight of the immediate goal. Regulatory reporting requirements related to lost or stolen sources must be considered. In incidents when a large population is affected, epidemiological data associated with long term risk will be of concern. Interface with security/investigational personnel may require health physics assistance. The health physicist must be able to quickly evaluate a situation from various perspectives, taking into account unknowns and other variables, and translate the radiological information into information that is usable to the requesting organization. However, the first step is simply to gather enough information to ensure initial decision-making can be performed quickly and effectively. One of the roles of the Radiation Emergency Assistance Center/Training Site (REAC/TS) is to provide advice and consultation to healthcare and health physics personnel tasked with responding to a radiological incident. It is often the case that there is not enough information available early in the incident to provide precise radiation exposure information or to accurately determine internal contamination levels. Therefore, it is necessary that health physics personnel are able to assess the situation and estimate the magnitude of the potential radiation doses so that early medical decisions, and other triage decisions, can be made. In nearly all cases it is not necessary to have precise dose calculations performed in order for healthcare providers to begin initial treatment and medical assessment. As additional information becomes available, the initial dose magnitude estimations can be refined into more precise dose projections. An awareness of available tools and an understanding of the needs of the medical staff are necessary for early health physics support of the healthcare personnel treating patients involved in a radiation incident.

Synopsis ID: [94]

Systematic Aspects of Designing Effective Physical Protection Systems of Russian Nuclear Facilities

Izmaylov, A.[1]

[1] JSC "Federal Centre Of Science And High Technologies "SNPO "ELERON", Russian Federation

Corresponding Speaker: A. Izmaylov

Development and upgrading Physical Protection Systems (PPS) of Russian Nuclear Facilities (NF) are high priority tasks for providing nuclear technologies security. Noted, that PPS is a complex "man-machine" system and its analysis and design require a scientific approach. Herewith we should take into account a correlation of PPS subsystems (technical security equipment, physical barriers, guard forces etc.), and also their interconnection with related safety and security systems (technological safety, nuclear material accounting and control, cyber security, etc.). The paper will highlight effective PPS development based on systematic approach. Special attention devoted to influence of the Design Basis Threat (DBT) accepted for specific NF on technical and organizational decisions. Also, this paper underlines an importance of cohesive legal and regulatory documents on physical protection development for all stages of PPS lifecycle (development, implementation and operation). This is mostly important for pre-design stage when main design solutions have to be developed based on analyzing and justification of PPS structure and composition. State Corporation "Rosatom" developed a methodology of Nuclear Facilities vulnerability analysis, PPS effectiveness evaluation, and conceptual designing. Appropriate computer programs developed for this purposes are described briefly. Physical protection personnel education, training and professional development performs in "Rosatom" training centers and Russian universities (National Research Nuclear University "MEPHI" etc.). PPS monitoring system developed by "Rosatom" allows to determine the most relevant areas to distribute funds (material and human resources). Russian systematic design methodology described in the paper complies with corresponding approach used by International Atomic Energy Agency (IAEA). Russian PPS systematic analysis experts take active part in IAEA activities (Coordinated Research Project NUSAM et al). Key words: nuclear site, physical protection system, system analysis, IAEA, legal and regulatory documents.

Synopsis ID: [63]

A New Generation of Active Intrusion Detection System for Physical Protection

Yuan, Z.[1], Chen, H.[1], Jing, Y.[1]

[1] Shanghai Nuclear Engineering Research & Design Institute, China

Corresponding Speaker: Z. Yuan

In this paper, we intend to present a new detection system based on millimeter wave radar. Using this technique, we can detect, locate and track multiple intruders on a electric map using virtual perimeter. We believe this technique would be a great improvement for intrusion detection.

The millimeter wave radar is a radio distance measuring equipment, which emits electromagnetic wave on the target and receives the echo, thus obtaining information including distance, position, height, velocity, etc. The millimeter wave radar detection system consists of the radar component, processing server and video assessment equipment. The radar component is about the size of a dome camera, installed on a standing pole of 3~10m high. The radar can locate every object within a range of 1.5km with the precision about 30cm, while the traditional intrusion detection system can only work within the isolation zone. The physical barrier is not necessary which can be defined virtually on the electric map. The millimeter wave radar can retrieve various features about the behavior of the detected objects, including velocity, intensity, position, etc, allowing it to process with more information to identify alarms not caused by real intrusion such as birds or other small animals. On the other hand, it can discover suspicious activity such as lingering near the protection area, or over speed vehicles, while traditional detection system is blind beyond the isolation zone. The radar detection system also has positioning function allowing the operator in CAS to track the intruder, which will greatly facilitate the response force. The construction of the millimeter wave radar detection system is also significantly easier. It requires several standing poles and connecting cables. During extreme condition, it can even be deployed immediately using battery and wireless network.

A typical applicable scenario for the millimeter wave radar is open area, such as water, or material storage yard. The convenience of installation makes it very suitable for temporary barrier or as a complimentary detection method for traditional detection system. We believe it can also be used against airborne attack, which has become an increasingly threat since remote controlled drone is now a commercialized product.

There is defect for the millimeter wave radar detection system. The millimeter wave can penetrate through fog, smoke, dust, but the signal will attune significantly in heavy rain, which will lead to decrease of detection range. Besides, the sight line between radar and the target object cannot be blocked, so it cannot be used for interior detection.

Except for the several defects existed, we believe the millimeter wave radar detection is a great improvement for intrusion detection. Traditional intrusion detection system must be installed in an area isolated by physical barrier. It can only provide passive protection that an alarm will be triggered only when someone enters the isolation zone. The 1st generation of intrusion detection system (e.g. Infrared beam) detects intruder based on the existence of signal. It is easy to bypass or compromise. The 2nd generation of intrusion detection system (e.g. microwave, electric field) involves complicated signal processing, which provides much higher reliability. However, false alarm is almost inevitable during extreme weather. We believe the 3rd generation of intrusion detection system should introduce more features to identify the actions of intruders. Besides achieving high detection rate, low false alarm rate and inference resistance, it should also have the following features: target identification; trajectory tracking; behavior detection. And we believe the millimeter wave detection system as a new generation of detection system has a very promising prospect.

Synopsis ID: [117]

Radioactive Waste Monitoring: Opportunities from New Technologies

Finocchiaro, P.[1], Ripani, M.[1]

[1] Istituto Nazionale di Fisica Nucleare - Laboratori Nazionali del Sud, Italy

Corresponding Speaker: P. Finocchiaro

Nowadays new technologies allow the development of low-cost systems capable of monitoring the radioactivity coming out of (spent) nuclear fuel casks or radwaste drums. In particular simple, compact and effective radiation counters were developed at INFN for the detection of gamma rays and neutrons. In the framework of the protection against unauthorized removal of nuclear material during use, storage and transport and against the sabotage of nuclear material and nuclear facilities during use, storage and transport, one can think of installing a set of such detectors on the casks containing nuclear materials. The initially measured counting rates would be the reference values to be checked throughout the transport operations and eventually during the interim storage. Any change in counting rates, or even a sensor blackout, should be immediately interpreted as a possible safety or security breach. In particular the gamma ray sensor exploits scintillating optical fibers and silicon photomultipliers, whereas the neutron sensor is based on 6Li as converter and silicon diodes to detect the capture products. Both devices can be interconnected via cables and/or wirless links to a computer system where a powerful console and a database can store all the information coming from the distributed sensor network, being able to interpret the data and to generate warnings or alarms if needed. The two kinds of sensors have been thoroughly tested with laboratory sources, and in particular the neutron sensor was also calibrated at an international metrology institute (PTB) in a certified neutron field. Field tests were also performed in a radwaste storage site and others are planned in the near future. Moreover, a device initially developed for particle physics research was converted into a powerful tool to inspect the (spent) nuclear fuel casks by means of the muon tomography technique. It makes use of the natural cosmic radiation as probe and two large plane detectors to reconstruct a 3D density profile of a cask and its content. The techniques and their possible applications in the field will be discussed in detail.

Synopsis ID: [139]

The Impact on Nuclear Security by the Development of Unmanned Aerial Vehicle Technology

Hu, H.[1], Liu, W.[1], Liu, X.[1]

[1] State Nuclear Security Technology Center (SNSTC), China

Corresponding Speaker: H. Hu

With the continuous progress of science and technology, UAV (Unmanned Aerial Vehicle) technology characterized by "low, small and slow" has been greatly developed, and has been gradually popularized and applied in industries and other related areas. UAV brings convenience for people's life and work, but also has certain impacts on the security of some related industries. With the aim to prevent terrorists from sabotaging nuclear facilities and/or unauthorized removing nuclear and other radioactive materials, nuclear security plays an important role in ensuring the safety and security of nuclear and other radioactive materials, nuclear facilities and and related activities. With the rapid development of UAV technology, how to prevent terrorists from using UAV to sabotage nuclear facilities, and how to improve the protection level of by using UAV technology, is a new issue in the field of nuclear security. In this paper the potential threat to the security of nuclear facilities is analyzed, according to the development and application of UAV. In addition, technical characteristics of UAVs and the current status of UAV defense technology are analyzed. At last, the development ideas and suggestions for nuclear security to deal with UAV issues are put forward, from both the defense and application aspects.

Synopsis ID: [80]

The U.S. Department of Energy's Use of Performance Testing to Evaluate the Effectiveness of Physical Security Systems

Brooks, M.[1], Hojnacke, M.[1], Sandoval, J.[2]

[1] U.S. Department of Energy

[2] U.S. Department of Energy, Sandia National Laboratories

Corresponding Speaker: M. Brooks

Fundamental Principle J in the amendment to the CPPNM outlines that 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. The U.S. Department of Energy (DOE) Safeguards and Security (S&S) Program incorporates a risk-based approach to protect assets and activities against the consequences of attempted theft, diversion, terrorist attack, industrial sabotage, radiological sabotage, chemical sabotage, biological sabotage, espionage, unauthorized access, compromise, and other acts that may have an adverse impact on national security or the environment or that may pose significant danger to the health and safety of DOE employees or the public. The implementation of a graded physical protection program must be systematically planned, executed, evaluated, and documented as described in the site/facility security plan. Physical protection programs must be based on the most recent DOE Design Threat Basis (DBT) policy in conjunction with local threat guidance. DOE employs the concept of Essential Elements (EEs), which is defined as protection and assurance elements necessary for the overall success of the S&S program at a DOE facility or site, the failure of any one of which would result in protection effectiveness being significantly reduced or which would require performance of other elements to be significantly better than expected in order to mitigate the failure. EEs can include but are not limited to equipment, procedures, and personnel.

EEs must be periodically tested to verify their continued functionality, operability, effectiveness, and/or performance. Testing frequency may be based as applicable on manufacturer's recommendations, consensus standards, facility-/site-specific conditions and operational needs, or other criteria that will ensure program effectiveness. Testing of elements that are not prone to failure and that are not subject to compromise without noticeable tampering, such as walls and fences, is not required as long as it can be documented that tampering with such elements would be detected in time to prevent compromise of overall protection.

One means of verifying the effectiveness of an EE is through a Performance Test (PT). A PT is defined as a test to evaluate the ability of an implemented and operating system element or total system to

meet an established requirement. PTs must be used to realistically evaluate and verify the effectiveness of EEs to identify needed training and provide training for personnel, identify areas requiring system improvements, validate implemented improvements, and motivate personnel. Such tests must adhere to the requirements found in DOE security policy.

DOE intrusion detection and assessment systems, system components, and EEs must be performance tested at a documented frequency. The testing program for systems and system components must be developed and implemented in developed security planning documents. PTs must be conducted to validate system effectiveness. The DOE DBT policy prescribes performance metrics (adversary capabilities, baseline scenarios, and system effectiveness requirements) used to determine acceptable system effectiveness levels. Metrics are used to determine high, moderate, and low system effectiveness.

The PT must be conducted to determine the proper settings for high detection rates with the lowest possible nuisance alarm rates. Tests must be performed along credible pathways with a low profile target (crawling) and a higher velocity and profile targets (walking, running, fast crawl, rolling) or as appropriate given space considerations for interior applications. If assessment is by fixed closed circuit television, the PT must be conducted under the lowest lighting conditions that are routinely available. The testing must be conducted against the worst case "light to dark ratio" to determine if shadows or dark spots in the field of view degrade assessment viability. PTs must ensure that the alarm communication line or data link is capable of transmitting an alarm signal and that it has not been compromised. The intrusion detection system must be designed, installed, operated, and maintained to ensure that the number of false and nuisance alarms do not reduce system effectiveness.

Synopsis ID: [134]

Physical Protection Measures and System

Lavia, F.[1]

[1] Nucleoelectrica Argentina S.A.

Corresponding Speaker: F. Lavia

PHYSICAL PROTECTION SYSTEM INDICATORS

DETERMINE THE DAILY SITUATION OF PHYSICAL PROTECTION SYSTEM (SPF) PURPOSE: The operational status / degree of efficiency of the SPF must be determined daily. That status/ situation will be indicated through 3 alternatives shown by a color (red, yellow and green). This status will lead to measures, which are defined below.

INDICATORS 1) Measure EFFICIENCY of the Physical Protection System 2) Physical Protection Daily form A set form with fixed factors / associated number (to quantify) To be completed daily. Form indicating SPF status. The synthesis of the data must be translated into 3 colours:

Where,

GREEN INDICATES THAT THERE IS PHYSICAL SAFETY

YELLOW INDICATES TAKE CAUTION/CORRECTIVE OR PREVENTIVE MEA- SURES and be specially /particularly/ specifically/ alert. There are moderately vulnerable factors that endanger Physical Protection if short /medium term measures are not taken. It also implies Alert the Safety Sub-Manager and the RESPONSE FORCE.

RED INDICATES THAT THE SITE DOES NOT HAVE PHYSICAL PROTECTION AND IS TOTALLY VULNERABLE. Immediate measures must be taken; the whole Organization must be alert, as well as the Site Management, the NUCLEAR REGULATORY AUTHORITY and the Company's (NASA) Board. Electronic systems should be reinforced with HUMAN RESOURCES, especially with RESPONSE FORCE: NATIONAL MILITARY POLICE AND ARGENTINE COAST GUARD.

Each indicator must be CLASSIFIED according to its specific weight within the Comprehensive System of Physical Protection, i.e., its relative importance within the System should be weighed. Following the same criterion within the same indicator, its characteristics should be weighed, among them: 4) WEIGHT: 1-5 5) OPERATIONAL%: from 0 to 100.

METHOD TO DETERMINE THE STATUS: The procedure/method to determine the Status will be carried out by filling in several forms. For each complete indicator (units/ distances/ sectors/ etc.) =

100 % Established by each indicator the operational or non- operational percentage and their weight, how the state of the Physical Protection System is influenced should be determined. The general operational status of the SPF, green, yellow or red will be determined as follows: a) By the sum of the status of each indicator, that is, it will be the result of the addition of each indicator. b) The status of each indicator, (green, yellow or red) will depend on: 1.- Weight 2.- Operational %

FORMS These are the forms that should be completed:

a. SYSTEM OF BARRIERS OF PHYSICAL PROTECTION b. PERIODIC CONTROL OF BARRIERS, EQUIPMENT AND SYSTEMS c. TRAINING NEW PHYSICAL PROTECTION STAFF d. SIMULACRUMS/TRAINING DRILLS e. PERFORMANCE AND EFFICIENCY OF THE PHYSICAL PROTECTION SYSTEM

Synopsis ID: [57]

Developing and Sustaining the Physical Protection for Nuclear Facilities through Application of Nuclear Security Management System

Prabandari, Y.[1]

[1] National Nuclear Energy Agency of Indonesia (BATAN), Jakarta, Indonesia

Corresponding Speaker: Y. Prabandari

Currently, the nuclear research has been developed and implemented in many countries. Not only can be used in various fields, nuclear technology can also be misused for malicious purposes. In addition to the issue of nuclear safety, the issue of nuclear security also can become an obstacle in the use of nuclear, especially in developing countries that have a nuclear power plant construction program. Physical protection system is an important part of nuclear security. IAEA as an international organization that oversees nuclear utilization has published the Nuclear Security Fundamentals; Recommendations; Implementing Guides; and Technical Guidance specifically related to physical protection. INFCIRC/225/Revision 5 states that "Quality assurance is one of elements of a state's physical protection regime for nuclear material and nuclear facilities". Therefore, BATAN as a nuclear research institute in Indonesia has developed a management standard that allows an organization establish a comprehensive nuclear security management systems (NSMS). This standard is one of the tools to build a security system in the scope of the nuclear facilities in terms of quality assurance. This standard requires organizations to assess security risks in the scope of work, ensuring that security measures have been carried out to meet the requirements of regulatory bodies and legislation related. Each element of NSMS prepared by the methodology Plan-Do-Check-Act (PDCA). PDCA approach encourages organizations to manage nuclear security management system in stages starting from the identification of the requirements of regulatory agencies and other regulations until the evaluation phase as well as proactive measures for continuous improvement. These processes are done to build a nuclear security management system holistically, including how to manage physical protection for nuclear facilities. BATAN provides nuclear security certification as evidence that the organization/ work unit in BATAN has met and implemented the NSMS requirements. Certification is provided through performance audits conducted by Center for Nuclear Standardization and Quality (PSMN BATAN). Audits are conducted on the basis of document completeness and audit of field to determine compliance with requirements. The scope of the audit that has been done is still limited to the function of the nuclear security unit in BATAN, especially the implementation of regulation, guarding, escort, and patrolling. The nuclear security unit is one part of the physical protection system that has the task of safeguarding nuclear installations, and the environment. Currently, the certification of NSMS is still within the scope of the function of the nuclear security

unit, and along with the stabilization of implementation of NSMS is expected that the scope of its certification will increase. The successful implementation of NSMS is largely determined by personnel awareness and support of top management. Therefore, the efforts to build awareness of personnel should also be performed. In conclusion, physical protection systems can be built and managed by implementing nuclear security management systems. NSMS provide opportunities for the development and continuous improvement through measurement, process monitoring, and management review.

Synopsis ID: [292]

Global Approach to the Security of Nuclear Installations and Management of Their Security Level

Desvergnes, G.[1]

[1] Assystem, France

Corresponding Speaker: G. Desvergnes

Faced with the increase of multi-form threats connected mainly to terrorism, the protection of critical installations and high value nuclear sites has to be the object of a global approach to take into account the various physical as well as logical vulnerabilities. This approach is reinforced when using new technologies that while bringing more performances also add complexity to their control and their security due to their connectivity with the outside world.

Thus the installation's risk analysis has to take into account the physical and human aspects to propose solutions which deal with physical protection, cyber defense and the fight against internal threats. This approach follows the principle of defense in-depth, the final objective being to ensure the installations security but also the continuity of the activities thanks to resilient systems.

The answer to this risk analysis is always a combination mixing detection and protection technologies as well as human procedures. In addition, it is also crucial to continuously check if the installation is still at its desired level of protection during its entire life cycle.

As the second largest private Nuclear Engineering firm worldwide, Assystem offers Long term maintenance and sustainability solutions to the nuclear industry, with a particular focus on security and monitoring systems' Long term operation (LTO) management for Nuclear Power Plants (NPPs). Since technological obsolescence can become a very important risk factor for an optimal continuity of operation, Assystem studies and implements maintenance strategies for these systems. Our industrial maintenance global approach has for objective to guarantee, on the long term, the systems performances regardless of the technological evolutions since the original design.

Principle of defense in-depth

Generally speaking, devices to be implemented lean on the defense in-depth concept with a design of increasingly sensitive zones and their application on any high value sites such as nuclear facilities.

Thereby, this concept means to :

Detect any risk of intrusion as early as possible,

Have physical protection systems intended to prevent and in any case to delay any intrusion in the sensitive zones,

Alert the quick response team in case of a real alarm (after necessary verifications) in a way that the time of intervention is compatible with the devices intended to delay,

In addition, discourage the intrusion attempts thanks to the visible reinforcement of the new protection system.

Focus on Nuclear facilities

According to the principle previously described, a zoning is defined according to the category and to the amount of materials present in the premises (Controlled-access zone; Zone with normal protection; Zone with reinforced protection; Internal zone; Vital zone; Storage or warehouse).

Security level management

Besides the global approach allowing to take into account the various links in the chain of components or sub-systems that are part of it, it is important to guarantee that the security level of the installation is maintained over time. Indeed, various factors can bring the security level to deteriorate during the installations life cycle like for instance: - Failure of one of the system's components, - "Zero Day" vulnerability, - New type of physical threat like overflights by unmanned aerial vehicles, - Exploitation of a security vulnerability not identified originally, - Failure of the system in case of simultaneous attacks, - To oversee a risky psychological behavior of an operator. . .

In conjunction with our global security approach, this abstract is also intended to present an innovative solution of management of the installation's global level of security based on a real-time software tool that automatically and manually collects data allowing to evaluate this level. The processed data take into account the physical security, the cybersecurity of the system and its environment, and the operating safety.

With this tool, the security level can be maintained to its nominal functioning range thanks to automatic mechanisms, but also procedures achieving maintenance of operational readiness for equipment and software and procedures for the preservation of security conditions for the cybersecurity part.

With our long term maintenance experience side by side with EDF, based on the lessons learned while maintaining various systems like for instance the plant's physical protection systems (video surveillance, anti-intrusion and access control), Assystem has developed and implemented its global approach to the security of the nuclear installations through a complete plant life management (PLM) programme.

Our PLM programme has been successfully implemented for more than 25 years throughout the 19 French NPPs all part of the second largest fleet in the world. We believe that our global security approach presentation during the 2017 IAEA International Conference on Physical Protection of Nuclear Material and Nuclear Facilities, would contribute effectively to the conference's objectives by sharing feedback and by showcasing our security software tool created to make sure the security level is always optimal as it always should be.

Synopsis ID: [244]

Improvements in Transportation Security Analysis from a Complex Risk Mitigation Framework for the Security of International Spent Nuclear Fuel Transportation

Williams, A.[1]

[1] Sandia National Laboratories, Department of Energy, United States of America

Corresponding Speaker: A. Williams

A recent study in managing the multi-modal and multi-jurisdictional risks related to the international transportation of spent nuclear fuel (SNF) describes a new framing of transportation security. This study argues that applying a complex risk mitigation framework built on the interdependence of security, safety and safeguards can improve the security design and analysis of transportation security analysis. More specifically, the concepts of hierarchy and emergence from complexity and systems theories are combined into a state-space description of complex risk and an analytic approach that enumerates its related hypothesized causal mechanisms. This complex risk approach enables decision makers to better conceptualize and contextualize how the SNF cask, though regarded as low risk in and of itself, might exhibit higher risk behaviors that challenge security along an international transportation route. This study also demonstrates that considering SNF transportation security as part of an integrated complex risk management framework provides higher fidelity assessments across two novel analysis techniques: dynamic probabilistic risk assessment (DPRA) and system theoretic process analysis (STPA). DPRA uses phenomenological models of system evolution and stochastic behavior to account for possible de- pendencies between failure events and provide a unified framework for predicting the distribution of security risk associated with international SNF transportation security. STPA uses complex, socio-technical system models (inclusive of organizational influences, environmental pressures and interdependence between components) and a top-down analytical process for linking specific design details (e.g., selection of security technologies or procedures) to support the overall system objectives of improving security (and overall complex risk mitigation) along an international SNF transportation route. The benefits of this complex risk framework were demonstrated against a set of hypothetical scenarios drawn from a wide range of publicly available reports and articles detailing SNF (specifically) and special nuclear material (SNM) transportation cases (more generally). The results of this study—which conclude that an integrated complex risk mitigation framework offers several benefits to reducing security vulnerabilities to international SNF shipments—seem expandable to improving transportation security analysis writ large. The ability of the complex risk framework to increase coordination between security, safeguards and safety (as well as mitigating conflicts that diminish security) in international SNF

transportation offers lessons to all other transportation of nuclear (and radiological) materials. Being able to include contextual influences, environmental pressures and interdependencies with safety (and safeguards)—whether international or domestic—helps identify solutions more aligned with the complex realities and potential real world hazards faced by transporting nuclear and radiological materials. Incorporating complexity and systems theories into a systems engineering framework for analyzing complex risk better addresses the non-traditional risk-related pressures and dynamics the challenge traditional transportation security analysis techniques—ultimately enabling the development of improved mitigation and management strategies to ensure the protection of nuclear and radiological materials against 21st century threats.

Synopsis ID: [103]

Arrangement of Physical Protection Actions during International Transport of Nuclear Material

Elabd, A.[1], Elhefnawy, O.[1]

[1] Egyptian Nuclear and Radiological Regulatory Authority (ENRRA),Egypt

Corresponding Speaker: A. Elabd

The transport of nuclear material around the world is an essential activity to suppot the application of nuclear technologies for electricity generation, medical and other applications. The recommendations were made in Chapter 6 of INFCIRC/225/Rev.5 for the requirements measures against unauthorized removal and sabotage of nuclear material during transport are not listed in the sequence in which they have to be implemented. So, the present paper introduces an arrangement of physical protection actions during international transport of nuclear material which could be taken into account by States, their competent authorities and shippers and/or carriers when planning, approving, operations, contingency plan, review and learning, based on the recommendations of INFCIRC/225/Rev.5 and the contents of the Convention on the Physical Protection of Nuclear Material (CPPNM) as follows:

– Requirements phase State or the competent regulator acting on its behalf should define the requirements for the physical protection of nuclear material in transit and incorporated into a transport security plan (TSP). In defining these requirements the State or competent regulator will take account of the recommendations of INFCIRC/225/Rev.5, State's obligations to comply with the requirements of the CPPNM and any commitments made by the State (either as a supplier or recipient) to protect nuclear material in accordance with the Nuclear Suppliers Group Guidelines (INFCIRC/254).

– Planning phase The planning of transportation is responsible by the owner of the nuclear material, in conjunction with the shipping facility, the receiving facility and any transport company to be used. A key aspect during the planning stage is to decide on a suitable point for the handover of physical protection responsibility from shipper to receiver and hence from one State to another. So, the plan will need to comply with the regulations and requirements of the sending State, and with the regulations and requirements of the receiving State and of other States which are transited. Also during the planning phase, the consignor/carrier/consignee and competent authority should ensure that all personnel involved in the transport arrangements and its security are suitably trained and qualified, commensurate with their roles and responsibilities. Recently, some organizations make use of independent experts that specialize in emergency planning and crisis management to help ensure that the exercises are managed effectively and with an experienced and independent perspective. In addition, there are various issues as safety and security interfaces need to be considered by the relevant parties during the planning phase and an agreement reached on the optimal arrangements.

– Approval phase The approval by the competent authority of the TSP should be based on a detailed examination of proposed physical protection measures, which should provide sufficient delay so that guards and/or response forces have time to intervene to prevent any malicious acts. Once the transport arrangements have been approved by the relevant authorities, the agreed physical protection measures adopted in the plan must be adhered to. If there are any reasons that the physical protection measures cannot be implemented in accordance with the plan, the carrier should implement mitigation measures and inform the relevant authorities as soon as possible.

– Operation phase Responsibility for monitoring the transport operation may belong to the carrier, or the escort commander, or both. The role of a Centre for monitoring and communication is extremely important and supports command and control decisions. The Centre should also have the capabilities, authority and understand the terms of engagement so to call on additional forces if required. Tracking of international transportations of differing commodities is now offered as a standard practice by many road/truck and maritime companies and all Category I/II shipments should be tracked using secured communications.

– Contingency plan phase Contingency plan should be developed for all anticipated scenarios and for as many situations as possible. The contingency plan should be built into exercises and training programmes and should be rehearsed and reviewed as many times as required. Within the contingency plan there should be performance indicators to assess if the required outcome is being achieved. Also, it is important to avoid gaps and overlaps in accountability between the various parties.

– Review and learning phase To assess the effectiveness of the security measures and continuous improvement, the plan should indicate the quantitative and qualitative evaluation processes which will allow for a timely identification of issues and recommendations for improved performancestandards. It is also important to assist States and operators that may be considering the need to ship such cargoes for the first time and where they lack experience. Also, there are lessons to be learnt from previous transports, operational experience and many other industries. The best practices can be best achieved through workshops, table-top exercises, best practice guides, and by coordination through nuclear related organizations such as the IAEA.

Synopsis ID: [295]

Cyber Security in Marine Nuclear Transport Systems

Burgul, R.[1]

[1] International Nuclear Services

Corresponding Speaker: R. Burgul

"If you spend more on coffee than on IT security, you will be hacked. What's more, you deserve to be hacked" [U+2015] Richard Clarke

The sheer volume of computer vulnerabilities, proficient cyber attackers, freely available hacking tools and lax organisations has seen the proliferation of cyber-attacks to unprecedented levels. What's more, the ingenuity of attackers has meant that not only are traditional IT systems (which provide common corporate services such as email and Word processing) at risk but increasingly, attacks on industrial control systems (ICS) which control industrial processes and associated equipment are becoming more and more prevalent.

This paper will detail the history of cyber-attacks generally and will then focus on attacks within the nuclear and marine sectors. The paper will look at the consequences of previous attacks and the potential consequences of future attacks and will show why the focus is changing from Confidentiality (attempts to gain access to information in an unauthorised manner, eg Edward Snowden) to Availability (attempts to deny access to information or systems to legitimate users, eg ransomware attacks).

The consequences of such attacks will be examined and this paper will posit some potential impacts on the global nuclear sector. In this way, the paper will show why it is important for nuclear organisations to take the cyber threat seriously. We can look at the consequences of other major events such as the BP oil spill and whilst that wasn't a cyber-attack, by juxtaposing, we can understand the consequences if we assume that it was a cyber-attack.

The paper will explain the work undertaken within International Nuclear Services to assess the vulnerability of our marine vessels to cyber-attack. Our vessels have multiple systems on board covering various systems such as engine management, chart display, GPS location and corporate services. INS's vulnerability analysis centred around key questions posed by INS stakeholders: Is it possible to create an Uncontrolled Radiological Release (URR) through a cyber-attack of an INS vessel? Is it possible to create operational difficulties through a cyber-attack of an INS vessel? Combined with other questions related to commercial resilience and business continuity, INS set out to answer the above in order to provide assurance to key stakeholders. This paper details INS's journey and posits simple approaches for other nuclear organisations to be able to provide similar assurance to their stakeholders.

Synopsis ID: [209]

Best Practices and Lessons Learned in LANL Approaches to Transportation Security

Drypolcher, K.[1], Abeyta, C.[1], Matzke, J.[1], Silva, M.[1]

[1] Los Alamos National Laboratory, Department of Energy, United States of America

Corresponding Speaker: K. Drypolcher

The International Threat Reduction group (NEN-3) at Los Alamos National Laboratory has a programmatic mission to identify, control, and recover disused sealed sources. These nuclear materials (NM) when removed from community access, reduce domestic and international threats that could result from the malicious use of such material. Permanent removal of NM requires the ability to transport the material securely and in a configuration that minimizes vulnerability during movement. Protection during transport starts with the identification of the nuclear materials and packaging configurations and does not end until the confirmation of secure storage at the destination has been verified.

During transportation of NM the risk of sabotage or theft is heightened due to the material being removed from the protection applied at its facility of origin. As the International Atomic Energy Agency points out, it is a fundamental principle that Member States should take appropriate measures within the framework of their national laws to establish and ensure the proper implementation of the State's physical protection regime. The challenges associated with protecting nuclear material from unauthorized removal and sabotage during transport are unique compared to when it is stored at nuclear facilities, and thus require a dedicated approach 1. Implementation of security for the transport of NM starts with the type and quantity of material to be transported. A graded approach is used to determine the security requirements for transportation. The security planning, physical protection and transportation plan for Nuclear Regulatory Commission (NRC) category quantities of material dictate the security requirements.

In addition to the U.S. Department of Transportation (DOT) and NRC requirements, our transport security must consider the Department of Energy requirements that also use a graded approach, taking into consideration the accountable material quantities and attractiveness levels. In order to ensure the physical protection of the NM in transit, we have adopted a defense in depth position that involves several layers and methods of protection as recommended by the IAEA. These defensive mechanisms are both administrative and engineered controls that address structural, technical, and personnel vulnerabilities. For transport of Category III NM quantities or higher transportation security, shipments utilize continuous and active monitoring systems, trustworthy (background vetted) and reliable drivers, notifications to sites and states, secure transport verification, delay elements such as a "stop box" within the transport vehicle, hardened locks and doors, and

transportation security plans. This paper will highlight through procedure changes, photos, and recent lessons learned, the steps NEN-3 has taken to ensure driver reliability, reduce insider threat, assess risks, and exceed the basic requirements for transport of nuclear material laid out in section 6.6 of the IAEA recommendations in INFCIRC 225 Revision 5. It is our hope that the lessons learned and best practices developed at Los Alamos National Laboratory and presented in this paper will provide an opportunity for others to compare their physical protection regimes and share experiences with the implementation of INFCIRC/225/Rev.5 in a way that furthers the tenets of the Convention on the Physical Protection of Nuclear Material (CPPNM).

1 IAEA Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5)

Synopsis ID: [99]

Tracking without GPS

Hocde, K.[1], Langlois, D.[1]

[1] IRSN, France

Corresponding Speaker: K. Hocde

The Institute of Radioprotection and Nuclear Safety (IRSN) is the technical support organization for the French Authority in charge of nuclear security in France and responsible of the tracking of nuclear materials transports on the French territory. IRSN conducts studies related to security of nuclear and other radioactive materials, nuclear facilities and transports.

In the field of the security of nuclear and other radioactive materials transports, the least is to track down the transport with reliability, robustness and accuracy. If well done, any unexpected change of speed or trajectory will be detected, and response forces will know by advance where to intervene. Among Global Navigation Satellite System (GNSS) technology, Global Positioning System (GPS) is the most developed and most used. GNSS is nowadays the only technology for tracking which is available 24/7 whatever the weather, cheap (GPS receptors can be bought for less than 100$) and can localize within 10 meters radius – as soon as you are on the surface of earth. This hegemony make it used in every tracking system, including those of sensitive materials transports.

However, new threats and new strike vectors are emerging in organized crime. More and more examples around the world come to show that sensitive transports should not rely only on GNSS. For instance, GPS jammers are developing. Today, it is possible for civilians to buy or even build quite easily a device that can blind any GPS receptor within a range of kilometers. The use of such devices in heists has now been proven. Moreover, a more pernicious tool is emerging: GPS spoofer. It is now possible, with civil technology, to deceive a receptor and make it think that it goes somewhere, at some time. A lot of scenarios of attack can be imagined with spoofers. They have in common the fact that – if GNSS only is used – it is impossible to know that the attack occurs. Accordingly to its missions, IRSN looks into the problem of receptor deceivers and study ways for navigation without GPS.

Other technologies of tracking exist or are developing. Despite none of those can nowadays outperform GNSS, a correct combination of such systems could track down or guide a transport in a GPS-denied environment. It exists two ways of tracking: absolute and relative. If absolute kind deducts the position from the distance to known coordinates, such as the satellites' ones for GNSS technology, relative kind calculates the position accordingly to a first one known and datas it collects as speed, magnetism, pressure, etc. New absolute tracking technologies flourish thanks, among others, to the Internet of Things. New waves, new protocols and new tags can now be found. Spoofing or even just jamming one of such plus one GNSS starts to be a tour de force. Relative

tracking technologies are also promising. In particular, thanks to the development of Unmanned Air Vehicles. Inertial units get better and lighter. Soon, it may be possible to navigate with the analysis of images taken by an on-board camera. This presentation investigates new technologies of tracking, both absolute and relative and beyond that the pairing of these ways. As a matter of fact, the correct combination of an absolute tracking system and a relative one could outpass the main traps used by deceivers, as one system would correct the weaknesses of the other.

Synopsis ID: [55]

Cyber Security Accidents and I&C Systems in Nuclear Power Plants

Kandil, M.[1]

[1] Nuclear and Radiological Regulatory Authority, ENRRA, Cairo, Egypt

Corresponding Speaker: M. Kandil

Abstract— New nuclear reactors being proposed to built with involve digital computers and communication system and network technologies which expanded recently in the I&C systems of nuclear power plants for both safety related and non-safety related. According to this expanded, cyber security concerns are increasing in nuclear facilities as in IT industries and other process industries. Some of the current nuclear facilities were not specifically designed and constructed to deal with the new threats, including targeted cyber attacks. Thus, newcomer countries must consider the Design Basis Threat (DBT) as one of the security fundamentals during design of physical and cyber protection systems of nuclear facilities. Moreover New nuclear power plants (NPPs) must have comprehensive cyber security measures integrated into their design, structure, and processes. In the absence of effective cyber security measures, the impact of nuclear security incidents can be severe. Many reports and standards are issued for cyber security in industrial control systems. Nuclear regulatory requirements based on the standards for industrial control systems have also been announced. However, it does not clearly indicate what I&C system roles and the cyber security features that should be considered to keep their functions necessary for a secure operation within the operation environment of NPPs in accordance with a secure process. In this paper, the important of the security of the digital and computers of I&C systems of nuclear power plants for achieving the safety of the plant. In addition, the cyber security issues for I&C systems in NPPs are presented and cyber physical frameworks to prevent the possibility of cyber security accidents.

Keywords- nuclear power plant, I&C, Control system, , cyber security, Safety and Non-safety related I&C Systems, Information security, the Design Basis Threat (DBT, Defence in depth.

Synopsis ID: [123]

Implementation of Computer Security Measures into Existing Physical Protection Strategies in Germany

Büttner, J.[1]

[1] Federal Ministry for the Environment, Nature Conservation, Building and Nuclear Safety, Germany

Corresponding Speaker: J. Büttner

In recent years, the number of software-based components in nuclear facilities is increasing. Therefore, nuclear security in terms of computer security becomes more and more a key factor. National regulations for nuclear computer security are urgently needed and take place in many states. Furthermore, the IAEA Nuclear Security Series is revised continuously in order to give proper recommendations to the Member States and to reflect best practices and lessons learned. This paper deals with the implementation of computer security aspects into established physical protection strategies in Germany. It will cover the current regulatory framework for nuclear security in Germany as well as planned guidelines in draft status and shows the implementation in a state with distinct federal structures. As Germany has up to now two separate DBTs, one for physical protection and one for computer security, advantages and possible disadvantages will be addressed.

Since 2013, in Germany the Cyber DBT is in force, last being reviewed in 2016. In the same year a guideline regarding computer security for nuclear installations handling with nuclear material of categories I and II was implemented. This guideline had several milestones to be fulfilled every year up to 2016. Now, the full guideline needs to be implemented in nuclear security regimes by above mentioned nuclear installations. Additional guidance is given by two explanatory notes for NPPs, and for interim storages, respectively.

Additional guidelines are in drafting status. For nuclear installations with nuclear material of category III a similar guideline to the above mentioned for categories I and II is currently developed. Lessons learned from the implementation of regulatory framework will be included. Second, a guideline for implementation of article 44b of the German Atomic Energy Act is being drafted. This article 44b regulates the need for reports to competent authorities in case of computer security incidents in nuclear installations. The guideline will give advice about triggers and procedures for reporting. The reporting system of the Atomic Energy Act is also influenced by reporting needs according for critical infrastructure in general in Germany. As NPPs are also critical infrastructure, a procedure combining both aspects had to be found.

The implementation of computer security regulation into existing physical protection strategies can be challenging. Many aspects have to be considered, not only form a security perspective, but also

from a safety one. Always, lessons learned from prior integration activities and from computer security incidents, which may occurred during the implementation process in other nuclear installations worldwide, should be integrated.

Synopsis ID: [126]

Physical, Corporative and Industrial Digital Security Convergence: Gaps to Close

Busquim E Silva, R.[1], Marques, R. [2], Cruz, J.[3], Piqueira, J. [3], Ferreira Marques, A.[4]

[1] Brazilian Government

[2] Polytechnic School of University of Sao Paulo

[3] Polytechnic School of University of Sao Paulo

[4] CTMSP

Corresponding Speaker: R. Busquim E Silva

Digital systems are extensively used in nuclear power plants (NPPs) and fuel cycle facilities (FCF) as part of the physical protection system (PPS) network, for data and information share/storage in corporative networks and as the heart of industrial control system (ICS). Although digital setups perform different functions according to its safety or security domain, their role in complex systems include acquisition, transmission, analysis, delivery and storage of essential data. Nowadays, ICS, corporative and PPS networks are not physically and logical integrated in general. Although there is a recent organizations consensus that cyber security extends beyond information technology (IT), NPPs and FCCs usually manage computer security in at least three spheres: at a security operation center for access and surveillance control; at an IT department (or similar) for corporative network; and at operational level for industrial instrumentation and control. However, cyber-attacks may compromise physical, corporative and ICS security and physical security attacks may compromise computer security - for the purpose of this article, computer security includes PPS & corporative network and all ICS. The facility physical security depends on a number of decisions identified through risk management process; IT has been carrying out threat assessments to design, deploy and implement corporate networks; and ICS safety systems have been designed based on risk evaluation. Nevertheless, all cyber security implementations (and regulations) must follow similar trends as physical and computer security are tied together because of the increasing use of the same of similar digital assets and the increasing complexity and connectivity of networks. At a technical level, the binary data, as transmitted throughout the PPS, ICS and IT networks, are the same. Nevertheless, decision makers at organizational level must guarantee that securing the data is as important as securing the facility and securing the ICS. Therefore, a single and skilled team must be responsible for procedures and policies for all ICS, IT and PPS networks. Another main issue that should be addressed by organizations is the distance between managers - who play an essential role in cyber decisions - and PPS, IT and ICS people

- who run the plant/systems and implement management decisions. The gap between IT, ICS people and general employees may be shorten by cyber security training courses and awareness, as well as by the adoption of integrated policies. To summarize, the design of all digital physical networks and computer security defenses must be shaped by engineering aspects towards a threat-informed security design in view of its influence on physical security, and single governance must be in charge of it. The gap among corporative, physical and industrial digital security must be closed and the simple analysis of the architecture design and application of security measures must be replaced for an iterative engineering evaluation based on risk management.

Synopsis ID: [239]

Deterring, Protective, Delaying and Detective Application Security Controls for Nuclear Facilities

Gupta, D.[1], Lou, X.[1], Waedt, K.[1], Lange, M.[2]

[1] AREVA GmbH, Germany

[2] Magdeburg-Stendal University of Applied Sciences, Germany

Corresponding Speaker: D. Gupta

All nuclear facilities have to comply with stringent nuclear safety requirements. In this paper a part of the cybersecurity threat to nuclear safety will be analyzed. Assuring cybersecurity is usually broken down into enforcing security confidentiality, integrity and availability (CIA), with a strong focus on availability and integrity. In order to meet these security targets security controls are applied. At a high level these are typically subdivided into preventive, detective and corrective security controls, as e.g., applied by Draft IEC 63096. Corrective security controls can be broken down according to the phases of the security incident management, e.g., security response (immediate procedures to be followed by on-site staff etc.) and recovery (e.g. based on software backups). These are the last parts in the Security Defense-in-Depth (Security DiD) approach. In this paper, we will focus on the first parts of the Security DiD which includes deterring, protective, delaying and detective security controls.

Safety Defense-in Depth (Safety DiD) is traditionally considered in all Instrumentation and Control (I&C), Electrical Systems (ES) and Physical Protection architecture designs. However, the Security DiD is different from the Safety DiD. While the Safety DiD is achieved by including different independent systems, each composed of redundant subsystems, into the different architectures. The Security DiD addresses a sequence of security countermeasures that complement each other. Deterring security controls are all those security countermeasures that will make it harder for an attacker to come close to his target and discourage attackers from trying to initiating cyberattacks.

Part of this is the confidentiality of information, needed by an attacker in order to plan and execute a cyberattack. This includes information about physical characteristics of the site, physical controls that are in place, personal information about staff working at the concerned site, facility layout plans etc. Without this information in place, the attacker will need to put some effort to retrieve the necessary details from different sources, potentially leaving some unchartered parts. This is part of the "deterring security controls", as they raise the bar for a potential attacker. Similarly, physical protection security controls, like different fences, signs and lighting, doors and gates with access control are "deterring" as the attacker would have to climb over the fence or unlock a gate in order to pass one level of Security DiD.

These security controls are "deterring" as they do not provide a 100% protection of the targets. Each of the deterring security controls provides a maximum resilience, e.g., on what effort is needed to breach a door or gate.

A protective security control assures reliable protection of a primary or supporting asset against an assumed specific security threat. As an example, if strong encryption is applied to a software archive, its content can be considered as adequately protected, assuming that the encryption algorithm is sufficiently strong and the implementation is flawless. Similarly, a physically unidirectional security gateway (data diode) provides reliable assurance that data is transferred only in one direction.

Some security controls can support in delaying a cybersecurity attack, potentially rendering it ineffective. For example, a login may be protected with a password. After an invalid password entered by an attacker, the time interval before a new entry acceptation, may be gradually increased. Therefore, a brute force password guessing attack is considerably delayed, potentially up to the point where the attacker runs out of time for completing an attack.

Detective security controls are needed as a further Security DiD layer. At this point, it has to be assumed that the attacker already got access to the system. The challenge is to detect an abnormal intention or activity of the attacker as the final system compromise may be triggered at a later point in time, e.g., by loading manipulated software or by changing set-points that disable warning limits. The basis for implementing these detective security controls is cybersecurity forensic readiness and the principles of evaluating the digital evidence.

This paper will provide a comprehensive view of these first layers of a Security DiD, while analyzing—how these can be represented and measured for support towards an effective Attack Tree Analysis with Nuclear Safety [IAEA NSS 13]. As the primary target needs to be protected while considering the coordination of safety and security [IEC 62859]. Part of this work is done in the context of "Enhancing Computer Security Incident Analysis and Response Planning at Nuclear Facilities"—IAEA CRP J02008 project.

Synopsis ID: [293]

Integrating Cyber Security and Safety Systems Engineering Disciplines With a Common Code of Practice

Piggin, R.[1], German, A. [1]

[1] Atkins Ltd., United Kingdom

Corresponding Speaker: R. Piggin

This paper explores the ability of these systems engineering disciplines to combine and produce a code of practice including principles, models, methods, tools and techniques to create robust critical infrastructure by design and enable through life resilience.

Safety and security systems engineering disciplines are independent domains, with little interaction to date. There is increasing convergence driven through common technologies, platforms and networking, where safe operation of complex systems requires appropriate security. The two disciplines may also conflict, creating new functionality, vulnerabilities and hazards that may require additional mitigations to reduce risk provide critical services.

New technologies and programmes that include interconnected safety-related programmable electronic (digitisation) systems, including the increasing numbers of complex autonomous systems result in the need for engineers engaged in the design, development, maintenance and use to ensure that these systems are both safe and secure. The aim of the Code of Practice is to identify current good practice and existing standards whenever practicable. The key benefit of the code will be to provide current good practice for Engineers and Organisations to ensure that their Cyber Safety risks are managed so far as is reasonably practicable, meeting regulations and hence legislation. Such a code should assist in the provision of adequate evidence of Cyber and Safety risk management.

The code will address topics including:

Uncommon Language. The domains of Cyber Security and Safety use differing language to describe similar issues and a Code of Practice would provide definitions to promote common understanding;

Safe and Secure Principles. All codes of practice benefit from principles that then drive the detailed codes. These principles would need to be developed;

Lifecycle Management. Lifecycle management will provide an outline of the requirements to manage safety and cyber security through life;

Safe and Secure by Design. This will provide guidance on selecting an appropriate systems engineering approach including life cycle and safe and secure requirement decomposition methodology to ensure that safety and security features are identified and embodied in the design and build.

Security topics can be addressed in the context of the system life cycle processes contained in ISO IEC IEEE 15288 and the security-related activities and tasks. In addition, it should also cover potential faults and vulnerabilities that are discovered using combined techniques (e.g. Functional Failure Analysis, System Threat and Hazard Analysis, Common Cause Analysis) and mitigations designed into the site/platform, systems, equipment and components. These features and mitigations should be verified and validated throughout the build, and test and acceptance activities;

Risk Assessment: Risk assessment approaches to bridge safety and security risk assessment will be described to provide comprehensive methodologies and address the use of the ALARP principle in security;

Models The basic models for managing faults and vulnerabilities are coincident at the highest levels and the code of practice would explore these further and provide clarity regarding the similarities and differences;

Regulator Required Risk Control Systems. Both Safety (Regulation defined) and Cyber Security use common risk control systems to manage safety and security risks. It is contended that combining these risk control systems would provide both synergy and therefore greater understanding of the risks and their management; and ensure that cyber security effort is proportional to the safety hazards being managed;

Managing Hazards And Vulnerabilities Through Life: This will include continuing management of hazards and vulnerabilities through life using appropriate secure lifecycle processes (including procurement for instance) and Risk Control Systems it would also include guidance concerning existing safety-related systems and their security assessment and vulnerability mitigation;

The basic models (such as Common Fault and Vulnerability Principles) for managing faults and vulnerabilities are coincident at the highest levels and the code of practice would explore these further and articulate similarities and differences.

The paper will describe the development of a code of practice for safety and security, with a cross functional stakeholder and participants from across industry sectors, including nuclear regulators, safety regulators, cyber security and safety engineering specialists.

Synopsis ID: [236]

The Role of Regional and International Organizations

Gadano, J.[1]

[1] Ministry of Energy and Mining, Argentina

Corresponding Speaker: J. Gadano

In light of recent events (9/11 and other terrorist attacks we have witnessed in the last few years) the security paradigm has dramatically changed in fundamental ways: attacks, which used to be local or regional issues, have turned into local-regional events with global impact, and that have generated changes in the way states have to design their security regimes. Furthermore, while states used to fight organized groups, lately the image of the "lone wolf" has risen. The perpetuators are always upgrading their tactics and methods, and have the means, and are more aware of the installation´s security measures and response plans, and might even have access to these installations, through local operators. States now not only have to deal with a constant reconfiguration of the threat, but are exposed to an adversary that is willing to give his life for a cause, and therefore does not even have to plan his escape. In this asymmetric war, traditional "war rules" and rules of engagement are not valid anymore. Delay and response systems need to adapt to these characteristics present in modern terrorist profiles and threats. Although Nuclear Security remains a State responsibility, the fight against terrorism cannot be alone. We need to address this problem as an international community: we should recognize that nuclear security in one State might depend on the effectiveness of the nuclear security regimes in other states. There is an increasing need for more regional and international cooperation to enhance nuclear security worldwide. The international organizations that fight terrorism plays a central role in this scheme, by sharing best practices and developing standards that states regulatory and legislative bodies (with the support of regional organizations and initiatives) can build on, and adapt to regional and national frameworks. In this process, guidances and norms should avoid establishing a definition of credible threat, since it is constantly changing, but should provide interactive mechanisms to adapt to new scenarios. The Design Based Threat is a core instrument for the establishment and sustainability of security systems, instrument that has to be upgraded and updated on a regular basis Multilateral fora, such as IAEA, GICNT, CPPNM, CTBTO for example, plays a key role in the efforts to secure the nuclear facilities. It is really fruitful to test source and facility security, detection, delay and response mechanisms through information sharing, and regional and bilateral drills. Testing national and regional interagency coordination within the framework of international organizations is of vital importance in order to strengthen both national and regional nuclear security.

Synopsis ID: [138]

The Benefits and Challenges of International Cooperation to Support Nuclear Security Capacity Building

Xu, Z.[1], Deng, G.[1], Gu, S.[1]

[1] State Nuclear Security Technology Center (SNSTC), China

Corresponding Speaker: Z. Xu

This paper discussed the contribution of international cooperation to the enhancement of global nuclear security capacity building, as well as the challenges faced by some States. The IAEA's central role in promoting and coordinating international cooperation in nuclear security areas was also discussed. Nuclear security related international cooperation could be categorized to multilateral cooperation, bilateral cooperation and cooperation under some specific subjects. The most representative and widely recognized multilateral and bilateral cooperation for nuclear security capacity building is the cooperation mechanisms and activities sponsored or organized by the International Atomic Energy Agency (IAEA), which include, but not limited to, International Conference on Nuclear Security and on some other specific subjects, Nuclear Security Plan (2014-2017, 2018-2021), Resolutions on Nuclear Security during General Conferences, Training Courses and Workshops at national, regional and inter-regional level, as well as expert missions such as IPPAS Mission. The nuclear security capacity in Member States has been strengthened significantly through participating in the related cooperation mechanisms and activities. Another important multilateral cooperation on nuclear security is the Global Nuclear Security Summit, which took place four times since April 2010. The most important achievements of the Nuclear Security Summit meetings are to have ensured strong political commitment, promoted capacity building on nuclear security in some States, recognized the importance of international cooper- ation in the areas of nuclear security world wide. But the major problem of Nuclear Security Summit meeting is that the participation in the meetings is only under invitation, therefore the representativeness is not sufficient. Some other initiatives such as Global Initiative to Combat Nuclear Terrorism (GICNT) and so on, also provided some important contribution to enhance capacity building in nuclear security related areas through multilateral and bilateral cooperation, but their representativeness is also not wide enough. Although international cooperation can provide great contribution to strengthening global nuclear security capacity building, there exist some challenges for some States to participate in the cooperation. The willingness to cooperate with other countries and international organizations as well as NGOs in the areas of nuclear security is not always high for some States. In some developing countries and in particular some least developed countries, the capability to receive assistance through international cooperation is not strong enough: Lack of appropriate infrastructure and relevant technology, lack of sufficient well qualifies human resources, lack of financial support, just name a few. In order to ensure the majority of the countries to benefit from international cooperation, IAEA can play the

central role by exploring and applying a comprehensive international cooperation mechanisms and approaches.

Synopsis ID: [171]

Japan's International Cooperation in the field of Nuclear Security within the Forum for Nuclear Cooperation in Asia (FNCA) -Current Activities and Future Challenges-

Senzaki, M.[1]

[1] Japan Atomic Energy Agency, Japan

Corresponding Speaker: M. Senzaki

At present, several Asian countries have been considering the introduction of nuclear power plants. In the future, a dramatic increase of the use of nuclear material is foreseen and nuclear security and safeguards as well as safety will become more important in the promotion of the peaceful uses of nuclear energy. On the other hand, there is a continuing risk that nuclear or other radioactive materials could be used in malicious acts. This risk is regarded as a serious threat to international peace and security. The responsibility for nuclear security rests entirely with each State and an appropriate and effective national regime for nuclear security is vital in facilitating the peaceful uses of nuclear energy and in enhancing efforts to strengthen nuclear security as well as nuclear safety and safeguards worldwide. For these reasons, the Nuclear Security and Safeguards Project (NSSP) which started in 2011 within the framework of FNCA, aims to cooperate with FNCA member countries in order to strengthen their infrastructure for nuclear security and safeguards. FNCA is a Japanese government-led cooperation framework for the peaceful uses of nuclear technology in Asia. The framework for FNCA cooperation consists of a Ministerial-level meeting, a Coordinators meeting, a Panel meeting and 10 topical projects. The participating 12 countries are Australia, Bangladesh, China, Indonesia, Japan, Kazakhstan, Korea, Malaysia, Mongolia, Philippines, Thailand and Vietnam. The purpose of the project is to share experience in, knowledge of, and information on implementation of nuclear security and safeguards and exchanging views on policies, strategies and frameworks for better performance in these areas. This paper outlines the role and objectives of NSSP as well as the FNCA framework, and provides examples of how NSSP member countries work together to strengthen nuclear security, to enhance safeguards effectiveness and to raise awareness on security and safeguards. Particularly, the 6 year activities of this project produced excellent outcomes to raise the awareness of the importance of nuclear security, facilitated information sharing of nuclear security, promoted capacity building for nuclear security and enhanced nuclear security regimes in FNCA member countries. Also, The Project organized 3 Open Seminars (number of sessions: 11, total participants: 140), co-organized by FNCA, Host Country and the Japan Atomic Energy Agency (JAEA) in Vietnam (2012), Kazakhstan (2015) and Indonesia (2016). Open Seminars offered good opportunities to understand the importance and sharing of information to strengthen nuclear security and safeguards. As lessons learned from the Project, (1) there were various technical, cultural, socio-economic differences as well as nuclear energy situations among the FNCA member countries, but

the Project achieved a mutual understanding about the importance of strengthening nuclear security and safeguards in their respective countries, both during the workshops, the Open seminar and other activities, (2) the expert network established through the Project activities has the potential to promote and strengthen further cooperation among Asian countries in the field of nuclear security and nuclear safeguards, (3) the Project activities needed to be enhanced through the collaboration with JAEA, the IAEA, APSN and other existing multilateral frameworks. This paper also describes future challenges (3 years Plan) and strategies of NSSP for the contributions of FNCA member countries and for the international collaboration with other organizations (IAEA, APSN and others). The Project conducted a survey within FNCA countries about future activities of this Project. At the 6th workshop in 2016, FNCA member countries discussed the results of the needs survey and the prospects for future activities. The following fields of this project were selected. 1) Nuclear Security: Nuclear forensics, cyber security, nuclear security culture, and security of radioactive sources. 2) Safeguards: Additional Protocol, others. 3) Common for security and safeguards: Capacity building (Human Resources Development, HRD, others) by Centers of Excellence (COEs) in the region.

Synopsis ID: [173]

CIAE' Experience in 5th Collaborative Materials Exercise

Wang, T.[1], Liu, G.[1], Wang, F.[1], Zhang, Y.[1]

[1] China Institute of Atomic Energy, China

Corresponding Speaker: T. Wang

From 2015 to 2017, China Institute of Atomic Energy participated the 5th Collaborative Materials Exercise organized by ITWG. In our laboratory, the work including analyzing the properties of the two pellets, data interpreting and the attribution had been done. According to the timeline of nuclear forensics, 24-hours, 1-week and 2-months material analyzed reports including the analytical results and the relevant attribute were submitted. The capability of nuclear forensic analyses has been improved in our laboratory by this exercise.

Synopsis ID: [187]

Strengthening the Global Nuclear Order through Enhanced Reporting Mechanisms

Heinonen, O.[1]

[1] Foundation for Defense of Democracies, Finland

Corresponding Speaker: O. Heinonen

Safeguards, security and safety have been – due to technical and legal reasons - often viewed as separate areas in nuclear governance. The silo of these concepts however fail to adequately recognize and harness the synergetic effects each has on the other in contributing to the efficiency and effectiveness of the overall nuclear order. For instance, near real-time nuclear material accountancy of sensitive nuclear materials such as highly enriched uranium and plutonium, together with monitoring systems, provide valuable information about the location and status of nuclear material. This in turn is useful for nuclear security measures. Similarly, such information serves to benefit nuclear safety by contributing as input to criticality controls and locations of nuclear materials. Nuclear safety, security and safeguards seek to: prevent safety or security related nuclear accident or emergency; respond and mitigate its consequences; remediate sites after accidents; and confirm that nuclear energy is used for peaceful purposes. To achieve its objectives, the global nuclear systems require a strong safety and security conscious nuclear industry, responsible users of radioactive and nuclear materials and facility operators, capable and effective nuclear regulators, and stakeholders who reinforce and ensure a robust institutional framework. In measuring states implementation and compliance of the various legal instruments and standards, the IAEA together with the UN Security Council play a pivotal role through their regular reports. Currently, information on states' undertakings on nuclear safety, safeguards and security are scattered within various IAEA and other UN documents, including records of review meetings and the UN Security Council resolution 1540 committee. Such information are not only unthreaded, thereby making it more difficult to present a holistic picture, but data provided is also often lacking in public assessments on the effectiveness and efficiency of those measures.

In order to provide the international community with a full picture on the global status of nuclear safety, safeguards and security, the IAEA should be tasked to provide a biannual implementation report. Such a report, which would be in line with the Ministerial Declaration of the December 2016 International Conference on Nuclear Security that emphasized the central role of the IAEA in coordinating international cooperation and organizing information exchange, would assess the effectiveness of states undertakings on the ground to ensure nuclear energy is used in a safe, secure

and peaceful manner. The report should indicate where enhancements are required and suggest improvements taken by individual states or by the international community.

A transparent evaluation report would include an assessment of the adherence and implementation of all treaties, conventions, resolutions and codes of conduct for all states of the United Nations. The report should describe the size of the nuclear program including the use of radioisotopes and nuclear materials, and the independence and size of nuclear regulatory bodies without disclosing confidential safety and security related information. Much of the material that is useful for such assessment already exists in the IAEA and UN reports. States should be encouraged to make national reports from the review meetings and the IAEA peer review reports or their summaries and recommended good practices publicly available. Mechanisms to have information available on the implementation the Convention of on the Physical Protection of Nuclear Material (CPPNM) or the IAEA Codes of Conduct, which do not have such review meetings, need to be developed for a transparent assessment, using, for example, experiences from reporting by the Biological Weapons Convention.

Synopsis ID: [190]

Challenges and Responses for Ensuring Physical Protection of Nuclear Materials and Facilities: Prospects and Opportunities

Rehman, H.[1]

[1] Center for International Strategic Studies, Pakistan

Corresponding Speaker: H. Rehman

Challenges and Responses for Ensuring Physical Protection of Nuclear Materials and Facilities: Prospects and Opportunities Proliferation of the nuclear material related expertise and associated technology has long been an international concern due to the dangers involved in it. The threat posed by non-state actors such as terrorists, extremists, and illicit network groups, increased the requirement to focus more over the issue of physical protection of nuclear material and facilities. For the fact, it has high magnitude of causing destruction, and disorder in systems. The legitimate concern is that terrorist organizations might try to get approach to these deadly materials through multiple means including illicit trafficking. This concern became real and significant when terrorist networks, such as ISIS, were found to have intended to attain nuclear materials as a mean for their terror activities. In response, to these existing and emerging nuclear terrorism threats, International, multinational, and bilateral nuclear security initiatives have been placed such as the UN Security Council Resolution 1540, the Convention on the Protection of Nuclear Material, Facilities and the Convention to Suppress Acts of Nuclear Terrorism. To highlight the interdependent factors of existing measures for nuclear material and facilities protection and emerging challenges, this paper will dwell into the following queries: What factors are raising the risks of nuclear threats? What are the vital challenges and gaps in achievement of the ensuring physical protection of nuclear material and facility safety and security goals? What are the major developments and progress in the Nuclear Security Regime? What is a way forward to manage this elusive international security environment? This study aims to undertake an analysis of existing measures for the primary physical security areas of detection, delay, response, vulnerability assessment and technologies that support to ensure protection of the nuclear material and facilities. Including the features; new detection technologies, integration of information technology with physical technology systems, design basis threat analysis, progress in area of research and development (with reference to cyber threats) and success of personnel reliability programs (PRPs). While exploring emerging trends and growing challenges, it would appraise the threat level and loopholes in the existing nuclear security measures at the national and international level. Furthermore, it will also discuss regional cooperation possibilities by including factors of porous borders; a unique geographical position with a large coastline; tensions with neighboring states and the presence of terrorist elements in the region. It will explore a possibility of proposed multi-level approach of regional cooperation as well which entails

cooperation in nuclear security measures, in areas of intelligence sharing, border control working groups, bilateral exchange of an incident reports, joint response activities, investigation group for threat analysis, sharing best practices by regional centers of excellence, track II dialogue. The above mentioned concerns will be discussed in the context of global nuclear cooperation regime. The future for nuclear safety and security standards and practices can be forecasted by the existing initiatives and more involvement and enhanced role of the IAEA. It will provide broader scope for nuclear security, technical assistance at multiple levels, while offering reliability, inclusivity for convening nuclear related matters. This will also draw together like-minded states to lead towards a long term goal of global nuclear safety and security culture by lowering the risks of nuclear dangers.

Synopsis ID: [175]

China's Practice in COE Operation and Nuclear Security Training & Education

Gu, S.[1], Xu, Z.[1], Chen, C.[1]

[1] State Nuclear Security Technology Center, China

Corresponding Speaker: S. Gu

The China's Center of Excellence on Nuclear Security has come into operation at the eve of the fourth Global Nuclear Security Summit (NSS). To give full play of the COE and develop it into a platform for providing systematic and comprehensive education and training on nuclear security, in order to enhance the nuclear security capability in the region and beyond, the State Nuclear Security Technology Center (SNSTC), as the operation and management agency of the COE, has been making great efforts on improving training course design, curriculum development and operation management, on establishing professional instructor team, as well as on enriching teaching approaches including 3D Virtual Simulation Teaching System and Physical Protection Assembly Connecting Training Platform, etc. Since the operation of COE in March 2016, over 50 domestic and international training courses and workshops have been hosted by SNSTC, under the cooperation framework between CAEA and IAEA and the US Department of Energy. These activities have covered almost all the areas of nuclear security. Among the more than 1200 participants involved, 80% were from China and 20% were from other countries. Besides, the SNSTC also independently developed and conducted a series of training programs as requested by domestic facilities to meet their specific training needs. This paper focused on China's practical achievements on COE operation and nuclear security education & training, and shared the experiences achieved by SNSTC from COE operation on nuclear security training & education, training course design and curriculum development. Meanwhile, this paper will also analyze the needs and tendency of nuclear security training & education based on China's practice, and discuss how to develop a systematic and comprehensive training mechanism with the COE platform and to consolidate the cooperation with IAEA NSSC Network, to contribute to the nuclear security capacity building in China and the region.

Synopsis ID: [210]

The French Nuclear Centre of Excellence – CoE

Derouet, V.[1], Dandrieux, G. [2], Mariotte, F.[3], Renaudeau, F. [4], Bosquet, P.[5]

[1] EDF

[2] Ministry Of Ecology Sustainable Development And Energy

[3] CEA

[4] Ministry of Defense

[5] AREVA

Corresponding Speaker: V. Derouet

Today, it is important to have in mind that new international standards for nuclear industry have been published or are being developed in particular by the IAEA. As States and Industries have improved their understanding of security and cyber security risks, and ultimately threats, they have been prompted to establish guidelines and take specific actions to reduce the level of these security risks at existing nuclear facilities. One major issue for States and operators is to ensure qualified people are available or that staff can be trained to ensure properly their security missions. To address this issue, the IAEA promotes the creation of COE that are focus on high level expertise for nuclear security capacity building at national or regional level based on a high level of scientific and technical development. These centres have a special focus on training activities and may be recipients of international training courses from the IAEA.

In line with the Nuclear Security Summit 2016 and the Nuclear Industry Summit 2016, the French Nuclear Industry is continuously developing nuclear excellence, with the strict respect of safety, security and non proliferation issues. For Nuclear Security issues, France is developing its Centre of Excellence with the strong support of both French Nuclear Industry and French Security Sectors. In this presentation, we will develop how we capitalized the work achieved by the French relevant organizations to build/design the French COE and obtain the main key assets of the French COE: - Excellence of the French Nuclear Industry - Capacity of France to develop Nuclear Security Education and Training - High quality Courses and trainings provided by a network of world class Universities, Engineering schools, Schools of Social studies - High-level expertise in Nuclear Energy and Industry dedicated to the French Nuclear Industry and other countries - Long time and strong culture of partnerships with all relevant international organizations (AIEA, WANO, INPO, WNA, etc.)

The French COE will also have the particularity to inter-act with the relevant security and cyber security organizations, not only in usual COE domains like R&D and training programs, but also with relevant security institutions like the French National Council for Private Security.

In addition, the French COE will contribute to deliver tools for the benefit of others missions in the Nuclear or Security sectors in France.

Synopsis ID: [235]

Centre of Excellence in Argentina

Bieda, T.[1]

[1] Ministry of Energy and Mining, Argentina

Corresponding Speaker: T. Bieda

Argentina is currently driving a change in its nuclear facilities' security paradigm. We acknowledge that we are currently living in a post 9-11 paradigm, in which adversaries are willing to use any means necessary in order to carry out an attack and cause massive destruction and panic. In this sense, Argentina is working in the upgrading and updating of its response protocols, mechanisms and capabilities in case a potential terrorist attack actually takes place. Such updating means being aware and ready for any kind of attack, recognizing that the adversaries might come from various places and be driven by very different reasons and beliefs. We are working hard in the fight against the theft of radioactive sources and nuclear material, as well as sabotage or direct attacks against any nuclear facility all across the country, since our nuclear facilities are not all located in the same place, not even in the same province. This is the reason why we are carrying out a profound change in our protective forces. By Argentinean law, National Gendarmerie is the force in charge of protecting nuclear facilities in the country. What we are aiming at is the creation of a specific branch, inside that force, to guard and protect the nuclear sector specifically, which will not be reassigned to other non nuclear facilities. In this way, we are creating an elite group that will protect one of our country's most important assets. With such goal in mind, Argentina is in the process of creating a Centre of Excellence in order to train police/military forces. The centre will combine table-top exercises and classes as well as on-the-ground training, all in the same place. The place in which this facility will be built must be secluded, away from any urban settlement, in order to carry out the training activities without interfering with their every-day lives. We also expect this Centre of Excellence to become a regional centre, suited to train security forces from all our neighbour countries. The main areas on which training will be given are: - Basic practical radiation knowledge - Security and Safety in transport of radioactive sources and other nuclear material. - Perimetre nuclear asset custody and guard. - Preparedess and safeguarding of crime scenes involving nuclear or radioactive material for forensic analysis.

- Cybersecurity and new threats. - Human Resource Management in order to combat insider threats. - Force on force adversaries combat. - Tactical communications while on patrol. - Fixed site security. - Security drills. - Intrusion detection timelines. - Set up and use of detection instruments and technology. - Configuration and use of delay barriers.

Synopsis ID: [232]

US Center for Security Technology, Analysis, Response, and Testing

Monroe, L.[1], Leifheit, K.[2], Crawford, C.[3]

[1] National Nuclear Security Administration, Department of Energy, United States of America

[2] Leifheit Security Group, United States of America

[3] Oak Ridge National Laboratory, Department of Energy, United States of America

Corresponding Speaker: K. Leifheit

The United States Department of Energy, National Nuclear Security Administration, Office of Defense Nuclear Security has initiated, through Congressional authorization, a Center for Security Technology, Analysis, Response, and Testing (CSTART). The established Center is to carry out the following: (1) Provide to the Administrator, the Chief of Defense Nuclear Security, and the management and operating contractors of the nuclear security enterprise a wide range of objective expertise on security technologies, systems, analysis, testing, and response forces, (2) Assist the Administrator in developing standards, requirements, analysis methods, and testing criteria with respect to security, (3) Collect, analyze, and distribute lessons learned with respect to security,

(4) Support inspections and oversight activities with respect to security, (5) Promote professional development and training for security professionals. (6) Provide for advance and bulk procurement for security-related acquisitions that affect multiple facilities of the nuclear security enterprise,

(7) Advocate for continual improvement and security excellence throughout the nuclear security enterprise, (8) Such other duties as the Administrator may assign. As these functions allow for a Center with data, knowledge, input, etc. around the state of the nuclear security systems, operations, etc., the opportunity exists to expand such a center to also provide technology refresh through contracting for testing and evaluation of nuclear security technologies, research and development of technologies considered to be lacking or inadequate, integration of safeguards and security technologies, where appropriate, training in appropriate technologies, approaches, and techniques, and other functions applicable to a center of excellence. The Center will also focus on identifying and sharing best practices across a wide spectrum of nuclear protection disciplines, including performance assurance, security training, vulnerability and risk assessments, policy development, and the governance model for organizations with a nuclear mission. Finally, the Center will work to improve nuclear protection programs by carefully analyzing failures and deficiencies connected to nuclear protection programs and sharing those lessons learned with the broader nuclear protection community. This paper is intended to describe the current state of the CSTART, efforts to expand the

participation and portfolio of the Center, future directions and opportunities, and the management structure of such a Center. The paper will provide a discussion on the causal factors that led to the establishment of the Center, the evolution of the Center, including challenges in its establishment, and will describe in detail how the Center will assist in building and strengthening the NNSA nuclear protection program. When fully developed, the Center will provide a valuable U.S. Government capability in support all aspects of the nuclear security enterprise.

Synopsis ID: [124]

Moroccan Nuclear Security Training and Support Centre: Contribution Tool for National Capacity Building

Mellouki, R.[1], Ghazlane, H.[1], Nasri, B.[1], Soufi, I.[2]

[1] National Centre for Nuclear Energy, Science and Technology (CNESTEN), Morocco

[2] Ministry of Energy Mines and Sustainable Development, Morocco

Corresponding Speaker: R. Mellouki

Capacity building is a concept defined within International Atomic Energy Agency (IAEA) as a set of a systematic and integrated activities related to a) education and training; b) human resource development; c) knowledge management; and d) knowledge networks in order to get a continuous improvement of competencies of governments, organizations and individuals in the field of the safety, security and sustainability of a nuclear power program. This paper will be focused on the first component of education and training, particularly training. At this moment, Morocco do not have a nuclear power program, however capacity building within all national competent authorities is taking in consideration by effort spent on education and training. Effort related to nuclear security and safety is being done within some universities in the country. Training aspect is considered within Technical Support Organization (CNESTEN). Approach to training is translated through establishment of a Nuclear Security Training Support Centre (NSSC) in 2009 with the support of IAEA. The NSSC is supervised by a national steering committee representing all competent authorities (regulatory body, ministry of Foreign Affair, ministry of Energy and Mines, Ministry of Health, National defense Administration, General Directorate of National Security, Royal Gendarmerie, General Directorate of Civil Protection, Customs Administration, CNESTEN as NSSC secretary and chairman). A National training needs assessment has been conducted within all stakeholders, using as a basis the IAEA nuclear security training catalogue. During the last five years (2013-2017), 35 workshops and training, both at national and regional level, were conducted. Around 950 persons have been targeted. An average of 190 persons is trained each year, and around 6 activities were conducted under the auspices of the Moroccan NSSC. The beneficiaries of these are mainly national competent authorities (members of the steering Committee), users of radioactive material and participants from other countries. International cooperation is also an important component for the success of NSSC activities: most of NSSC activities are done with the support of IAEA and the US Department of Energy (DOE); some activities were done in cooperation with European Union and Arab Atomic Energy Agency. The sustainability of NSSC activities is taking in consideration within Moroccan Integrated Nuclear Security Support Plan (INSSP) and bilateral cooperation with other countries (US /DOE) and organizations.

Synopsis ID: [104]

Cyber Security Assessment in Supporting Nuclear Security for Nuclear Material Storage

Setianingsih, L.[1], Istiyanto, J.[1],Putra, A.[2]; Pulungan, R.[2] , Ashari, A. [2]

[1] Nuclear Energy Regulatory Agency (BAPETEN), Indonesia

[2] Universitas Gadjah Mada, Indonesia

Corresponding Speaker: L. Setianingsih

As the increase number of nuclear energy utilization, the risks associating its implementation tend to be higher. Data collection and management related to the nuclear energy application are not yet put in a securely restricted handling. The development of information technology has made it possible for borderless geographical transfer data. Security for the cyber transaction becomes an important matter to concern. Nuclear security covers as well the needs of cyber and information technology security.

Current condition for material storage is operated and controlled through a system of which access to the nuclear material can be hacked through remote access after having successfully attacked the computer system. Unprotected computer digital control system can create a risk of illegal control for nuclear material through a malware system inserted in a USB connection. The impact of consequences resulted by such cyber security attemps may lead to loss of nuclear material control. By having seen the vulnerability and risk associated to faulted system, the author proposes to create a model of preventive action in anticipating the possible attacks.

Computer system applied for monitoring and controlling area of nuclear material storage can create several security issues in entrance level access such as unauthorized personnel entrance and hacked system to the door control system There are several concerns regarding the computer system currently available on the nuclear storage facilities. They cover the need to solve how we can enhance the computer security for preventing the illegal access to the nuclear material storage.

The problem formulated is intended to cover only strengthening computer security system applied in nuclear security currently installed in nuclear material storage for research reactors. Nuclear materials are supposed to be regulated and controlled under supervision of nuclear energy regulatory agency. Once the nuclear material falls out of regulatory control through illegal possession due to theft and hijacking including through unauthorized access can lead to increased consequences which can be caused by incidents or accidents involving nuclear materials for non-peaceful utilization.

Scope of the study shall cover the identification and assessment of the cyber and information security threat that may lead to result in nuclear security threat. Provided that the threat of security can be identified, measures of each subject will then be associated to the necessary preventive actions. Formulation of preventive actions in eliminating the threat that may violate the security in general will be characterized based on the specific aspects.

As a communications infrastructure, the Internet is exposed to numerous threats, the majority of which stem from traditional TCP/IP vulnerabilities. The vulnerabilities can be exploited to replay control messages, request essential resources to exhaust computational and communications capabilities, eaves-drop on sensitive process information via man-in-the-middle attacks, inject malicious commands to perform inappropriate actions or display fabricated monitored values. (C.Alcaraz, 2015). With the development of ICS (Industrial Control systems), we gradually adopt IT solution to promote the overall connectivity and interactivity and improve the ability of remote access. This new application reduces the isolation between ICS and externals greatly. However it also brings some new security issues. Although we have taken a lot of security measures for traditional IT systems, many of these measures can't be applied directly to the ICS environment. (Fan, Xiaohe et al , 2015). There are many defense systems which can stop the cyber terror attacks. Usually the psychological disorders are accompanied. In this case, the significant social anomy could be spread out like the radioactive material contamination concerns. (H. Cho, 2016). The research objectives can be stated that we need to design a cyber security system that can prevent illegal access to the material storage. Furthermore, we need to limit access to the computer system for authorized personnel by authentication process which in this case a human reliability program can complete the assessment process on hiring the employees apart from elevating the security level in related computer system. In term of the interest to provide assurance for the computer system to keep it secured from illegal remote control, we need to design a cyber security system that has the capability to block the access for the control system

Understanding the nature of the affecting measures of those subjects can be essential to limit the success probability for a scenario to happen. Complete assessment and early detection to possible threat can be initiated to achieve the provision of nuclear security demands as requested by international world.

Accomplishment of securing cyber communication in nuclear industries not only can it maintain nuclear for peace utilization but also sustain the operational process for the system. Eventually it is expected that it can as well prevent loss of time and unnecessary resources. Upgraded cyber security in nuclear security can increase accountability for the confidentiality, integrity and availability as the basic requirements for secured cyber/IT systems.

Synopsis ID: [108]

Assessment for Information Security Systems Based on CO-BIT 5 in Indonesian Nuclear Energy Regulatory Agency

Riyadi, E.[1], Istiyanto, J.[1], Putra, A.[2], Ashari, A.[2]

[1] Nuclear Energy Regulatory Agency (BAPETEN), Indonesia

[2] Universitas Gadjah Mada, Indonesia

Corresponding Speaker: E. Riyadi

Nuclear Energy Regulatory Agency as an Indonesian government agency authorized with regulating the nuclear energy utilization in Indonesia through regulation, licensing and inspection should be able to maintain the confidentiality, integrity and availability of licensee's data that can affect a country's resilience. The licensee's data security is particularly important given the rapid increase in information technology, which could increase vulnerability to cyber-attack. COBIT 5 presents best practices from ISACA on governance and management organizations in the IT field which has built more than 15 years of practical use and application of COBIT in many IT companies, risk control, as well as security. Through the processes associated domains of information security such as APO12, APO13, BAI6 and DSS5; COBIT 5 provides qualified information security governance. This paper aims at assessing the information security in Nuclear Energy Regulatory Agency, and then determine critical success factor which is a list of policy recommendations that can be implemented to support high-level management in a decision-making process.

Synopsis ID: [193]

How to Arrange Exercises in Cyber Security

Nielsen, T.[1]

[1] Swedish Radiation Safety Authority, Sweden

Corresponding Speaker: T. Nielsen

Cyber security has fast grown to be regarded as a well invested source to secure or mitigate attacks on your operations. It is also known that I&C systems outside your core operation with often limited protection can be manipulated and affect your main process indirect. For example, a cyber attack against your ventilation system for your server room can make your server stop working due to too hot environment or a cyber attack at your access control system might make it impossible to gain passage to a certain room.

Some attacks are made by youngsters just for fun while other attacks have resources from State level to do it, regardless which one is doing it you need to prepare for both cases and doing exercises in this area both field exercise and table-top exercise is a good way of understanding your own capabilities and resources.

Exercises is a great way of preparing yourself and your organization. Exercises will improve your skills and capabilities and in the end give you an understanding of your u p's and down's.

So how did we do in Sweden? We have a co-operation between authorities in the Nuclear Security Coordination Group. Member of this group is the Police, National Grid, Civil contingency agency, Secret service, we as the regulatory authority and the Coast Guard.

Cyber threats and attacks are on everybody agenda to be prepared against and the good examples we had from conducting transport security exercises Pilot2015 made it easy for the co-ordination group to take a decision to do cyber security exercises, iPilot2017. Consistent of a cyber security field exercise for technical personnel and a table-top exercise for management level.

Like the exercise before we early decided to do it in a cooperation with IAEA. We also needed funding and applied to the EU internal security fund, ISF. A year ago we got ok from EU and the planning got more intense.

Exercise planning -purpose, scope, objectives, target group and limitations -exercise types and forms -time table for exercises -planning organization -exercise documentation -using the draft to IAEA computer security exercises handbook (working material)

CRATE Early in the planning phase we decided to use the Cyber Range And Training Environment (CRATE) that the Swedish Defence Research Agency (FOI) developed and maintained.

Cyber security exercises normally have limitation regarding your different computer systems. The first one is, don't do it, never use your real system. Using CRATE makes it possible to smoothly deploy and configure a large number (thousands) of virtual machines in a controlled environment. CRATE is also equipped with host based traffic generators emulating user behavior and tools for logging and monitoring the environment. This lab resource is used to create computer networks for use during experiments, competitions and exercises in cyber security.

Initiating and carrying out the project -practical preparations -implementing organization -exercise documentation -scenarios -briefings

Co-operation with the players In close co-operation with the players, IT security technical personnel at NPP's in Sweden, we decided about scenarios for the field exercise. We also decided that the outcome or shortcomings from the field exercise would be the input to the table-top exercise a few weeks later.

As always logistics plays a big role in exercises like this and specially when preparing a program for international expert/observers coming from abroad.

Evaluation From the very beginning an evaluation – follow up was prepared.

Everything processed through Initial Planning Conference, IPC, Main Planning Conference, MPC, and Final Planning Conference, FPC.

Good examples Good examples and what to avoid while planning will also be shown.

The actual exercise is in October 2017, that means that some information about the outcome of the exercise will be delivered at the conference first handed.

Summary Key Exercise Points with clear: -defined objectives -scenario -identified and pre- pared logistics requirements -definition and understanding by all players about their roles and responsibilities.

Synopsis ID: [141]

Review and Update Experiences to National Design Basis Threat for Physical Protection System Development at Nuclear Facility in Indonesia

Rismawan, D.[1]; Suharyanta, S. [1]

[1] Nuclear Energy Regulatory Agency (BAPETEN), Indonesia

Corresponding Speaker: Rismawan, D

Design Basis Threat (DBT) is one of the basic requirements in designing a physical protection system in nuclear facility. DBT contains the type of characteristics and intensity of all potential threats that have possibility to occur and attack the facility. The type of characteristics and intensity of the threat will always change according to the conditions and strategic situation in each local area and global issues of a country and even internationally, Indonesia has many island including cultural that have a specific characteristics in every area and also the sectoral ego in national institutions, and it will be a big challenges for BAPETEN as a Competent Authority to collect every informations related to security that will be use for DBT datas. Therefore the national DBT document should always be reviewed regularly and coordinate with multi-sector related security stakeholders at the national level. Indonesia as an IAEA member state has ratified CPPNM and its amendment into the physical protection regulatory system and implements it as a prerequisite for the licensing of nuclear installation operations. This paper will discuss Indonesia's mechanism, experiences and challenges in conducting regular review of DBT documents every two years since 2002 based on the Indonesia original characteristcs.

Synopsis ID: [45]

Upgrading the Physical Protection System at Nuclear Research Reactor in Thailand though the International Physical Protection Advisory Service

Youngchuay, U.[1]; Bhenboonmee, T. [2]

[1] Don, Thailand

[2] Ae, Thailand

Corresponding Speaker: Youngchuay, U.

A category III nuclear material at a nuclear research reactor located in Bangkok, Thailand was last installed the Physical Protection System (PPS) in 2010. The objectives of the upgrading are strengthen the performance of the PPS to oppose and limit the adversary toward the nuclear facility at Thailand Institute of Nuclear Technology (TINT) and provides the maintenance plus extended warranty and preventive maintenance for the installed equipment. The current PPS was reviewed and evaluated by experts from the Pacific Northwest National Laboratory (PNNL) then four areas of upgrading options were suggested as following: Reactor Hall, Reactor Building Exterior, Fresh Fuel Storage and Guard Post/Access Control. The security enhancements are based on performance objectives found in IAEA document INFCIRC/225/Rev.5. The PNNL is the implement agent on behalf of the United States Department of Energy (DOE). Next steps for a security upgrading are established the contingency plan and evaluate the performance of the new PPS. Key Words: Category III PPS, Thailand Nuclear Research Reactor, INFCIRC/225/Rev. 5

Synopsis ID: [217]

International Cooperation for Strengthening Nuclear Security Capacities within "Public Company Nuclear Facilities of Serbia"

Arbutina, D.[1], Mladenovic, M.[1], Žarković, D.[1]

[1] Public Company "Nuclear Facilities of Serbia", Serbia

Corresponding Speaker: M. Mladenovic

Public Company Nuclear Facilities of Serbia (hereinafter PC NFS) is the only nuclear operator in Serbia. It was founded in 2009 under the Law on Ionizing Radiation together with the Serbian Regulatory Body. Since its establishment, PC NFS has continued all nuclear activities previously managed by Vinca Institute of Nuclear Sciences; Two research reactors (RA-final shut down and RB-zero-power critical assembly, operational but currently not-licensed), RWM facilities- old Hangars H1 and H2 with legacy waste, new hangar H3 (for the storage of intermediate and low level radioactive waste) together with the secure storage for the high activity sealed radioactive sources, and closed uranium mine Kalna are the part of the Company. Strengthening nuclear security is the vital part of the development strategy of PC NFS. Department for nuclear security was founded in the 2016, first time after repatriation of spent nuclear fuel to the country of origin (Russian Federation) in 2010 which has shown the willingness of PC NFS management to make nuclear security equal to the radiation and nuclear safety, emergency response and preparedness and radioactive waste management. Since 2003, The United States Department of Energy's (DOE) has endeavored to provide technical and financial assistance to Vinca Institute of Nuclear Sciences to improve protection of nuclear and radiological material. After the PC NFS was founded, all the cooperation in the field of nuclear security was continued through PC NFS. The last building, upgrade and maintenance of PPS at the Vinca site (site which uses PC NFS and INS Vinca together) which has covered facilities of interest both in PC NFS and INS Vinca was successfully finished at the beginning of 2016. Scope of this paper is to provide the results of the project, issues that we were facing during the building and upgrade of the system which, at the end, made PPS at both PC NFS and INS Vinca significantly upgraded (without going into the sensitive information). We will also provide the results of cooperation with US DoE in strengthening complete nuclear security regime within PC NFS through trainings and workshops that were provided by the experts from the various US DoE national laboratories and organizations (up to date we have finished three workshops: Workshop on Mitigating the Insider Treat Using Behavioral Science, Insider Treat Identification and Mitigation, Site Security Plan and in May 2017 we will have International Response Training Course) which helped us in strengthening our nuclear security capacities as well as enhanced our cooperation with the Serbian Regulatory Body. Those workshops and training has involved not only the PC NFS staff but also the representatives from all the other relevant institutions. Paper will also cover the efforts in

strengthening the nuclear security culture as the foundation of every nuclear security regime and continuous education of our staff through cooperation with IAEA and WINS.

Synopsis ID: [90]

EXTREME Tabletop Exercise

Funk, P.[1], Delaunay, N.[1], Badinga, M.[2]

[1] IRSN

[2] European Nuclear Safety Training and Tutoring Institute (ENSTTI), France

Corresponding Speaker: P. Funk

Since 2010, ENSTTI, European Nuclear Safety Training and Tutoring Institute, provides training and tutoring activities to transfer the knowledge and know-how of the European nuclear safety and nuclear security organizations. This presentation describes the tabletop exercise that is proposed by ENSTTI since 2013, namely EXTREME, with the support of the IAEA. This exercise was developed by IRSN, and is still managed by IRSN facilitators. The threat of nuclear terrorism is a global problem and strengthening the overall capability of the response to such threat is a permanent concern. To improve its capabilities in cases of an attack on a nuclear power plant, each concerned country performs regularly exercises generally limited to the actions of response forces. EXTREME (EXternal Threat REsponse Management Exercise) tabletop exercise aims to address through the response to a severe attack scenario the complexity of such a situation by taking into account the necessity to implement simultaneously the contingency and emergency plans. To this intend, it addresses the allocation of responsibilities between authorities and operators in terms of actions to be taken in case of a severe attack on a nuclear site, nuclear safety and nuclear security interfaces (coherence and complementary aspects of emergency and contingency plans), the management of interfaces between on site and off site response forces and the decision process including information exchange between stakeholders. EXTREME is 2.5 day scenario-driven tabletop exercise to address mainly crisis decision management. The scenario considers an attack on a nuclear power plant requesting an emergency response at national level. It does not address the physical protection of the facility nor the detailed national emergency organisation. Although nuclear power plants are designed to sustain such attacks, the emergency preparedness and response management has to be prepared. The scenario provides successive failures of nuclear safety and nuclear security functions requiring timely and appropriate measures to be taken to stop the aggression and to restore nuclear safety. The four phases of the emergency are addressed: the reflex phase deploying pre-determined response, the reflection phase in which actions taken are based on the diagnostics and the prognosis of the situation, the response phase to overpower adversaries and the recovery phase for return to a safe situation. EXTREME scenario is cut in nine sequences used by facilitators to lead participants through the case study to express their comments, points of view, criticisms. . . The objective of these facilitated discussions is to identify and develop key issues related to the effectiveness of the

response, such as balance between nuclear safety and nuclear security, information exchange and management of decision addressing nuclear security and nuclear safety decision. The final discussion tries to identify good practices and recommendations. Since 2013, four EXTREME tabletop exercises have been organized. The aim of this presentation is to explain the content of the exercise and the main issues and lessons learned that come out of the discussion with the participants. Lessons learned are addressed regarding decision making process, coordination and interfaces, planning and training, and time management.

Synopsis ID: [212]

Enterprise Mission-Essential Task List for Protective Forces

Parker, J.[1]

[1] National Nuclear Security Administration, Department of Energy, United States of America

Corresponding Speaker: J. Parker

Mission Essential Task List - A list of tasks required for mission accomplishment. The METL serves as the direct linkage between mission accomplishment and training. It is a mission-down analysis of requirements that is performance-focused and serves as a common operating language. As a METL analysis must be based on a valid and complete set of job tasks with identified levels of skills and knowledge needed to competently perform the tasks associated with assigned duties, it is synonymous with the term "Job Analysis" as defined and referred to in federal law and DOE policy. Stakeholder organizations: These are the organizations that have a vested interest in how the Protective Force performs its mission. They are generally identified as Protective Force Operations, Protective Force Training, Protective Force Performance Assurance/Testing, Risk/Vulnerability Assessment, and the Field Office. It is imperative these organizations collaborate on identifying, planning, and conducting performance assessments that are designed to achieve a common objective: improving mission performance. To this end, stakeholders are required to meet on a recurring basis to discuss METL Assessment results, provide comments and feedback on recent training/operations, and collaboratively determine future actions.

Field Manual: This document is a compilation of Collective, Leader, and Individual tasks with conditions, standards, performance steps, references, and supporting narrative descriptions. The information was aggregated from existing NTC/DOE and U.S. military doctrine. This manual serves as the common operating language among stakeholder organizations and must be used by each. However, it does NOT dictate how each task is to be specifically performed: if a site has a different tactic, technique, or procedure based upon site-specific methods required for effectively accomplishing a given task, then the site should use that approach and document it accordingly. The Field Manual is a comprehensive guide to facilitate the development and execution of mission related training, assessment, and evaluation activities. It is reasonable that restrictions in time, personnel, and resources will limit the quantity of tasks that can be trained in a given year; therefore, there is no requirement - written or implied – that PF organizations either conduct or be assessed upon the totality of tasks or performance steps within the manual.

Process Overview: Task Evaluation and Task Assessment are the processes used to measure performance proficiency (knowledge, skills, and abilities) and to guide the training program in determining and adjusting training content and priority. Task Evaluation is essentially the "testing" of task performance. Task Assessment is a qualitative judgment—part of an ongoing, working process—to determine the current demonstrated level of proficiency as well as what specific, follow-

on training is essential to reinforce and/or build upon current levels of demonstrated proficiency. All tasks (Collective, Leader, and Individual) are assessed and evaluated based upon task-specific conditions and standards.

♣ Task assessment relies upon the expertise of the subject matter expert (SME) conducting the assessment and culminates in assigning a specific value ("T," "P," or "U") for the assessed task.

Trained (T) means the unit has demonstrated proficiency in accomplishing the task to standard.

Practice (P) means the unit has demonstrated performance capable of completing the task but has some difficulty or has failed to perform some performance step(s) to standard and requires additional practice. This does NOT imply the unit cannot accomplish the mission.

Untrained (U) means the unit has not demonstrated proficiency to standard. This could be a reflection of substandard performance, or it could be that the unit has never been trained on the given task.

♣ Stakeholder Meeting

During the quarterly stakeholder meeting, the group determines the overall rating for each task, based on the values from each stakeholder. There is no specific formula or percentage required to determine a "T, P, or U" because the program is designed to encourage discussion among the stakeholders so everyone clearly understands the current level of performance. When the group cannot come to consensus on a rating, the PF commander (senior PF leader) makes the final decision.

It is critical to have comments for every task rated a "P" or "U". The group should clearly articulate in the comments column what specifically needs to be improved. The comments should answer, "Why is this task or performance step a P/U and what specifically needs to be improved?"

Stakeholders should then prioritize the training program based on assessment values.

Sites must consider what can be accomplished with excellence. Quality of training and testing is much more valuable than quantity. Stakeholders should determine what is reasonable and achievable based on available resources.

Synopsis ID: [215]

Using Virtual and Augmented Reality to Improve Cyber Security and Physical Protection of Nuclear Material and Nuclear Facilities

Clements, S.[1], Vandyke, S.[1],Godwin, L.[1], Macdonald, D.[1], Cramer, N.[1], Riensche, R.[1]

[1] Pacific Northwest National Laboratory, United States of America

Corresponding Speaker: S. Clements

For decades physical protection specialists have performed vulnerability assessments to identify attack vectors that attackers can use to either sabotage nuclear facilities or steal nuclear material. They then build protection systems to defend potential pathways. Over the years these systems have become more interconnected for better detection, assessment, and response but in so doing have developed a reliance on digital connectivity that may be vulnerable to cyber-attack. It is difficult to quantify the level of risk associated with these integrated digital systems against a blended attack. Physical enabled cyber-attacks or cyber enabled physical attacks take advantage of weaknesses inherent in both the cyber and physical domains to diminish defenses, and could provide attack paths that are not appropriately protected. This paper discusses how the use of virtual and augmented reality systems can aid in understanding the blended attack and help develop robust protection mechanisms against the advanced cyber/physical adversary. Virtual and augmented reality complement traditional tabletop analysis and software based modeling and simulation tools in use today.

This paper addresses the virtual and augmented reality work being conducted and expands upon the work done for the IAEA Computer Security Conference in June 2015. Currently, the system effectiveness of cyber-physical protection systems is evaluated and measured using table top exercises, Monte Carlo simulations, and uniquely developed vulnerability assessment software packages. The results are interpreted by subject matter experts and implemented by highly trained security practitioners. Decision makers and other stakeholders must trust in the experts' judgement, but may not truly understand all of the intricacies or the justifications for the recommended changes. The training techniques used to show each of these individuals the interdependencies of today's modern interconnected systems, at the level they need for understanding, varies widely and has been met with varying degrees of success. These techniques range from classic classroom instruction, hands-on performance based repetition, and high-level briefings to show the "art of the possible". It's been proven that there is a bigger impact on the security professionals when the material is made relevant to their situation, and they can experience it firsthand. A recent attempt at modernizing the delivery method for cyber-physical awareness training involved a representative model of a nuclear power plant in which a guide walked a user through a blended physical and cyber security scenario. The model was tremendously successful with thousands viewing it and hundreds of conversations on the challenges of today's interconnected cyber and physical security systems. The model was subsequently used to brief multiple ambassadors, displayed at additional conferences and used in

multiple training exercises. One drawback of this diorama is its size and weight. It is fragile, cumbersome, time consuming and expensive to ship the model to each venue, and valuable opportunities have been lost as a result. Additionally the model was built around one possible cyber-physical attack scenario and can only be used for that specific pathway.

Virtual and augmented reality can provide many of the benefits of the physical model, and can take awareness and instructional training to the next logical step. It is immersive, realistic, and lets the participants truly experience the scenario they are being shown. It engages multiple senses and helps users experience the cyber-physical interplay in much more depth and realism than classroom training, formal presentations, or table top analyses ever could. Additionally virtual and augmented reality systems are compact enough that they are man portable and can be checked as luggage. Multiple systems can be transported at a fraction of the cost of the physical model. Additionally, the scenarios can be easily tweaked and modified to meet the end user's needs. This includes tailoring the granularity of the training to the expected technical level of the audience, and highlighting specific challenges they may be facing. The use of virtual and augmented reality can provide enhanced and customized training and awareness that is not achievable using today's standard training methods.

This paper will compare and contrast traditional classroom and performance based training, tabletop analyses, software modeling and simulation, and static physical models against virtual and augmented reality and highlight lessons learned from research and development efforts to build training and awareness exercises in virtual worlds.

Synopsis ID: [237]

Interactive 3D Models and Simulations for Nuclear Security Education, Training, and Analysis

Warner, D.[1], Dickens, B.[1], Heimer, D.[1], Knudsen, R.[1]

[1] Los Alamos National Laboratory, Department of Energy, United States of America

Corresponding Speaker: D. Warner

The Application and Modeling Development (AMD) Team of Los Alamos National Laboratory (LANL) develops Three-Dimensional (3D) fully immersive virtual reality tools for training nuclear security professionals internally at LANL, as well as for a wide range of domestic and international audiences. AMD provides first person fully interactive models that supplement and include written procedures for the purpose of training, testing, and demonstration. 3D applications produced by AMD can also include real world data and physics and allow users to view the environment from any angle, effectively changing the camera position to any desired location and/or zooming in and out, which is not possible with video training. This technology has been used in training scenarios relating to the assembly of complex machinery, performing high hazard tasks, first responder and security personnel drills and inspections relating to nuclear and biological facilities, and insider threat vulnerabilities. Other 3D model applications include nuclear facility accident event reconstruction and presentation of concepts for potential project development. The benefits of 3D virtual applications, such as significantly improved security, safety, efficiency and information retention, and the ability to modify scenarios, apply to workers handling nuclear materials and operating nuclear facilities, specifically in the context of insider threat prevention and protection. Virtual training applications provide a mechanism for recognizing vulnerabilities and threats in nuclear facilities by combining the 3D world with 2D graphics and information. Virtual nuclear facility models include graphical tags on components and materials determined to be vulnerable to the insider threat. Clicking on a tag displays written documentation about the vulnerability, material, and/or component. In addition to textual information, the asset itself can be displayed separate from the virtual environment allowing users to zoom in and out and to rotate the item to gain visual clues. This type of interaction allows users to acquire a great deal of detail about critical components, which can specifically relate to the insider threat. 3D models and simulated training removes exposure risk and allows for the production of real and virtual facilities, events, and scenarios. LANL AMD team has compiled an exhaustive library of assets related to unique and real nuclear facilities, which provides the capability to meet the requirements of a broad range of nuclear security applications. Our goal is to continue to expand this training capability and enhance the way virtual reality is adopted and applied to the physical protection of nuclear facilities and materials. In this paper, we will provide examples of 3D environments developed for training and demonstration purposes and

discuss the capability of including real world data and physics models in our applications and the applicability of these models to insider threat training and analysis.

Synopsis ID: [229]

Regulatory Oversight of Trustworthiness for Employees in Research Reactors

Alsalman, A.[1]

[1] Energy and Minerals Regulatory Commission, Jordan

Corresponding Speaker: A. Alsalman

Trustworthiness programs applied in nuclear facilities based on risk assessment and using graded approach. The program elements depend on the threat assessment for the nuclear facility and the hazard which could be posed if an accident intentionally or unintentionally take place.

Since there is an elevation in the threat profile an establishment of trustworthiness program for employees in research reactors becomes a must. The value of the program is to minimize the probability of insider threat, and to implement mitigation measures against insider threat to strengthen the integrated nuclear security system for research reactors.

Trustworthiness program for research reactors should apply the requirements of the nuclear power reactors. Graded approach shall be considered in the depth of the implementation of the program elements. The Criteria for identifying the critical positions and functions should be based on the categorization of the safety and security events that could lead to unacceptable consequences or theft of nuclear material. In addition, relying on the job analysis would help in categorizing the trustworthiness levels and give the operator the basis for targets identification and compartmentalization of critical areas within the facility. It is strongly recommended to apply the trustworthiness program for nuclear material (Category I), but with the present changes in the intention by adversaries to acquire nuclear materials there should be an enhancement in the nuclear security measures and systems which include the application of trustworthiness program for other categories of nuclear materials and activities which should be derived from the present threat assessment and the new adversary intentions.

Addressing the challenges of implementing the trustworthiness program for research reactors will be different from research reactor to another reactor depend on the uniqueness of the design of each research reactor. The type of it is applications in parallel with the regulatory influence and the legal infrastructure would support the establishment of such nuclear security tool for research reactors. This tool will also help in assessing the vulnerabilities in the physical protection systems for research reactors which will be different for each one. As the threat changes the threshold of applying such tool of nuclear security for nuclear material and facilities should be designed or modified if necessary to cope with the new challenges facing nuclear security of research reactors Through conducting risk assessment and applying graded approach in designing the physical protection system for a research

reactor the depth and the complexity of the application of the trustworthiness program could be identified.

Synopsis ID: [259]

Safety and Security a Single Entity for the JM-1 SLOWPOKE- 2 Reactor

Cushnie, R.[1], Preston, J.[1]

[1] The International Center for Environmental and Nuclear Sciences, Jamaica

Corresponding Speaker: R. Cushnie

The International Centre for Environmental and Nuclear Sciences (ICENS), the licensed operators of the JM-1 SLOWPOKE-2 Research Reactor, is poised to establishing itself as a centre of excellence and model institution for other small IAEA member states. Its stakeholders have identified key areas which they believe will require modernization, expansion, and restructuring in order to achieve this; details of which can be found in the five (5) year corporate plan.

The modernization at the facility will include the development of systems to automate many processes. One of such is the reactor auxiliary monitoring network, which will assist the reactor management to better track and trace auxiliary system performance in order to be better able to carry out predictive maintenance. This is especially important as these auxiliary systems have been in operation for almost three decades and experience intermittent failures. Another major initiative to modernize, includes the upgrade of the original Mark-2 (MK2) reactor console to its digital equivalent, a project which is in the advanced stages of planning. In addition, the physical and cyber security elements also required modernization in order to meet the demands of the ever evolving threat to nuclear and radioactive material along with the need that will ensue due to the impending changes.

The planned expansion will be applied to services, research, expertise and personnel. It is aimed at increasing: efficiency, throughput and the visibility and relevance of the facility. It is expected that this expansion will increase reactor utilization, where, additional research and experiments will be developed and will be complemented by additional capacity in training and teaching.

One side effect of initiatives of this nature (modernization and expansion), manifested itself in the need to bolster the safety and security (physical and cyber) mechanism at the facility. It is a well-known fact however, that the implementation of safety elements may at times contravene those of security. ICENS, in seeking to maintain the appropriate balance between the two, has begun to envision the two elements as a single entity. As such, the direct management of the safety and security (cyber and physical) now resides in a single department within ICENS that oversees the

design and implementation of policies, procedures and practices related to safety and security. This paper will delve further into rationale and response to these plans.

Synopsis ID: [8]

Considerations for the Design and Implementation of Physical Protection for a Proposed New Multipurpose Research Reactor Complex (MPRRC)

Ofodile, O.[1], Agedah, E.[1]

[1] Nigeria Atomic Energy Commission, Nigeria

SYNOPSIS

Nigeria, through the Nigeria Atomic Energy Commission (NAEC), has designed a physical protection regime for a proposed new Multi-Purpose Research Reactor Complex (MPRRC) which will integrate equipment, personnel and processes. The major part of the physical protection regime deals with measures against unauthorized removal or sabotage of nuclear material and nuclear facilities. Thus, in implementing its nuclear energy programme, Nigeria, through the relevant stakeholder organisations, has developed some relevant guidance documents that provide for the development of the physical protection measures for all nuclear facilities in the country including research reactors. Specifically, Nigeria:

a. Is domesticating all the relevant international treaties and statutes including the CPPNM, 2005. b. Has finalised the Nigerian Regulations on Physical Protection of Nuclear Material and Nuclear Facilities. c. Has finalised the Draft Regulations on Nigerian State System of Accounting for and Control of Nuclear Materials. d. Has produced a draft Guide on the Implementation of Human Reliability Programme (HRP) for Research Reactors. e. Has finalised the National Nuclear and Radiological Emergency Plan (NNREP).

Considerations for the physical protection of the proposed new MPRRC are based on the provisions of:

a. IAEA's NSS 13 which provide amongst others, the requirements for measures against unauthorised removal of nuclear material and sabotage of nuclear facilities respectively. b. IAEA's NST023 of July 2014 on the Developing, Implementing and Maintaining an Integrated Physical Protection System for Nuclear Facilities based on INFCIRC/225/Rev. 5.

Until recently, many research reactors were sited in geographic locations without serious considerations for security. For example, the only research reactor in Nigeria, NIRR-1 became operational in 2004. Today, NIRR-1 is undergoing a core conversion from HEU to LEU fuel while a pilot human reliability programme (HRP) is on-going to mitigate any insider threat situations. Due to the potential security threats to nuclear facilities all over the world, the siting of the proposed new MPRRC takes

into cognisance pertinent geographical features that enhance security of the facility. The siting characteristics considered for the location of the proposed new MPRRC include: a. Location in an area under the control of the State. b. Less traffic in the surrounding area. c. Advantageous topography from a security perspective. d. Location in a low population density area. e. Co-location with other facilities.

Thus, the proposed new MPRRC site is in a government-owned science and technology complex, about 75 km southwest of Nigeria's capital Abuja and can be reached via a major highway. The terrain of the site is a sparse forest with isolated trees and shrubs embedded into grass-land vegetation. The topography of the site is therefore excellent for the erection of guard towers to enable guards have a 360-degree viewing of the site. Furthermore, the population in the area is about 200. The closest populated area is about 13 km from the MPRRC site with an estimated population of about 200,000 people. In addition, there are a few already existing laboratories and facilities, including a Gamma Irradiation Facility, a Waste Management Facility, a multi- storey building for nuclear instrumentation and nuclear security laboratories, some administrative buildings and other research laboratories.

Staffing of the proposed new MPRRC also takes security into account. To be employed at the MPRRC, employees must undergo trustworthiness checks and be granted a security clearance based on the access required to perform their duties in addition to other trustworthiness programmes. Possible ways of countering potential external threats to the new MPRRC include:

Erection of guard towers with 360-degree and long distance viewing. b. Construction of security posts with access control and badging facilities etc c. Inclusion of electrified wire meshes and alarmed isolation zone between the outer and inner fences. d. Biometric access control to the secluded MPRRC area at the ACB and ACPs. e. Deployment of well-trained unarmed guards, armed guards and response forces to the MPRRC area. f. Elimination of the possibility of any intrusion from the air, by declaring the air space within and around the MPRRC site a "NO FLY ZONE". g. Availability of armed response organisations located within reasonable distances to the site.

Synopsis ID: [69]

Vulnerability Assessment Continuum

Edwards, J.[1], Rodger, R.[1], Thompson, K.[1], Baker, M.[1]

[1] National Nuclear Laboratory, United Kingdom

Corresponding Speaker: J. Edwards

Irrespective of whether a facility is operating within a Prescriptive or Outcomes/Performance based regulatory regime to meet INFCIRC225 Fundamental Principle J, Quality Assurance, a Duty Holder needs to effectively and efficiently assess the vulnerability of their physical protection system (PPS) to malicious threats targeting their assets; nuclear materials, other radioactive materials, structures, systems, components, people and information. The identification of the assets to be protected requires an assessment of the consequences of their loss, either through theft or sabotage, to determine their significance so that a graded approach (Fundamental Principle H) to their protection can be implemented. The PPS will be designed incorporating the principle of defence in depth (Fundamental Principle I) so that a combination of equipment, people and procedures will work in concert to minimise the likelihood of a single point of failure being exploited to create a potential vulnerability. There are a myriad of approaches available to a Duty Holder to undertake vulnerability assessments and this paper will look at the continuum of methods from simple checklists to complex computer based modelling and simulation passing through adversarial diagrams, path analysis, neutralisation analysis involving concepts of operations, and table top and 'live-play' exercises on the way. We will look at how the different approaches provide varying degrees of confidence and reproducibility of the likely effectiveness of the PPS. We will consider how the identification of the threat (Fundamental Principle G), including Insiders and External Attackers, and the organisational Security Culture (Fundamental Principle F) can influence the outcomes of the assessment. We also acknowledge how the results require Fundamental Principle L, Confidentiality, to be considered early in the process to adequately protect information related to any vulnerability identified.

Synopsis ID: [274]

Assessment of the Regulatory Framework in Nuclear Security: A Case of the Opportunities and Challenges of Malawi

Manda, C.[1]

[1] Environmental Affairs Department, Ministry of Natural Resources, Energy and Mining, Malawi

Corresponding Speaker: C. Manda

Malawi is one of the developing countries located in Sub Saharan Africa. The country is one of the member states of the International Atomic Energy Agency (IAEA) and is also a party to the Convention on Physical Protection of Nuclear Material (CPPNM). Currently in Malawi there is no nuclear power plant. Uranium mined at Kayelekera Mine and transported through Zambia to Namibia forms the major source and activity in the country. There, this study aimed at assessing the regulatory framework for nuclear security in Malawi to ensure an effective and sustainable nuclear security regime.

The paper employed a secondary review of the literature on the legislations and regulations governing nuclear security in Malawian. Key informant interviews were conducted to document the challenges and opportunities in the coordination and implementation of a nuclear security plan.

The study reviewed the regulatory framework in Malawi. The study observed that the law provides adequate security and physical protection of nuclear materials in the country. Despite of the law adequacy, the subsidiary atomic energy regulations were framed to promote more of the safety for radioactive sources than security of nuclear materials. The regulations in their applicability further highlights the complementarity of other national and international laws and regulations in promotion of security and physical protection of nuclear materials.

Recognizing the inadequacy of national regulatory infrastructure on security of nuclear materials, Malawi developed the guidelines on safe transport and security in transportation of radioactive materials and Intergraded Nuclear Security Support Plan (INSSP). The INSSP developed in 2014 provides a framework for coordination and implementation of an effective and sustainable nuclear security regime in Malawi.

Malawi continues to face challenges in the implementation of a nuclear security regime. These challenges emanate and have been facilitated from lack of an operational competent and in-dependent authority; lack of resources both financial and technical; and lack of coordination mechanisms. Despite of the challenges, the national regulatory framework with complimentary

international laws and regulations provides an opportunity for implementation of a sustainable and effective nuclear security regime.

Keywords: Atomic energy, Nuclear materials, Nuclear security, and Physical Protection

Synopsis ID: [172]

Physical Protection of Nuclear Material during Transport in Island Countries

Gunawan, I.[1]

[1] Nuclear Energy Regulatory Agency (BAPETEN), Indonesia

Corresponding Speaker: I. Gunawan

Background

The Act 10/1997 on Nuclear Energy ordains the use of nuclear energy is only for peaceful purposes to achieve public prosperity. The uses of nuclear energy shall considers the safety, security, peace, and health of the workers and public, and protection of the environment.

Indonesia utilizes radioactive sources and radiation generators for a wide variety of peaceful purposes; in industry, medicine, research and education. To some extent, the uses of radioactive sources for those purposes may generate radioactive waste and disused sources. While on the other hand, there are also waste of Technologically Enhanced Naturally Occurring Radioactive Materials (TENORM) from some industrial activities including oil and gas production processes as well as mining and processing of raw materials.

In respect to nuclear fuel cycle, Indonesia does not have any nuclear power plant. However, in its national long term strategic action plan, Indonesia has tried to introduce the use of nuclear energy to generate electricity. Currently it has three research reactors located in Serpong, Bandung and Yogyakarta with the power range of 100 kW – 30 MW.

The increase of act of terrorism has made the world considering the effort of physical protection of nuclear installations and material during usage, storage and transport. A series of international regulations and guidance have been published by both International Atomic Energy Agency (IAEA) and United Nations. The existence of nuclear installations in Indonesia and the use, storage and transport of nuclear material has encouraged the Indonesia Government to adapt the international regulations into its regulation. One of the regulations just recently enacted is BAPETEN Chairman Regulation Number 1 Year 2009 on The Physical Protection System of Nuclear Installations and Nuclear Material. The Regulation has stipulated the function of physical protection, the categorization of nuclear material, physical protection plan, and the requirements of physical protection system. The physical protection system which is established and developed is grouped by 3 (three) i.e. the physical protection system against unauthorized removal of nuclear material in use and storage, the physical protection system of nuclear material during transport, and the physical protection system against sabotage of nuclear installation and nuclear material during use and storage.

It is a provision and international commitment regulated by the International Atomic Energy Agency and followed up by a national regulatory body, in this case the Nuclear Power Control Agency (BAPETEN) that the presence of nuclear material should receive attention in the form of surveillance and security so that nuclear material is not abused in addition to Peaceful purpose. As for the purpose of security has been developed physical protection system intended to avoid deviations in transportation, use and storage of nuclear materials.

Review on Provisions Physical Protection System

There are one main legislations dealing with the issues of physical protection on transport, the Act 10/1997 on Nuclear Energy. In 2015, the government has enacted the inferior regulations of the Nuclear Energy Act for the issue of physical protection on transport; the Government Regulation No. 58/2015 on Radiation Safety and Security in Transportation of Radioactive Substances.

Indonesia has regulated the provisions of physical protection in transportation through Government Regulation No. 58 Year 2015 on Radiation Safety and Security in Transportation of Radioactive Substances which is a renewal of the BAPETEN Chairman Decree No. 1 Year 2009, in the form of Technical Security in Transportation of Physical Material and Hexafluoride Uranium (UF6) which is a Nuclear Material, which among others include: 1. Determination of Fissile Materials and uranium hexafluoride (UF6) which is a nuclear material into the classification of nuclear material. 2. Preparation and updating of the physical protection plan for the transportation of the fissile and uranium hexafluoride (UF6) material which is the nuclear material.

Physical protection plan for the transport of Fissile Materials and uranium hexafluoride (UF6) which is the nuclear material at least contains: 1.Preliminary notification to the consignee; 2.Selection of transportation mode; 3.Transportation routes; 4.Stops and transit; 5.Provisions on alienation; 6.Identification of carrier personnel; 7.Inspection of transport vehicles; 8.Security communication systems; 9.Guard or security officer; 10.Tracking equipment; 11.Terms of use of keys and seals; 12.Action after delivery; 13.Freight contingency plans; 14.Coordination with Response Unit; 15.Reporting procedures in both routine and emergency conditions.

Summary

The issuance of Government Regulation is not due to international pressure to Indonesia, but because of the need for nuclear installation and nuclear safety.

Normatively, the provisions of the existing protection system have been regulated in fundamental matters, but practically license holder and BAPETEN require further provision in field application, from design aspect, operation, maintenance, inspection, transportation, and evaluation of physical protection system.

Synopsis ID: [129]

Regulatory Framework for the Physical Protection of Activities and Practices Involving the Uses of Nuclear and Radioactive Material in Ghana

Annor-Nyarko, M.[1]

[1] Nuclear Regulatory Authority, Ghana

Corresponding Speaker: M. Annor-Nyarko

The safe use of radiation in Ghana spans 60 years; with the establishment of the Ghana Atomic Energy Commission by an Act of Parliament, Act 204 of 1963, as the sole Agency in Ghana responsible for all matters relating to peaceful uses of atomic energy further increased the use of radioactive materials in the Country. The promulgation of the Radiation Protection Instrument, LI 1559 in 1993 mandated the Radiation Protection Board (RPB) to regulate amongst others the protection of persons, public and environment against harmful effects of radiation. Ghana currently has facilities such as scanners, research reactor, radiotherapy facilities, Gamma Irradiator Facility and a waste management centre that uses radioactive or nuclear material. Some regulations and guidance documents governing the safe use of these facilities have been developed. Other standard operating procedures of Licensees incorporating some aspect of security of radioactive sources are in use and have been approved by the Radiation Protection Board. The possible use of nuclear material for non-peaceful purposes underlines the need for special protection of this material. Effective physical protection systems and administrative measures are therefore required to protect nuclear material and facilities from theft and sabotage. On the backdrop of this, in 2015 an Act of parliament established the Nuclear Regulatory Authority tasked, inter alia, to provide for the regulation and management of activities and practices for the peaceful use of nuclear technology. To fulfill the mandate of Regulatory Authority some regulations for which the security of nuclear and radioactive material is part are being developed. This paper seeks to highlight the regulatory framework for the physical protection of activities and practices involving the uses of nuclear and radioactive material in Ghana.

Synopsis ID: [11]

Regulation on Physical Protection in Indonesia

Pandi, L.[1]

[1] Nuclear Energy Regulatory Agency (BAPETEN), Jakarta, Indonesia

Corresponding Speaker: L. Pandi

Indonesia belongs to those countries which actively use atomic energy for peaceful purposes. Material and nuclear facilities is one of the strategic objects which could become the target of theft and sabotage, and also has a huge impact on the political field, the safety of workers, public and the environment. Therefore it needs a system of physical protection to prevent theft and sabotage. To support the security of the world, Indonesia has ratified the convention relating to physical protection. Ratification of the convention will be beneficial to the national interest and demonstrate Indonesia's commitment to maintaining world peace and security in accordance with the purpose of free and active politics. In accordance with Presidential Decree No. 76/1998 nuclear energy regulatory agency in Indonesia is BAPETEN [1]. International conventions relating to security that have been implemented nationally in Indonesia through legislation, including

i.e [2].: a. Act No. 8 Year 1978 on Ratification of the Government Regulation Concerning the Prevention of Spread of Nuclear Weapons; b. Act No. 9 Year 1997 on Ratification of the Treaty on the Southeast Asia Nuclear Weapon Free Zone; c. Act No. 1 Year 2012 on Ratification of the Comprehensive Nuclear Test Ban Treaty; d. Presidential Decree No. 49 of 1986 on Ratification of the Convention on the Physical Protection of Nuclear Material; e. Presidential Decree No. 46 Year 2009 on Ratification of the Amendment to the Convention on the Physical Protection of Nuclear Material; Indonesia has established the Government Regulation for implementation of International Convention Ratification i.e.: a. Government Regulation No. 33 Year 2007 on the Safety of Ionizing Radiation and Security Radioactive Sources [4], b. Government Regulation No. 29 Year 2008 on Licensing of Utilization of Ionizing Radiation Sources and Nuclear Materials [5], c. Government Regulation No.54 Year 2012 on Nuclear Safety and Security Installations [6],

Government Regulation No. 61 Year 2013 on the Management of Radioactive Waste [7], e. Government Regulation No. 2 Year 2014 on Licensing of Nuclear Installations and Utilization of Nuclear Materials [8] and f. Government Regulation No. 58 year 2015 on Radiation Safety and Security in Transportation of Radioactive Materials [9]. For implementation at nuclear facility, BAPETEN as Nuclear Regulatory Agency Agency has established BAPETEN Chairman Regulation (BCR) No. 1 Year 2009 on Provision of Nuclear Installations and Materials Physical Protection Systems [10]. In this paper discussess the regulation related to physical protection in Indonesia and physical protection system and its implementation at GA Siwabessy Reactor.

Keyword: physical protection, regulation, nuclear

REFERENCE [1] President Decree NUMBER 76 year 1998 on Nuclear Energy Regulatory Agency, Jakarta (1998). [2] Apriliani, D. Role of Nuclear Forensic Investigations of Nuclear Security Events in Indonesia, Nuclear Safety Seminar Proceeding, p. 86-91, ISSN: 1412-3258, Jakarta (2014). [3] The Act No. 10 year 1997 on Nuclear Energy, Jakarta (1997). [4] Government Regulation No. 29 Year 2008 on Licensing of Utilization of Ionizing Radiation Sources and Nuclear Materials, Jakarta (2008). [5] Government Regulation No. 33 Year 2007 on the Safety of Ionizing Radiation and Security Radioactive Sources, Jakarta (2007). [6] Government Regulation No. 54 Year 2012 on Nuclear Safety and Security Installations, Jakarta (2012). [7] Government Regulation No. 61 Year 2013 on the Management of Radioactive Waste, Jakarta (2013). [8] Government Regulation No. 2 year 2014 on Licensing of Nuclear Installations and Utilization of Nuclear Materials, Jakarta (2014). [9] Government Regulation No. 58 year 2015 on Radiation Safety and Security in Transportation of Radioactive Materials, Jakarta (2015). [10] BAPETEN Chairman Regulation No. 1 Year 2009 on Provision of Nuclear Installations and Materials Physical Protection Systems, Jakarta (2009). [11] Syarip, Tjiptono, T., and Purnomo, H., Improvement of Physical Protection and Safety System of Kartini Research Reactor to Meet the IAEA Standard Requirement. Nuclear Safety Seminar Proceeding, p. 108-116, ISSN 1412-3258, Jakarta (2008). [12] Susilowati, E., Contribution of G.A. Siwabessy Reactor Operation to the Power Reactor Development in Indonesia , Nuclear Safety Seminar Proceeding,p. 81-85, ISSN: 1412-3258, Jakarta (2014).

Synopsis ID: [203]

Evolution of Brazilian Physical Protection Regulations

Alves Tavares, R.[1]; Bloomfield Torres, L.[1]; Silveira Monteiro Filho, J.[1]

[1] Brazilian National Nuclear Energy Commission, Brazil

Corresponding Speaker: L. Bloomfield Torres

The Brazilian Physical Protection regulation, named CNEN NE 2.01"Physical Protection of Operational Units of Nuclear Area" was first issued by CNEN (National Nuclear Energy Commission) on August 1981. Since then, it was revised twice, on April 1996 and September 2011, only regarding minor aspects. It provides requirements and criteria for the establishment of physical protection systems by a traditional prescriptive approach. The prescriptive approach, despite the advantages of clear requirements definition, simplifying regulatory efforts (inspections just verify strict compliance to regulation terms, over different types of facilities/operations), does not allow a clear and effective performance measurement, may lead to insufficient or excessive security measures (in both cases, causing inadequate expenditure of material and human resources), and the possibility of providing a false sense of security. In order to overcome the inherent limitations of the current approach, CNEN is revising its Physical Protection Regulation, through adoption of a combined approach (performance-based and prescriptive), also incorporating sabotage and insiders aspects, allowing further adherence to international good practices, such as INFCIRC 225 Rev.5 and the 2005 Amendment to the Convention on Physical Protection of Nuclear Material – CPPNM. In planning and designing their Physical Protection Systems, operators must establish a threat assessment to their facilities. In this process, credible/plausible theft and sabotage scenarios are defined. In addition, exercises and performance tests are executed periodically, enabling operators to evaluate, all aspects of their Physical Protction Systems (personnel, equipments and proceedures, etc.) in accordance with regulatory requirements. Considering the current scenario and conditions, the starting point to the revision process is a national design-basis threat (DBT) elaboration, which is currently being held by SIPRON (Brazilian Nuclear Program Protection System), a branch linked to the Brazilian Presidency of Republic Security Cabinet, in which CNEN participates in cooperation with other institutions like Brazilian Intelligence Agency, Federal Police Department, Defense Ministry, etc. It will enable the redesign and re- evaluation of PPS for existing nuclear/radioactive materials, facilities and transport operations. The current physical protection regulation (CNEN NE 2.01) revision process will output three new documents, aiming to cover comprehensively physical protection of different types of facilities (nuclear and radiological) and transport operations of nuclear/radioactive materials, considering the peculiarities involved on each. CNEN NN 2.01 will focus on nuclear materials and facilities, CNEN NN 2.05 aims to deal with transport operations, and CNEN NN 2.06 is about security of radioactive sources and associated facilities. The new CNEN NN 2.01 intends to establish some

new design performance requirements related to the main security functions (detection, delay and response) such as estimated detection probabilities for each security area, time delays for physical barriers, path analysis, global PPS PE (probability of effectiveness) and new testing scenarios. Those requirements represent an operator design self-evaluation, which is not part of the process nowadays. The future testing scenarios will include sabotage and insiders actions. Among possible impacts that will have to be considered in the revision process, further training and capacity building on operators, other government agencies and decision-makers posing a big challenge to all these stakeholders.

Synopsis ID: [49]

Shock Wave Propagation around Convex Structure

Trélat, S.[1], Eveillard, S. [1]

[1] Institut de Radioprotection et de Surete Nucleaire (IRSN), France

Corresponding Speaker: S. Trélat

In a security context, it is important to know the blast characteristics whenever an explosion occurs near critical infrastructures. The problem arises from the impact of an overpressure wave on structures that may be catastrophic under certain conditions. IRSN, as the technical support to the government authorities in France involved in the security of nuclear material, conducts studies and experiments in order to get a good knowledge of the blast characteristics and the control of the different phenomena governing blast propagation. In this regard, IRSN has designed and built an experimental set-up to achieve non-destructive shock waves propagation studies at small scale. The set-up, which basically consists of a modular table, allows supporting reduced scale structures as well as reduced scale detonating solid charges. Explosive charges are hemispherical and centrally initiated from the bottom using electronical detonators. Experiments are conducted with an equivalent mass of TNT ranging from 10 to 100 g. A specific steel covered and reinforced plate is carried by a special stool designed to support the explosive charge. The modularity of the blast table enables to place the explosive charge at any location on the table. The modular table is located in a closed bunker. The position of the table into the bunker is optimized in such a way that the possible disturbances which may arise from waves reflection on the bunker walls are minimized. Experimental campaigns are performed at a Research Center located in the vicinity of Paris. The Research Center ensures all the pyrotechnics handling aspects of the experiments, and also provides the data recording system.

As a final goal, the set-up must be used: • first, to obtain experimental data on the blast loading characteristics resulting from the detonation of a condensed charge near a specific structure versus the distance between the explosive charge and the structure, • then, to understand in a better way the wave reflection phenomena (regular, Mach, etc.) and improve existing predicting analytical methodologies, • finally, to validate numerical simulation codes against experimental data in the free field and over-obstructed terrain. These data can also be used as input data for numerical assessments of the structure resistance. The set-up offers the possibility to measure the load in terms of pressure-time curves, even for very complex situations like multiple shock waves reflections, waves combination and diffraction. The present work summarizes the development of the set-up as well as some tests that have recently been performed: free-field blast tests (i.e. blast tests performed without structures) and tests with a convex structure. The main features of the table, the instrumentation and the pyrotechnics are shown. Overpressure maxima, arrival time of the shock wave and impulse are generally expressed as non-dimensional characteristics of the pressure-time history. The results

obtained should be compared with reference curves available from the open literature and numerical model results.

Synopsis ID: [50]

Dopex Project: Toward Fast-Computing Tools for Weapon Effects Evaluation on Nuclear Facilities

Eveillard, S. [1],Trélat, S.[1], Van Doresselaer, N. [1]

[1] Institut de Radioprotection et de Surete Nucleaire (IRSN), France

Corresponding Speaker: S. Eveillard

IRSN provides technical support to the government authorities in France involved in the security of nuclear material, nuclear facilities and the transportation of nuclear material. IRSN conducts studies and experiments in order to develop different technical tools and software for fast or detailed evaluations, to support the technical assessments.

The aim of the DOPEX project is to develop fast-computing tools for the specific requirements of nuclear security. It is designed to evaluate weapon effects for an aggression scenario against nuclear facilities and material. These tools are dedicated to IRSN's engineers with a broad expertise in nuclear facilities design, but who are not necessarily experts in weapon effects. The tools are a great help for a first evaluation in case of technical assessments carried out according to the regulation. These nuclear security fast-computing tools are used to identify the potential vulnerabilities and to estimate a first order of magnitude of damages for the considered aggression. For crisis situations, the nuclear security fast-computing tools can estimate the state of nuclear facilities after an attack or identify the potential aggravating factors by an aggression scenario in progress. A fast evaluation could lead to the revision of the projected source term for possible radiological consequences. The goal of fast-computing tools developed in the DOPEX project is to give a first order of magnitude of damages in maximum ten minutes time. It is a qualitative approach for a first evaluation, before possible additional detailed studies carried out with Computational Fluid Dynamic (CFD) and transient dynamics software.

Each tool, corresponding to a specific aggression, is made of empirical relations and analytical physical models for weapon effects from the scientific literature or IRSN's research works. This qualitative approach uses simple physical models and simplistic hypothesis of the physical phenomena observed:

Simple geometric conditions and structures, not complex configurations;

The physical modules do not consider all physical phenomena observed, just the main phenomena (for example, the presence of detonation products in confined space is not considered).

The tools take into account some particularities of the nuclear facility by a tridimensionnal geographic model in input (for example, topography environment). Users of the DOPEX tools define as input

different geographic coordinates and aggression means. The different computing steps (downloading 3D model, extraction of dimensions and calculations of weapon effects) are automatically performed by the tool employed. In a few minutes, a non-expert in evaluation of weapon effects can read and analyse the final results on a map or a 3D model mesh.

The DOPEX tools are fast and give a global overview of damages expected or caused. It should be taken into account that the DOPEX tools provide results with a certain degree of uncertainty. The results however are a great indication of how the incident or accident situation could be recovered or/and whether a further in depth study is necessary. In this case, the CFD software will be used, knowing that the computing time is more important than for the DOPEX tools. Furthermore, some computer development works are in progress to carry out a fully automatic connection between DOPEX's modules (geometric and physical) in order to improve the man- machine interface and to reduce computing times. Others tools are still under development and the current physical models used in the DOPEX tools are continuously improved to reduce uncertainty, thanks to research such as developed abacus or analytical models.

Synopsis ID: [276]

Assessment of Nuclear and Other Radioactive Material Attractiveness as a Part of the Graded Approach for Nuclear Security Management of a Research Reactor

Kovtunov, V.[1] Boeck, H. [1], Sterba, J.[1]

[1] Vienna University of Technology/Atominstitut, Austria

Corresponding Speaker: V. Kovtunov

Attractiveness of Nuclear and Other Radioactive material for adversaries plays an important role for the establishment of security arrangements on a research reactor. In order to assess the attractiveness of materials two main factors are taken into consideration: severity of consequences due to potential malicious act by means of using stolen material and several phases that adversaries have to overcome in order to successfully achieve the goal – fabricate a devise for a malicious act. Three phases are considered: acquisition, processing and utilization. The dominant factor of the attractiveness is the severity of potential consequences that can be achieved by means of using a fabricated device. Consequences can be divided to the following sub-factors:

- Health impact o Number of fatal cases o Permanent injuries
- Economic impact (property)
- Environment
- Social impact
- Contaminated area

Depending on the type of fabricated device that is used in a malicious act, different sub-factors become dominant for the consequences. Some devices may be used to cause injuries to individuals by exposing them to highly radioactive material. In this case the factor Contaminated area doesn't play as much a role as Health impact. Therefore Health impact becomes the dominant factor for the consequences, e.g. number of fatal cases or permanent injuries. Another type of devise can disperse material. In most cases the radiation would be too dispersed to be the only reason for immediate fatal cases. The Social impact is hard to assess due to the fact that it strongly depends on how the situation is dealt with by the authorities. The Economic impact on property can be a large contaminated area. Economic, Social and Environment impacts are proportional to a surface of a contaminated area. Therefore in this case, the surface of a contaminated area becomes the dominant factor for the consequences. A device that is capable to produce a nuclear explosion can be used as a weapon of

mass destruction. This type of a device when used in malicious act leads to the most severe consequences. Before adversaries reach the goal and commit a malicious act with certain consequences, it is necessary to overcome a number of obstacles such as: manage to steal, transport, chemically process the material if needed and fabricate a device. These challenges may be subdivided into the following phases: acquisition, processing and utilization. Each phase may represent certain challenges for adversaries depending on material properties and capabilities of the adversaries. It is important to point out that there is a possibility when adversaries do not possess knowledge regarding specific properties of certain materials on a research reactor but nevertheless they may still attempt a theft. In any case properties of materials dictate the complexity of acquisition, processing and utilization. Details on how different properties of materials may affect certain phases will be presented on the poster. Properties of Nuclear and Other Radioactive material and relevant tools that are used to handle them on site vary. Taking into consideration these differences, the phases (acquisition, processing and utilization) are assessed separately for Nuclear and Other Radioactive material. Finally the assessment process of Nuclear and Other Radioactive material attractiveness requires combined assessment of two main factors: potential consequences and properties of materials that may challenge the adversary to fabricate a device using materials from a research reactor. The proposal on how to estimate the attractiveness of materials, taking in to considerations all factors and sub-factors will be presented on the poster. The graded approach describes elaborated procedure of the risk assessment, taking in to consideration different factors and helps to identify correspondent security strategy. Current approach considers additional factors in comparison with the graded approach described in “Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities” (INFCIRC 225/Revision 5). The assessment of materials represents only a part of the graded approach for Nuclear Security Management of a research reactor. Identification of levels of security and requirements for them are out of the scope of this poster.

Synopsis ID: [61]

Developing and Sustaining a Physical Protection Regime in Myanmar

Tun, K.[1]

[1] Division of Atomic Energy, Ministry of Education, Myanmar

Corresponding Speaker: K. Tun

Myanmar formally acceded to the Convention on Physical Protection of Nuclear Material (CPPNM) and its amendment, the only legally binding international undertaking in the area of physical protection of nuclear material, on 6th December 2016 and entered into force on 5th Jan 2017. Following the accession to CPPNM and its amendment, Myanmar is working step by step approach to implement the obligations under the convention. At present, Myanmar has neither nuclear research reactors nor nuclear power reactors and its related facilities and activities. Myanmar also is a country without nuclear instillation. The utilization of radiation sources and irradiating apparatus are limited to the use in medicine, industry, agriculture, livestock breeding and research. Nonetheless, Myanmar government is aware of the importance of physical protection of nuclear material used for peaceful purposes and of nuclear facilities used for peaceful purposes that are essential for the prevention of nuclear terrorism and establishment of effective global nuclear security regime. Myanmar has views about nuclear that in order for the utilization of nuclear energy to be peaceful and secure, nuclear disarmament and nuclear non-proliferation must be achieved on the global scale. Physical protection plays an important role in supporting nuclear nonproliferation and counter-terrorism objectives.

As a legislation issue in Myanmar, the Division of Atomic Energy (DAE), under Ministry of Education (MOE), enacted the Atomic Energy law on 8th July 1998 and it was mainly based on radiation safety, does not cover nuclear safety, nuclear security and safeguards (3S strategies). With the purpose of strengthening national nuclear related legislation, the DAE has just recently completed the drafting of the Myanma Nuclear Law that prohibits the use, production, storage, distribution and import/export of nuclear materials without government license and provision on physical protection of nuclear material and nuclear facilities is included. Three regulations on nuclear safety, nuclear security and safeguards are also described in relation to Myanma Nuclear Law.

Additionally, Myanmar is actively enhancing to create the intelligence systems to fight against the border illicit traffic by means of a good coordination of the stakeholders as well as to integrate the knowledge and experience of all the organizations related with the trafficking of nuclear or radioactive material. Counter Terrorism Law Myanmar was promulgated on 4th June 2014, and it is based on UNSCR 1373 and UNSCR 1540 which is related to nuclear material and nuclear facilities security issues.

At the national level, the DAE, in collaboration with stakeholders, has been conducting a series of workshops and trainings to exchange information, practices and experiences to protect against illicit trafficking, theft, unlawful taking of a nuclear material in domestic use, storage, and sabotage of nuclear material and nuclear facilities. Being a developing country, Myanmar people does not familiar with the physical protection system that is vital importance for the protection of public health, safety, the environment and national and international security. For that reason, the DAE raises awareness and knowledge about the core concepts of nuclear security through Media and social network.

For international cooperation, the DAE is engaging the Global Threat Reduction Initiative (GTRI) Programme and also conducted National Awareness Seminar and Training Course on Physical Protection and Security Management in collaboration with International Atomic Energy Agency (IAEA) and the United States Department of Atomic Energy (USDOE). To strengthen the state's Physical protection regime and to fulfill the international obligations, Myanmar has been participating in the Integrated Nuclear Security Support Plan (INSSP) since 2013. Bilateral cooperation, between MOE and Malaysia Ministry of Science, Technology and Innovation (MOSTI), is signed regarding nuclear security issue. Moreover, regarding with strategic trade control and container control, Myanmar cooperates with Australian Border Force (ABF), United Nations Interregional Crime and Justice Research Institute (UNICRI) and the European Union Chemical Biological Radiological and Nuclear Risk Mitigation Centres of Excellence Initiative (EU-CBRN COE), in conjunction with local stakeholders.

Moreover, Myanmar, a Southeast Asian Nation, is endeavoring to expanded cooperation among neighbouring countries on locating and recovering stolen or smuggled nuclear material, minimizing any radiological consequences of sabotage and preventing and combating related offences as well as the promotion of good neighbourliness and friendly relations and co-operation among States Parties.

Being a signatory to the treaty, Myanmar has greatest benefits to build up the national capacitiesin implementing the efficient domestic physical protection regime as well as to ensure the international trustworthiness in the future and enabling its participation at the international level. The main challenges facing in implementing the physical protection regime are lack of financial, no sufficient experts and infrastructural problems.

This paper describes consolidated efforts by Myanmar government such as in terms of regulatory framework, trade control, nuclear terrorism, awareness and engagement with local stakeholders and international organizations.

Key Words: amendment to CPPNM, Strengthen, Physical Protection Regime

Synopsis ID: [302]

Physical Protection of Nuclear Materials Issues in Tajikistan

Mirsaidov, U.[1]

[1] Nuclear and Radiation Safety Agency, Tajikistan

Corresponding Speaker: U. Mirsaidov

Tajikistan has legislation in place which regulates all aspects of the peaceful uses of nuclear energy, radiation protection, safety, physical protection, accounting for and control of nuclear material and import/export controls of strategic goods, including nuclear materials and technology. This legislation provides the basis for Nuclear and Radiation Safety Agency of RT (NRSA) and other State authorities to implement Tajikistan safeguards obligations pursuant to the Comprehensive Safeguards Agreement and the Additional Protocol.

State System of Accounting and Control of Nuclear Material at State level is performed by NRSA, the State nuclear regulatory authority of Tajikistan which is an independent Governmental authority and has the right to elaborate and approve regulations and guidance documents, issue licenses for relevant activities, carry out inspections and independently perform its regulatory decisions. Tajikistan does not have any operational nuclear facility. Eventual decommissioning of the former Argus Research Reactor depends on available financial resources.

Nuclear material is located in the following facilities, nuclear installations and Locations Outside Facilities (LOFs) in Tajikistan and accounted for within the relevant Material Balance Areas (MBAs) and Key Measurement Points (KMPs). NRSA was established as an independent State nuclear regulatory authority by the Law on radiation protection of 2003. It is responsible for licensing of all activities involving the use of nuclear material. Licenses ore issued for a period of 5 or 3 years and can be extended, renewed, cancelled or suspended. Conditions of the license are defined in an attachment to the license. NRSA elaborates and approves regulations and guidance documents related, inter alia, to accounting for and control of nuclear material and physical protection of nuclear material and facilities.

There are about 290 entities in Tajikistan using sources of ionizing radiation. Only nine of them possess items with nuclear material, e.g. closed sources containing plutonium, salts/solutions containing thorium or uranium and treated as open sources. These entities constitute MPs within a catch all MBA including all LOFs in Tajikistan (MBA code TK-Z). There is one more MBA recently established for Argus reactor at the S. Umarov Physical Technical Institute.

An “Order of organization of the Stale systems of accounting for and control of nuclear material and sources of ionizing radiation” approved by the Government Decree No. 499 of October 2013 foresees that an operating organization performs annual physical inventory taking. Tajikistan was one of the first of the post-Soviet Central Asian States to adopt a law on the State control of export of arms, military equipment and dual-use goods (in 1997).

In Tajikistan provided measures against illicit trafficking of nuclear and radioactive materials and there is presented certain approach in nuclear security issues. During the exploration of nuclear materials more than 500 “orphan” sources were discovered in storages, which were no longer in use or were a legacy from bankrupted companies. Very often managers of newly created enterprises/companies are not aware that such sources exist in the storages under their responsibility.

The joint project of NRSA AS RT and the US Nuclear Regulatory Commission was completed by inventorying and creating a database of radioactive sources. The purpose of this project was toinventory all available of IRS (sealed, open, generators and associated equipment) and create the database of them. Within the framework of this project, the inventory of all sources was completed in all regions of Tajikistan.

All the collected data by sources were entered in the database. This database is called RASOD. The uniqueness of the RASOD program is the automatic determination of current activity and the categorization of sources (the classification is made in accordance with the IAEA and the safety manual - No. RS-G-1.9, - Recommended source categories used in general practice). RASOD is an information system that allows the input, storage and processing of IRS data. RASOD is developed for the regulatory bodies on nuclear and radiation safety. Physical protection measures had been strengthened at the State Institution of “Radioactive Waste Disposal Site” and at the Tajikistan National University, Scientific Institute. A new central control panel of the physical protection system was installed also at the Republic Oncology Centre. Such upgrades were performed mainly through bilateral projects between NRSA and other States and IAEA.

The physical protection system at the SE Vostokredmet includes a combination of several technical features and guards from armed military forces as well as special services.

Synopsis ID: [93]

IPPAS Mission in Poland

Zagrajek, M.[1]

[1] National Atomic Energy Agency (PAA), Poland

Corresponding Speaker: M. Zagrajek

Although Poland never had neither any nuclear power reactor nor any nuclear fuel cycle facility commitment to nuclear safety & security as well as nuclear materials safeguards was always one of our highest priorities.

Republic of Poland is a contracting party of all instruments of international nuclear safety and security regime and takes active part in works of International Atomic Energy Agency, OECD Nuclear Energy Agency, European Nuclear Security Regulators Association and other relevant institutions.

First IPPAS mission was hosted in Poland in 1997 and as received suggestions and recommendations were considered very helpful in strengthening our national nuclear security regime decision was taken to invite IPPAS mission again. Advices form group of international experts in nuclear security selected by the IAEA are extremely important for us, both from the point of view of enhancing security of existing facilities (including 30MWth Research Reactor MARIA) as well as part of our preparations to implementation of Polish Nuclear Power Program.

Mission described in this paper was held in Warsaw from 22nd February to 4th March 2016 and covered modules 1, 2 and 3 according to "International Physical Protection Advisory Service Guidelines (Services series no 29)".

Following institutions were involved in IPPAS preparations and conduct:

PAA: National Atomic Energy Agency (Polish nuclear regulatory body) working as coordi- nating institution during mission preparations;

ABW: Internal Security Agency;

KGP-BOA: Anti-terrorist Operations Bureau of Police Headquarters;

NCBJ: National Centre for Nuclear Research, operator of research reactor MARIA;

ZUOP: Radioactive Waste Management Plant. operator of spent fuel storages and radioac- tive waste repository;

ME: Ministry of Energy;

PGE EJ1: future operator of Polish NPP. This paper will present:

Basic information on nuclear security regime in Poland including latest legal changes regarding DBT preparation, maintenance and use;

IPPAS mission preparations, conduct and lessons learned;

Planned steps to implement IPPAS mission findings (including considerations to establish 1st national INSSP).

Synopsis ID: [308]

Evolution of Physical Protection Systems and Measures, Technological Advancements and Future Challenges

Ahmed, I.[1], Mahmood, R.[1] , Sadiq, M.[1]

[1] Pakistan Nuclear Regulatory Authority, Pakistan

Corresponding Speaker: R. Mahmood

This paper focus on the regulatory experience and challenges towards the implemen- tation of Physical Protection Systems (PPS) and measures at par with international obligations and technological advancements. Following is the brief abstract of the paper:

IAEA Nuclear Security Series on "Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), provides recommendations for the physical protection of nuclear ma- terial against unauthorized removal in its use, storage & transport and provides recommendations for protection against sabotage of nuclear facilities. These recommendations detail the elements that should be included in a State's physical protection regime.

Development, implementation and sustainability of Physical Protection Regime is the responsibility of individual states and this regime include physical protection systems at nuclear facilities. Physical protection systems are integrated set of physical protection measures intended to prevent the completion of a malicious act. Whereas, physical protection measures are comprised of personnel, procedures, and equipment that constitute a physical protection system.

INFCIR/225 was first published in 1975 under the title The Physical Protection of Nuclear Material and Nuclear Facilities while fifth edition was published in June 2011. During this evolution, requirements for implementation of physical protection systems and measures has significantly changed based on international developments both in technology and legal instruments.

A review study by the authors reveal that implementation of PPS and measures has also been undergone through many phases in Pakistan and evolved from the concept of gun, guards & gates to deployment of modern PPS and measures based on up to date technology and in accordance with international obligations and standards. This paper will also discuss the regulatory challenges and regulatory experiences in implementation of physical protection systems and measures in Pakistan over the history to date.

Synopsis ID: [78]

Developing and Sustaining a Physical Protection Regime in UAE

Al Shehhi, O.[1]

[1] FANR, United Arab Emirates

Corresponding Speaker: O. Al Shehhi

The United Arab Emirates (UAE) has taken strong and sustainable actions to develop its physical protection regime,in early stages of the UAE civilaian nuclaer energy programe the government has prepared and formally endorsed a ploicy statements as refelection to its vision with specfic regards of its nuclear energy programe. In this statement the UAE government committed to establish and sustain phsical protection regime, in order to effectivelly protect the nuclear materials and nuclear facilities. Any offences involving theft of nuclear materials or sabotage of nuclear facilities will be traeted as criminal and it will be subject to svere penalities. The Government of the UAE is party to all international instruments relevant to physical protection, including the International Convention for the Suppression of Acts of Nuclear Terrorism and the Amendment of the Convention on Physical Protection of Nuclear Materials (CPPNM). The UAE provided its national report to the United Nations (UN) 1540 Committee, as well as the associated matrix. The Government of the UAE is a partner in the Global Initiative to Combat Nuclear Terrorism (GICNT) and hosted one plenary meeting, in June 2010, in Abu Dhabi. In 2009 the UAE has taken an important legal step by issuing a federal law by decree no.6 of 2009 which established Federal Authority for Nuclear Regulation (FANR) as the country independent regulatory body to oversight the nuclear sector including the nuclear security. FANR issued regulations and lunch regulatory oversight to ensure sustaibale physical protection is maintained for all licensed facilities. The UAE goverments also established other entities to support the overall physical protection regime, these entities has great contribution either directly or indirectly to the UAE physical protection regime. In order to fulfill its commitment towards establishing a strong technical cooperation programme with the International Atomic Energy Agency IAEA, the UAE has contributed and utilized the IAEA nuclear security program activates to develop its physical protection leglisalitves and the regulatory oversight. Furthermore, the UAE goverments hosted several peer reviews to ensure the highest standand and adherance to the international instruments and to ensure its commitment to complete transperacny of its civilian nuclaer energy program. The UAE made a number of bilateral government-to-government arrangements with different leading countries in nuclear industry such as United States of Amerca (USA), France and Republic of Korea

(ROK). These biletaeral arrangements enbale the UAE to excghane information and obtained technical and scintific support.

Synopsis ID: [156]

Strategy for Strengthening Physical Protection of Nuclear Materials and Nuclear Facilities in Indonesia

Riyadi, E.[1]

[1] Nuclear Energy Regulatory Agency (BAPETEN), Indonesia

Corresponding Speaker: E. Riyadi

Physical protection system is an integrated set of physical protection measures intended to prevent the completion of a malicious act. Physical protection against unauthorized removal of nuclear material and against the sabotage of nuclear facilities or transports has long been a matter of national and international concern and cooperation. Indonesia has agreed to strengthen the Convention on the Physical Protection of Nuclear Material. Indonesia has responded to this by engaging in a collective commitment to strengthen the protection and control of such material and to respond effectively to nuclear security events; also in implementing a comprehensive physical protection regime; including any obligations and commitments they might have with respect to international instruments on nuclear security.

Objectives: This paper will address on strategy for strengthening physical protection of nuclear material and nuclear facilities in Indonesia

Results: Physical protection regime in Indonesia is including the legal and regulatory framework governing the physical protection of nuclear material and nuclear facilities; the institutions and organizations within Indonesia which responsible for ensuring implementation of the legal and regulatory framework; facility and transport physical protection systems. This paper will discuss legal basis for physical protection, there are Indonesia's Presidential Decree No 49 of 1986 on Ratification to the Convention of the Physical Protection of Nuclear Material, BAPETEN Chair- man Regulation No. 1 of 2009 on Provision of Physical Protection for Installation and Nuclear Material; and also IAEA Nuclear Security Series No. 13 Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5). It also will be discussed further of physical protection regime, identification the stakeholders involved in it, their roles, responsibilities, its intersected and interconnected areas, the matters of coordination, collaboration, and cooperative interaction, and integration of tasks to be con- sidered for strengthening physical potection. Stakeholders are regulatory body (BAPETEN), operators/Non-Government Organisation/private bussiness operators (including shipper and/or carrier), police department/national security guard, ministry of defence/Indonesia army forces, ministry of foreign affairs, ministry of transportation, ministry of energy and mineral resources; and IAEA.

The State's physical protection regime is intended for all nuclear material in use and storage and during transport and for all nuclear facilities. The State should ensure the protection of nuclear material and nuclear facilities against unauthorized removal and against sabotage. The State's physical protection regime should be reviewed and updated regularly to reflect changes in the threat and advances made in physical protection approaches, systems, and technology, and also the introduction of new types of nuclear material and nuclear facilities.

Conclusions: Physical protection on nuclear material and nuclear facilities in Indonesia can be strengthened by reviewing and evaluating of its elements through continuous assessment. Strengthening physical protection is a shared responsibility among involved parties, within the Republic of Indonesia. They are regulatory body, operators, police department/national security guard, ministry of defence/Indonesia army forces, ministry of transportation, ministry of foreign affairs, ministry of energy and mineral resources; also IAEA as an umbrella for international cooperation.

Synopsis ID: [201]

Experiences Addressing IPPAS Recommendations through Organization Changes

Srimok, B.[1], Watcharasuragul, V.[1]

[1] Office of Atoms for Peace (OAP), Thailand

Corresponding Speaker: B. Srimok

Office of Atoms for Peace (OAP) has hosted the IPPAS mission once in 2005. At the time of the mission conducted, OAP was responsible for both regulatory and operational functions. Later, the two functions were divided; all operational functions were assigned to Thailand Institute of Nuclear Technology (TINT) and regulatory functions remain with OAP. It is not uncommon that addressing some of the issues normally takes time such as revising laws and regulations. Regardless of the organizations responsible for the recommendations, certain progress has been made to address the recommendations over the years. One of them was the enactment of a new Nuclear Energy for Peace Act, and that leads to a more robust legal and regulatory frameworks as well as a more pronounced physical protection regime. Most of the non-technical recommendations stated in the mission report can be fixed by the existence of the new Nuclear Act along with other relevant Acts and the development of internal procedures and working documents. Technical recommendations and issues related to physical protection system (PPS) and its implementations were co-response by TINT as an operator and by OAP as a regulator. TINT has continuously improved its PPS and related equipments. OAP has also adjusted and affirmed its roles as an oversight agency ever since. In the future, if Thailand would like to host the IPPAS mission again, many more relevant organizations shall be involved in the process in order to account for the expanded scope and more stringent criteria will be applied to the latest IPPAS mission.

Synopsis ID: [221]

Path for Thailand towards Accession to Convention on the Physical Protection of Nuclear Material and its Amendment

Soontrapa, C.[1]

[1] Office of Atoms for Peace, Thailand

Corresponding Speaker: C. Soontrapa

Thailand is among the last IAEA member states that has not yet become a contracting party to the Convention on the Physical Protection of Nuclear Material (CPPNM). However, recently in force on February 1, 2017, the Nuclear Energy for Peace Act of Thailand greatly facilitates Thailand's accession the CPPNM and its amendment. The history of the Act development will be briefly explained. Furthermore, the Act conformity to the CPPNM and its amendment as well as Thailand's path towards accession to the CPPNM and its amendment will be discussed.

Synopsis ID: [202]

Academic and Research on Physical Protection of Nuclear Material and Nuclear Facility Conducted In Thailand

Chanyotha, S.[1], Pengvanich, P.[2]

[1] Chulalongkorn University, Thailand

Corresponding Speaker: S. Chanyotha

Presently, Thailand possesses one nuclear research reactor and several research facilities with small amount of nuclear materials. With the recent introduction of new Law and Regulations that impose higher nuclear security requirements, these facilities as well as other facilities that utilize radioactive materials must be physically protected. Nevertheless, the concept of physical protection is still unclear to many of the facility operators, and regulator will need a better way to qualitatively, rather than quantitatively, evaluate the effectiveness of physical protection systems. Thus, academic and research are crucially needed for the successful implementation of the new requirements.

In recent years, education and training programs on physical protection have been established in Thailand and offered to various target groups, such as students and facility operators, in order to raise awareness and enhance nuclear security regime both in Thailand and in the Southeast Asian region. One of the education programs, for instance, consisted of students from 8 nationalities from the ASEAN countries.These programs are results of collaborations among various organizations including government, facilities operator, university, as well as international party.

Most current nuclear related research in Thailand focuses on various applications of the radioactive materials rather than the nuclear materials. Research activities related to physical protection have only been introduced in Thailand recently, and they still mostly take place within the university environment. The topics of research include development of tools or guidelines for the evaluation of physical protection at various types of facilities, development of radiation detection systems, and enhancement of the national security regime. As many countries in the Southeast Asian region also do not have well-established nuclear law, especially on the nuclear security aspect, policy research is also conducted.

This paper will present the current status of academic and research activities on physical protection in Thailand. Their challenges will be discussed. As with other countries that do not have a well-established nuclear power industry, human resources and capacity building in nuclear area are always a serious challenge. How many experts on physical protection are needed? If one country does not need many, how should we design a program to train and sustain them? In such case, regional collaboration can provide a solution. It is important to note that by having regional collaboration, the

nuclear security regime in the region is strengthened as a whole. Thus, this paper will also propose a collaborative regime for academic and research that can help cope with the sustainability issue.

Synopsis ID: [121]

Establishment of the Nuclear Security Training Center in Kazakhstan

Izmailova, N.[1], Bonner, T.[2], Chakrov, P.[1], De Boer, G.[2], Idrissova, M.[1], Kurmanova, A.[1], Mcaninch, C.[2]

[1] Institute of Nuclear Physics, Kazakhstan

[2] Oak-Ridge National Laboratory, Department of Energy, United States of America

Corresponding Speaker: N. Izmailova

Through a cooperative effort between the Institute of Nuclear Physics (INP) of the Ministry of Energy of the Republic of Kazakhstan and the United States Department of Energy, National Nuclear Security Administration (DOE/NNSA), a new Kazakhstan Nuclear Security Training Center has been constructed at the INP site in Alatau, Kazakhstan to support training based sustainment of nuclear protection programs. Commissioned in May 2017, the NSTC provides a modern venue for the conduct of Physical Protection and Nuclear Material Accounting and Control (NMAC) training, addressing both the theoretical and the practical elements of the two inter-related programs. Course development is in progress to address multiple elements of Physical Protection and NMAC programs, focusing on compliance to Kazakhstan regulations and International Atomic Energy Agency (IAEA) guidelines. Specific attention is being placed on the recommendations detailed in Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5) (IAEA Nuclear Security Series No. 13) and the Implementing Guide for the Use of Nuclear Material Accounting and Control for Nuclear Security Purposes at Facilities (IAEA Nuclear Security Series No. 25-G). The NSTC is intended to serve as a primary training location for Kazakhstan Nuclear Security and NMAC personnel, as well as to provide a regional training center on nuclear security related topics, ranging from courses at the fundamental level to more advanced and specialized training topics. Further, the center will serve as a venue for other related training, workshops, and meetings.

Features of the NSTC include: • Classrooms for lectures and other theoretical training, equipped with Smart Boards, and video projection equipment, • A nuclear facility security perimeter mockup, including barriers, alarm sensors, lighting, and video assessment equipment, • An access control training room, including appropriate access control equipment, radiation portal monitoring equipment and supporting hardware, • An intrusion alarm and assessment training room, including mockups of both video assessment and alarm sensors, • An enclosed vehicle access control portal, including inspection equipment and radiation monitoring equipment, and

A dedicated NMAC practical training classroom, equipped with mass measurement and non-destructive assay measurement equipment.

This paper and poster presentation provides background on the cooperative efforts between the INP and DOE/NNSA on the planning and construction of the NSTC, a pictorial and narrative summary of current training facilities and capabilities, and details regarding plans for training program development at the center.

Synopsis ID: [151]

Development of Physical Protection Educational Laboratories in the National Research Nuclear University MEPhI

Krasnoborodko, A.[1], Geraskin, N.[1]

[1] National Research Nuclear University MEPhI, Russian Federation

Corresponding Speaker: A. Krasnoborodko

NRNU MEPhI have the 20-year experience gained by experts in developing and implementing the educational programs of different graduate levels in the area of Nuclear Security. There are the Master of Science Graduate Program and Engineer Degree Program. To train high level specialists is needed laboratory with modern equipment. Joint efforts undertaken by the RF State corporation Rosatom, US Department of Energy, and MEPhI have resulted in creating the MS Graduate Program (MGP) in Nuclear material (NM) Physical Protection, Control and Accountability at MEPhI Department "Theoretical and Experimental Physics of Nuclear Reactors" in 1997. The educational program takes two academic years and the program has been developed for training of those persons, who have already completed technical education at the level of Engineer or Bachelor of Sciences in the associated directions. The graduates receive the MS degree in Physics. In 2001 further joint efforts was started the Engineer Degree Program (EDP) "Safeguards and Non-Proliferation of Nuclear Materials". This educational program takes 5,5 academic years. Under the EDP the students have an opportunity to have a specialized training in the following two directions: NM control and accountability and physical protection of nuclear objects and materials. The graduates from the areas of NS and NM physical protection shall: - Know all the regulatory requirements to physical protection systems (PPS) of nuclear objects, methodology for PPS development and upgrading, have a clear notion about a variety of PPS engineering and technical tools; - Have a capability to prepare the technical requirements on PPS creating or upgrading, have a capability to estimate the proposed decisions, organize and conduct the works on PPS creating or upgrading; - Have a capability to apply the methodologies for assessment of PPS effectiveness. PPS training laboratories have been created at MEPhI in 1998, under financial support from the US Department of Energy, and now, continued of financial support made enabled a major equipment update. Currently, the following PPS training laboratories are under construction and particularly in operation in university: "Interior sensors for physical protection systems"; "Access control and management system"; "Video-surveillance systems"; "Data acquisition and processing systems"; Laboratorial facility "Remote monitoring systems". The educational process in the PPS training and research laboratories includes studying the following PPS components: - detection systems and tools for physical protection of rooms buildings and perimeters, methodologies and specific features in their applications; - access control systems and tools: identification tools, control and management systems, devices of biometrical

identification, executive means, methods and technologies for creation of the distributed access control networks; - main components of video-surveillance system: camera-system, tools for transmission of video-pictures, commuters, recorders, methods and technologies for creation of the distributed video-surveillance networks; - methods and technologies for creation of the integrated security systems - alarm systems through radio-channels and telephone lines, the integrated PPS including systems for protection and situation assessment at lengthy perimeters; - fire alarm systems and automated systems. New educational equipment was installed in the PPS laboratories, and the works are currently underway on creation of new laboratorial facilities and development of new laboratorial practical works.

Synopsis ID: [155]

A Study on Systematic Implementation of Force on Force Exercise

Kang, M.[1], Kang, Y.[1]

[1] Korea Institute of Nuclear Nonproliferation and Control, Republic of Korea

Corresponding Speaker: M. Kang

The threat of terrorism to nuclear facilities is increasing globally, and the IAEA has established a Nuclear Security Program and instituted a series of publications on nuclear security to provide recommendations and guidance that member states can use in establishing, implementing and maintaining their national nuclear security regime.

INFCIRC/225/Revision 5 recommended that force-on-force exercise, including timely response of the guards and response forces, should be conducted regularly to determine reliability and effectiveness of physical protection system against the threat. These should be carried out with full cooperation between the operator and response forces. Performance testing of the physical protection system should include appropriate exercises, for example force-on-force exercises, to determine if the response forces can provide an effective and timely response to prevent sabotage. Significant deficiencies and actions taken should be reported as stipulated by the competent authority. The IAEA is also preparing force-on-force exercise program documents to support exercise of member states. Currently, ROK is implementing exercise on the force-on-force exercise evaluation system which is developed by itself for the nuclear power plant, and it is necessary to establish the exercise procedure considering the use of the force-on-force exercise evaluation system.

The purpose of this study is to establish the work procedures of the three major organizations related to the force-on-force exercise of nuclear power plants in ROK, which conduct exercise using force-on-force exercise evaluation system. The three major organizations are composed of licensee, KINAC, and the NSSC. Major activities are as follows. First, the licensee establishes and conducts an exercise plan, and when recommendations are derived from the result of the exercise, it prepares and carries out a force-on-force result report including a plan for implementation of the recommendations. Other detailed tasks include consultation with surrounding units for adversary, interviews with exercise participants, support for document evaluation, and self-training to improve the familiarity of the MILES. Second, KINAC establishes a force-on-force exercise plan review report and reviews the force-on-force exercise plan report established by licensee. Evaluate using exercise evaluation system and prepare training evaluation report. Other detailed tasks include MILES training, adversary consultation, management of exercise evaluation systems, and analysis of exercise evaluation results. Finally, the NSSC decides whether or not to approve the force-on-force exercise and makes a correction request to

the nuclear facility based on the exercise results. The most important part of ROK's force-on-force exercise system is the analysis through the exercise evaluation system implemented by KINAC after the exercise. The analytical method proceeds in the order of collecting data from the exercise evaluation system and analyzing the collected data.

The exercise application process of the exercise evaluation system introduced in ROK in 2016 will be concretely set up, and a system will be established to provide objective and consistent conclusions between exercise sessions. Based on the conclusions drawn up, the ultimate goal is to complement the physical protection system of licensee so that the system makes licensee respond effectively and timely against sabotage or unauthorized removal of nuclear materials.

Synopsis ID: [305]

Similarities and Differences of Nuclear Security Culture and its Self-Assessment in Nuclear Power Plant and Research Reactor

Khairul, K.[1], Yankov, V.[2], Antariksawan, A.[3]

[1] Center for Information and Nuclear Strategic Zone Utilization-BATAN, Indonesia

[2] Kozloduy NPP Plc, Security Division, Bulgaria

[3] Center for Nuclear Reactor Technology and Safety-BATAN, Serpong Nuclear Research Complex, Indonesia

Corresponding Speaker: V. Yankov

This paper is based on the experience of conducting pilot self-assessments of security culture at Indonesia's research reactors in 2012-2013, 2nd self-assessment 2015-2016 and Kozloduy NPP in 2014 and the efforts to enhancement the nuclear security culture afterwards. These were the first ever projects globally to put to the test the emerging IAEA self-assessment methodology for security culture at a nuclear facilities. The two objectives successfully accomplished were to hold a proof of principle for the IAEA methodology which was still under development at that time and identify security culture weaknesses and strengths at the corresponding facilities.

These two self-assessments showed that there are some specifics in conducting self-assessment in research reactors and nuclear power plants. Furthermore, the results from these self-assessments were quite different and the action plans developed after that used different approaches for enhancement of the nuclear security culture. Of course, since both self-assessments were conducted using same methodology, there were a lot of similarities as well.

Now when the IAEA Technical Guidance for Self-Assessment of Nuclear Security Culture has been finalized and is about to be released in the Nuclear Security Series for the use by IAEA member states, it is important to compare the experience related to the practical conducting of the self-assessments in different facilities. As the IAEA methodology gains traction globally, stakeholders must have a reasonably precise idea on what they can expect from undertaking self-assessment of security culture at different facilities which use nuclear and radioactive material.

Synopsis ID: [183]

Overview on CNESTEN Human Reliability Program

Abbassi, H.[1], Mellouki, R.[1], Ghazlane, H.[1], Boucetta, A.[1]

[1] National Center for Nuclear Energy, Sciences and Technology (CNESTEN)/ Morocco

Corresponding Speaker: H. Abbassi

A Human Reliability Program (HRP) is a "security and safety" reliability program designed to ensure that individuals who occupy positions allowing access to certain nuclear materials, facilities and programs meet the highest standards of: - Reliability : individual's ability to adhere to security and safety rules and regulations, - Trustworthiness, and - Physical and mental suitability. Development and implementation of an HRP can greatly strengthen both safety and security cultures in a nuclear facility. In this purpose, the National Centre for Nuclear Energy, Sciences and Technology (CNESTEN) launched officially its HRP since June, 2016. The objective of CNESTEN's HRP is to ensure a high level of safety and security during the operation of CNESTEN facilities and the conduct of its own activities. The process of lunching CNESTEN' HRP program is being supported by bilateral cooperation with the US Department of State through Partnership of Nuclear Security (PNS).

The concept of CNESTEN's HRP has been implemented following the five important steps below:

1. Establishing requirements for critical positions 2. Identifying critical functions and positions

3. Assessing regularly the compliance with the above mentioned requirements 4. Maintaining a certification system 5. Reviewing periodically the HRP program An Executive Committee (EC) has been established to manage CNESTEN's HRP Program. The EC is carrying out its activities in accordance with its Term of References Document which describes roles, responsibilities and process followed by the EC. . HRP implementation begins with defining criteria and requirements related to critical positions in the program. The main criteria adopted are the followings: 1. access to nuclear Material 2. access to radioactive sources with high activities 3. access to sensitive systems and information.

Once HRP critical positions were identified, workers received appropriate training for their positions. The training program includes the following elements: - HRP objectives, - components of the program/ responsibilities - benefits and positive aspects of the HRP - awareness on nuclear security - awareness on the medical component of HRP - behavior observation. CNESTEN's HRP involves three main components: - Manager review: Managers are an integral part of ensuring worker safety and security. They make a recommendation on HRP certification to EC based on a periodic assessment. - Medical assessment: a Medical doctor (occupational health physician) performs assessment of staff in critical positions based upon qualifications required for the specific position. Medical doctor makes recommendations on HRP certification to EC based on a periodic assessment.

- Security evaluation: Perform security review of all staff in critical positions (employees and subcontractors). The Security manager makes recommendations on HRP certification to EC based on security aspects. The manager's evaluation, medical assessment, and security aspects are submitted to the EC. A comprehensive recommendation is made after consideration of all the relevant information. Based upon the recommendation of the EC, the General Director of CNESTEN makes the final decision regarding HRP certification of an individual. Once an employee has been accepted into an HRP position, he is subject to an annual and continuous evaluation process to ensure sustained eligibility for his own critical position.

Synopsis ID: [158]

Strengthening Nuclear Security Culture within Public Company "Nuclear Facilities of Serbia"

Mladenovic, M.[1], Arbutina, D.[1], Milanovic, S.[1]

[1] Public Company Nuclear Facilities of Serbia, Serbia

Corresponding Speaker: M. Mladenovic

Public Company Nuclear Facilities of Serbia (hereinafter PC NFS) is the only nuclear operator in Serbia. It was founded in 2009 under the Law on Ionizing Radiation together with the Serbian Regulatory Body. Since its establishment, PC NFS has continued all nuclear activities previously managed by Vinca Institute of Nuclear Sciences; Two research reactors (RA-final shut down and RB- zero-power critical assembly, operational but currently not-licensed), RWM facilities- old Hangars H1 and H2 with legacy waste, new hangar H3 (for the storage of intermediate and low level radioactive waste) together with the secure storage for the high activity sealed radioactive sources, and closed uranium mine Kalna are the part of the Company. In autumn 2015, PC NFS has signed research agreement with IAEA under CRP on Development of Nu- clear Security Culture Enhancement Solutions(NSCES) with following research objectives and anticipated outcomes: adoption on nuclear security objectives; defining the key actions that contributes to the strong nuclear security culture; presenting the responsibilities and roles of state, regulatory body, management and individuals in strengthening the nuclear security culture to our employees; establishing system with clear roles, objectives and responsibilities; communicate across organizational boundaries, integrated management system as a common principle for safety and security at all levels, with proper coordination and cooperation, with a result in optimum protection . Scope of this paper is to provide the results from the 1st and 2nd year of work on the enhancing the nuclear security culture, development of trainings, cooperation with IAEA and other relevant institutions such as US DoE, WINS, etc. in order to implement international best practice and providing PC NFS strategic plans in the field of nuclear security culture (as well as providing the interface between safety and security culture within PC NFS). The 1st year results were first time shown at International Conference on Nuclear Security: Commitments and Actions, Vienna, Austria; 5-9 December 2016 where we have presented the results of the first self-assessment survey which has covered almost all of our employees (both security and non-security staff) which gave us the broader picture about the zero-point status of nuclear security culture and was the input for the interview phase- both group and individual where our psychologist (member of our expert team for monitoring the implementation of nuclear security culture (in charge for the development and application of self-assessment methodologies)) played the key role. Paper will cover analysis of self-assessment survey, interview

results, issues that we were facing with, as well as our recommendations for future upgrades of the interview techniques.

Synopsis ID: [75]

Polish Experiences in Self-Assessment of Nuclear Security Culture

Wiśniewska, M.[1]

[1] Poznan University of Technology, Poland

Corresponding Speaker: M. Wiśniewska

The main goal of the paper is to share the recent experiences gained during the research on self-assessment in Nuclear Security Culture conducted in medical facility in Poland. The project is supported by the IAEA under the Programme of Coordinated Research Activities from 2015 till 2018, under the name "Enhancement of Nuclear Security Culture in Medical Institutions Using Radioactive Sources and Materials". The main aim of the research is to promote, enhance and sustain Nuclear Security Culture attitudes among personnel who use or have access to radioactive facilities and materials in medical institution. During the study, the importance of the human factor in the security discipline and the value of self-awareness and responsibility of personnel is stressed out. Moreover, the researchers' goal is to tailor the self-assessment tool to the institution's needs. The research started in 2015 and is planned to be finished till the end of 2018. The programme runs at medical facility, second private radiotherapy center in Poland, located in Poznan, specializes in nuclear medicine, equipped with state-of-the-art General Electric PET/CT, MRI and ANGIO equipment. The poster presents the experiences from the research process in Radiotherapy Department. The research process starts with documents' review and discussions, then a survey and finally the interview in the focus group take place. The goal of the poster is also to share the experiences of the self-assessment team in cooperation with Radiotherapy Department. The research in Radiotherapy Department is perceived as completed when the self-assessment tool is accepted by the team and self-assessment survey in Nuclear Security Culture is done and concluded. After the report is finished, the next stage of research work can begin, according to the plan. The next part of research activity is addressed to PET's personnel of different levels in hierarchy, in the same medical institution using radioactive sources and materials. The same scientific approach is taken into account as in Radiotherapy Department. The findings from Radiotherapy and PET Departments are to be compared and combined. According to the programme, the self-assessment team moves to the next stage of the project, which is the Nuclear Security Culture self-assessment in other medical subsidiaries in Poland to make medical and non-medical personnel be continuously aware of their responsibilities due to their work with radioactive sources and materials. The overriding purpose is to let them understand what can be the consequences of their irresponsible or unaware behavior. Concluding, the goal of the project is to make each member of the organization, especially non-security personnel, become involved in promoting, enhancing and sustaining nuclear security culture approach. However, it shall not be

forgotten that example comes from the top. Managers at all levels in hierarchy and staff need to be convinced that Nuclear Security Culture is important.

Synopsis ID: [70]

Are You an Insider?

Rezende Martins, L.[1]

[1] CTMSP Brazil

Corresponding Speaker: L. Rezende Martins

This paper intends to present o different view of insider threat. Aiming the person, the poster induces the reader to think about his/her behavior. In the poster, several items will be displayed and they will lead the reader to meditate about what to do or what not to do. In the poster, named "Are You an Insider?", the author intends to ask some questions about the reader's behavior that will indicate the potential to be an insider. There will be questions about the behavior in and out of the facility. Unless the facility has a strong security awareness, the employees, contractors and visitants are not alert to those behaviors. All questions are based on the IAEA Nuclear Security Series No. 8 [1] and on author's experiences in Brazil.

Synopsis ID: [20]

Assessment of Educational Approaches To Strength the Physical Protection Regime of Turkey from Point Of View Nuclear Security Culture

Yücel, H.[1], Narttürk, R.[1]

[1] Ankara University, Institute of Nuclear Sciences, Turkey

Corresponding Speaker: H. Yücel

It is a fact that the nuclear security regime requires a global responsibility among the States because the risks related to nuclear security have a global impact. Hence, all States should work together to response effectively to the threats appearing in homeland or global scale threats. This needs to build a strong nuclear security regime for each State. The international instruments such as the International Convention for the Suppression of Acts of Nuclear Terrorism, the Code of Conduct on the Safety and Security of Radioactive Sources, International Convention on the Physical Protection of Nuclear Material (CPPNM) and its new Amendment, and also a Guidance on the Import and Export on the Radioactive Sources can help to enhance the security of radioactive and nuclear materials and associated facilities. This requires to adhere to the provisions and rules of these Conventions under auspices of IAEA's broad umbrella in perspective of nuclear security culture. In the current situation, a wave of violence is raising along our long southern borders due to the on-going civil war and domestic violence affecting this region. It is likely that well-organized terrorist groups may obtain radioactive or nuclear materials and use them for their attractive targets. It is likely that terrorists can cross the borders and jeopardize Turkey's security because these materials might accompany the movement of displaced persons throughout the region. Normally the radioactive and nuclear materials used in Turkey are maintained under the regulatory control of the Turkish Atomic Energy Authority. In view of peaceful nuclear energy, Turkey ratified the NPT in 1979 and has a safeguards agreement in force with the IAEA since 1981 and the Additional Protocol to its safeguards agreement has been in force since 2001. The safeguards inspection mechanism provides a good challenge for Turkey to obtain international aid in case of emergency. Non-destructive measurement techniques such as gamma-ray spectrometry are used for detection of radioactive materials during their illicit trafficking. PVT based panel detectors are installed at some land border gates to monitor heavy goods transported by vehicles. The required equipment and well-educated radiation experts are still limited to characterize the smuggled radioactive nuclear materials, especially they are of interest in nuclear forensics. The aim of this presentation is to assess the present status of nuclear educational approaches to strength the physical protection regime of Turkey. The young generations should be instil on nuclear security culture for the physical protection of radioactive and nuclear

materials in use, storage and transport, and for nuclear facilities. Within the context, the courses on nuclear security should be given in curriculum of nuclear education programs at the undergraduate and graduate levels. This paper describes briefly educational approaches to train radiation workers in medical and industrial sectors, the academic courses given to the younger generations in higher education about ionising radiation and its measurement and interpretation capability, radiation protection problems, radioactive material handling and transportation and the necessary equipment to be used for identification or discrimination of the radioisotopes, mainly used in medical, industrial and nuclear research activities. It is essential that, to improve the measurement capacity for categorizing and characterizing radioactive and nuclear materials, educate the younger generations, Turkey has to find smarter solutions in which valuable nuclear knowledge and experience can be obtained from the nuclear community by developing more nuclear cooperation among the Organisations considering the importance of national and international obligations on radioactive and nuclear materials on the global nuclear security system.

Synopsis ID: [279]

Interaction of Nuclear Material Control and Accounting System and Physical Protection System for Nuclear Security Objectives

Bokov, D.[1]

[1] Rostechnadzor, Russian Federation

Corresponding Speaker: D. Bokov

Systems of Nuclear material control and accounting (NMAC) and Physical protection (PP) are two main component of Nuclear Security system at facilities, dealing with nuclear material. Both systems are actually independent and have different functions, but should interact and together ensure nuclear security of nuclear material. Paper indicates areas where NMAC and PP systems are complement each other, as well as difference in functions of both systems.

For example, regarding access control: usually PP system focuses on access control to areas and rooms (including where nuclear material is stored or used), while NMAC system focuses on access control on nuclear material. At the same time in practice both systems are complement each other and some equipment and procedures may be used by both systems (such as video surveillance equipment or two person rule) but sometimes in different way (for example, PP system may use video surveillance and two person rule for entrances to area/room while NMAC may use video surveillance and two person rule for control of handling and use of nuclear material).

Paper shows how requirements for PP and NMAC systems may complement each other, how both systems should interact to ensure effective nuclear security at facility.

Example of interface of NMAC and PP systems provided: both systems are taking part in authorization procedures, but they may be different in main responsibilities: it is PP system that provide authorized access and control of such access for personnel to protected areas (including locations with nuclear material), but it is NMAC system that request such authorization for personnel, working with nuclear material, so there should be interface on authorization of personnel between two systems. Another example is authorization for nuclear material shipment: while it is NMAC that prepare nuclear material for shipment and provide arrangements for authorization of such shipment, part of such arrangements should include notification to PP system (once shipment was authorized), so PP system would let the vehicle with nuclear material for authorized shipment out of protected area.

Synopsis ID: [208]

Cyber-Security Aspects of Physical Protection

DePhillips, M.[1]

[1] Brookhaven National Laboratory, United States of America

Corresponding Speaker: M. DePhillips

This presentation/poster will look at the possibility to compromise physical security though cyber-attacks from a hacker's perspective. Cyber-security can be complex in that an adversary can exploit knowledge learned from publically accessible documents such as INFCIRC/225/REVISION 5, combine this with information of nuclear facility security learned from the internet to create a credible threat to a facility. Risk, consequences and relevant safeguards will be presented with the intent of curtailing any successful attack on a facility and its employees. A thorough review of INFCIRC/225/REVISION 5 reveals robust recommendations for a thorough security plan protecting a nuclear facility. These guidelines include provisions for cyber security since many physical security devices and safeguards are attached to either a computer or a computer network. Gleaned from this document and through modest research of security systems at nuclear facilities, cyber-security for critical systems relies on access control to air-gapped systems. Although not impossible to penetrate, air-gapped systems are extremely difficult to compromise using conventional, remote, hacking techniques. However, since compromise of these systems will greatly increase the possibility of a successful attack on a facility, a determined adversary will look for a vector into these machines. Reconnaissance, part of the hacking cycle, will lead an adversary to INFCIRC/225/REVISION 5. Section 4.28 tells the reader that an access control list of users should be maintained at the site. Absent ability to break-in remotely, human compromise gives an adversary the best chance of success (i.e., the access control list). Although section

4.17 states that this list should be protected against manipulation and falsification compromise; it does not make mention that alternatively this is a targeting list, requiring a higher level of security, including security-in-depth (e.g., training). Somewhat inspired, a hacker will use all tools at their disposal, including conventional attacks (e.g., phishing), to obtain a copy of the list. A captured list is a valuable item, it does not guarantee access to nuclear material, but it may disrupt an employee's life. With the list, an adversary could attempt to access secure systems using social-engineering techniques fortified by social networks (e.g., Facebook) to the ruthless (e.g., compromised family member). Safeguards such as administrative (e.g., Operational Security training and awareness) and engineering constraints (e.g., encryption) will be presented to help mitigate these potential compromises.

Synopsis ID: [72]

Strengthening of Integrated Police Operations under a Multidisciplinary Approach to Prevention, Detection, Research, Reduction and Response to Radiological Threats

Bastidas Pazmiño, X.[1]

[1] Ministry of Interior, Ecuador

Corresponding Speaker: X. Bastidas Pazmiño

For the purposes of globalization and the integration of the regions of the world, new characteristics have been created within the criminal sphere, such as the illicit trafficking of nuclear and radioactive material, which has led to a renewal in the operation of the First Response Forces such as the National Police of Ecuador, in order to reduce the impact that the succession of a criminal act of this nature may have on people and the environment. In this context it is necessary to adopt strategies that minimize radiological risks from prevention in the strengthening of the capabilities of the police units considering that the crime and its forms transcend borders; For this purpose, it is necessary to foster the development of knowledge that allows the unification of integrated investigation and control procedures within the area of citizen security, in line with the actions of the State and the institutions that are immersed within the Integrated Plan for Security Support Nuclear physics. For this reason it has been necessary to implement an Integrated and multidisciplinary Unit from the Directorate General of Operations of the National Police of Ecuador to deal with the threats with these materials and have the human resource specialist in different areas, based on the combination of Scientific experience, specific technical infrastructure and availability to cover police operations in the treatment of threats with nuclear or radioactive material, under 3 fundamental objectives:

Strengthen response capacity to prevent, detect, research, prepare and respond to terrorist activities using nuclear material and provide an immediate level of reaction.

Strengthen the capacities and competencies needed to respond to a threat involving this type of materials.

Integrate into a single system the competencies of each of the specialized units, with a view to effectively coordinating, conducting and directing activities aimed at combating trafficking in nuclear material and other radioactive materials.

INTEGRATED POLICE OPERATIONS UNDER A MULTIDISCIPLINARY AP- PROACH IN THE PREVENTION, DETECTION, RESEARCH, REDUCTION AND RESPONSE TO RADIOLOGICAL THREATS.

ORGANIZATION OF THE INTEGRATED UNIT AGAINST NUCLEAR / RADI- OLOGICAL THREATS

GENERAL DIRECTION OF OPERATIONS OF THE NATIONAL POLICE OF ECUADOR

Maximum planning body for police operations. • Responsible for programming, coordinating, advising, supervising and evaluating the compliance of the Institutional operations. • Lead police operations to threats with radioactive materials. • Inter-institutional coordination with entities of the State immersed in the Integrated Plan to Support Nuclear Safety in Ecuador.

DGI (General Direction of Intelligence)

Classified information for crime prevention in the traffic of nuclear and radioactive material, as well as application of police information systems. • Identify actors whose interests are related to terrorist activities.

CRIMINALISM

Management of information sources in order to clarify the radiological crime, taking into account the key challenges of Nuclear Forensic Research, such as the storage and management of evidence.

Integration of the national response protocols, complying with an interface with the protocols of scenes of radiological crimes. • Identification of technical assistance needs and nuclear forensic expertise.

BORDER CONTINGENCY ADDRESS

Coordination of activities and cooperation in the detection of illicit traffic in nuclear and / or radioactive materials at borders and response to them.

INTERPOL / AMERIPOL ECUADOR OFFICES

International coordination with police agencies / handling and exchange of information by means of notification qualification, in reference to the radioactive material product of traffic and criminal organizations that are immersed in the same.internacional

UNIT OF CUSTOMS AND TAX CRIMES

Scientific technical investigation against customs crime that includes radioactive material product of the traffic, through scientific technical investigation; Intelligence to detect criminal organizations engaged in the smuggling of radioactive material.

GIR (INTERVENTION AND RESCUE GROUP GOE (GROUP OF SPECIAL OPERATIONS

Proactive forces of immediate reaction in crime prevention and high risk situations. • Specialized tactical knowledge. • Neutralization, deactivation and intervention of explosive devices that may contain radioactive material.

UPMA (Environmental Protection Unit)

Executing agency for environmental policies. • Detection of radioactive material from traffic products, in routine checks.

ULCO (UNIT OF FIGHT AGAINST ORGANIZED CRIME)

Police intelligence operations to prevent criminal acts with the use of nuclear / radioactive material, against national and international Organized Crime and its neutralization / disarticulation.

In conclusion, the transversality of the culture of nuclear security to the organizational culture applied to this multidisciplinary unit, is to have each of the specialties that integrate it, with a sustained approach to develop and maintain relationships between police experts through the exchange of Information, interaction, strategic advice, establishment of working groups, training and continuous training, optimizing the human resource and strengthening the police response to radiological crime.

Synopsis ID: [153]

Bayesian Approach for Intrusion Detection in Physical Protection System

Kang, M.[1]

[1] Korea Institute of Nuclear Nonproliferation and Control, Republic of Korea

Corresponding Speaker: M. Kang

Scientific detection devices play an important role in a physical protection system. They can detect unauthorized intrusion in real time through the CCTV or sensors installed in the fence around the protected area in nuclear power plants. The intrusion detection strengthens the monitoring inside and outside the protected area. If a blind spot is present in the monitoring through CCTVs, a serious problem for protection can occur. Thus, the this study aims to propose a methodology that can estimate the detection probability of unauthorized actions through the Bayesian approach when a person(s) moves into the blind spot, which is outside the detection area.

The probability calculation according to the Bayesian approach consists of prior probability, posterior probability, and likelihood function. The uncertainty of intrusion detection for the target (person) can be expressed with probability using given data. A specific event occurred already with a specific probability and the probability with regard to the cause of the event occurrence, that is, posterior probability can be calculated using information that is already known prior to event occurrence, that is, prior probability. The most likely intrusion and event information can be obtained within a probability between 0 and 1 according to prior information and the maximum likelihood function. The closer the posterior probability to 1, the more the intrusion becomes evident.

In this paper, the Bayesian approach introduced in the above paragraph is extended to a network model to propose the detection probability of abnormal activities. It is necessary to construct a profile consisting of two patterns: frequently occurring normal behavior pattern and infrequently occurring abnormal behavior pattern. By comparing new input values with the above two patterns, it's possible to distinguish between normal and abnormal behaviors and then calculate the probability.

A pattern can be defined as a path where a person moves from an arbitrary location cell to the next adjacent cell when the screen in the CCTV is divided into cells of fixed size. A moving path from the time a person is discovered in a single monitor of the CCTV to an arbitrary time is defined as a normal behavior pattern, which can be expressed with a probability chain type. A path that passes through a blind spot is defined as an abnormal behavior pattern, which can be also be expressed with a probability chain type. Xi consisting of moving path patterns of people in the i-th CCTV is dependent on previous moving path patterns in the CCTV (X1, X2, X3,...,Xi-1) and Ab that represents

an occurrence of abnormal behavior (blind spot passing or hiding). Thus, a continuous moving path pattern of people in the CCTV can be expressed via the Bayesian network.

The scientific detection equipment are an important component in a physical protection system but the blind spot of a CCTV makes the protection of facilities in nuclear power plants vulnerable. Accordingly, the this study can calculate the detection probability of abnormal behavior and estimate the vulnerable path of protection by using the Bayesian approach proposed in the present study based on prior information about blind spots in individual CCTVs. For the future study, time information about how long a person remains in each divided cell on the screen of the CCTV will be added to expand the network model to raise the reliability of detection probability.

Synopsis ID: [248]

Legislative and Regulatory Framework for Physical Protection of Nuclear and other Radioactive Material during Transport

Ofoegbu, E.[1], Bello, N.[1]

[1] Nigerian Nuclear Regulatory Authority, Nigeria

Corresponding Speaker: E. Ofoegbu

The Nigerian Nuclear Regulatory Authority was established by the Nuclear Safety and Radiation Protection Act 19 of 1995 (Act) with the sole responsibility for nuclear safety and radiological protection regulation in Nigeria. The NNRA ensures transport safety and security of nuclear and other radioactive material through its regulatory control programme. The Nigerian Transportation of Radioactive sources Regulations was developed in 2006, however this Regulation is currently undergoing review using the GSR Part 3. Security is not adequately provided for in the the current Transportation Regulations, although, the NNRA ensures that Licensees make adequate provision for the security of nuclear and other radioactive material during transport, this was depicted during the transportation the nuclear fuel for the research Reactor in 2004 and the transportation of the Gamma Irradiation source from Lagos to Abuja. Nigeria is currently reviewing its Safety and Security of Radioactive Sources Regulations and adequate provisions have been made for security. Plans are underway to develop a transport security Regulation for nuclear and other radioactive material in the country. Furthermore the Draft Nigerian Physical Protection of Nuclear Material and Nuclear Facility provides for the security of nuclear material during transportation. Nigeria is also planning for the core conversion of the NIRR-1 nuclear fuel from High Enriched to Low Enriched Uranium and this will involve the transportation of the fresh fuel and the irradiated fuel to and from the facility and Nigeria is currently collaborating with some international stakeholders to ensure the safety and security of the nuclear fuel to and from the facility. This presentation therefore will give an overview of Nigeria current and future activities in the area of transport security for nuclear and other material.

Synopsis ID: [299]

A Proposal for Security Force Training and Qualification in Physical Protection

Cartaxo Da Costa, M.[1]

[1] Command of Land Operations of Brazilian Army, Brazil

Corresponding Speaker: M. Cartaxo Da Costa

I. INTRODUCTION

In compliance with the legal norms that regulate the physical protection of nuclear installations, it is of fundamental importance that members of the Security Force have excellent training and qualification in physical protection, considering their importance for installations security and radiological protection of individuals occupationally exposed to radiation and the public. Taking into account the needs and specificities of each area, topics are presented for the training and qualification process development, and improvements are suggested.

II.OBJECTIVE

The objective of this work is to present a proposal for Security Force members training and qualification in the matter of physical protection.

CRITERIA FOR PHYSICAL PROTECTION SERVICE PERSONNEL SELECTION

The selection of candidates, as well as their permanence in the Physical Protection Service, with a view to their loyalty and reliability, should be regulated by written procedures previously established, including, at least, the following requirements: 1) examination of the candidate life with a view to revealing unfavorable traits of character that may affect their abilities or motivation in the perfonnance of their duties; 2) medical and psychiatric examination to verify emotional instabilities that can render them incapable of performing their functions correctly; 3) permanent observation of all employees, with the objective of identifying abnormal procedures in the performance of their duties, and adopting appropriate corrective measures.

QUALIFICATION TOPICS

Security Force personnel should receive periodic training and retraining on subjects, practices and procedures appropriate for the effective performance of their duties including, but not limited to, the following topics:

purposes and principles of physical protection;

operation and testing of security systems and devices used;

individual authority and responsibility as part of the security force;

bombs and other types of threats;

actions to be taken to respond to emergency situations;

traffic control;

search and seizure methods;

writing reports;

rules, procedures and guidelines of the organization;

first aid;

basic guidance on radioprotection;

notions of technical facilities security;

emergency plan;

access controls;

security communications;

fire prevention and fighting;

self-defense techniques and weapons knowledge;

visit to radioactive and nuclear facilities;

conducting exercises and tests at the facilities by the Direction of the Department of Coordi- nation of the Protection System to the Brazilian Nuclear Program (Sipron); and

visit to the Support Force (Armed Forces or Auxiliary Forces unit) , previously designated to provide support within its sphere of competence, to a certain operational unit in an emergency situation).

CONCLUSION

Security Force members training and qualification process improvement requires the constant revision of CNEN NE 2.01 Norm, updating it in terms of the new areas of action, adapting it to the market demands and incorporating some improvements identified as necessary by the national nuclear authority and the users. This should be a dynamic process, seeking to keep abreast of market requirements, technological development and social needs. Currently, CNEN NE 2.01 Norm is being revised, according to CNEN-PR Ordinance No. 123, dated November 4, 2016, and will be renamed as NN 2.01 "Physical Security of Nuclear Materials and Facilities".

REFERENCES

Law No. 12,731, of November 21, 2012, which instituted the Brazilian Nuclear Program Protection System- Sipron.

National Nuclear Energy Commission, CNEN NE 2.01 Norm "Nuclear Area Operating Units Physical Protection". 2011.

Ordinance No. 21 I GSIPR, of June 2, 2011, which regulates the activities of the Brazilian Nuclear Program Protection Commission - COPRON.

Ordinance No. 8 I GSIPR, of March 24, 2011, which regulates the activities of the Planning Committee for Response to Nuclear Emergency Situations in the Municipality of Angra dos Reis - COPREN I AR.

Ordinance No. 31 I GSIPR, of March 26, 2012, which creates the Brazilian Nuclear Program Protection System Articulation Committee for the Security and Logistics Areas - CASLON.

Ordinance No. 40 I GSIPR, of June 25, 2012, which regulates the activities of the Planning Committee for Response to Nuclear Emergency Situations in the Municipality of Resende - COPREN I RES.

NG-03 - Sipron General Norm for Physical Integrity and Emergency Situations at Nuclear Facilities, of June 19,

Synopsis ID: [91]

Improvement of Transportation Protection System Using Fusion Technology

Kang, Y.[1], Koh, M.[1]

[1] KINAC (Korea)

Corresponding Speaker: Y. Kang

The ROK has laid down the Act on Physical Protection and Radiological Emergency (hereinafter "APPRE") based on the INFCIRC 225 of the IAEA and has been regulating the protection of nuclear materials during transportation. The transportation protection inspection of nuclear material is carried out according to the classification of the nuclear material and the 100% witness inspection is carried out in the case of transporting the nuclear material in the grade that uses the external road as of 2016. The ROK has difficulties in diversifying the route and time of transportation because the size of the territory is small, the population is dense, the road is stagnant at the time of commute, and the processing and suppliers of nuclear fuel are limited.

Therefore, the transport inspection is carried out under the application of higher protection requirement than IAEA recommendations according to the APPRE. This paper is also based on the same viewpoint, we propose a future method to systematically enhance the security level of transportation protection through the rapidly developing fusion technology. The method proposed in this paper may need to be revised according to the level of the national communication infrastructure and the cooperation system of the police or military. Transportation of nuclear material is generally the transfer from nuclear facilities to other nuclear facilities. In the case of nuclear fuels imported from overseas, international ports are used, and the facility is designated as a national important facility and has a high level of security facilities. However, transportation of nuclear material is relatively weak because it can not utilize the high level of scientific security equipment or physical barriers of the facility, and most measures must be resolved quickly by the security guard and the driver, and when the threat occurs, But it is important to contact the local police and the army quickly for emergency contact. In this way, it is very important to have a good communication, security guard and driver 's role in transportation protection. In addition to protecting against these threats, it is also important to show that the public is aligned and dominated on the roads available to the public and that a high-level security system is available. In order to overcome the above problem, we propose a transport protection system with fusion technology. This system is still a conceptual design stage and it is not a system currently in use in Korea. This system is a combination of IT technology and BT technology, and a similar type of solution is actively used in banking or electronic commerce. First, in the case of communication network construction, 4g LTE based communication that puts the server outside the communication is replaced with the communication using the current radio.

Voice chat system is already used through games, messenger, etc., and can be used regardless of distance if it belongs only to 4g LTE. Korea's LTE coverage is the top in the world and includes 95% of the country. The content of the communication is primarily protected by general obfuscation function, and it is impossible to eavesdrop on the ARIA-256 which is designated by the ROK standard encryption algorithm in 2004. Components participating in transportation using this system are mobile vehicle control center, individual transportation vehicle, police vehicle and communication network centered on the external server (central control room). Each car operates an Android-based development terminal. It connects to an external server in the form of an Android application and restricts the number of users using encrypted keys to a minimum. However, if the user is authenticated, can connect sever anywhere. In addition, in this paper, we propose an authentication method for security guard using FIDO technology standard, a method of generating threating code by introducing a new device S-glass, a request for protection of local police using local based system, and how to control the vehicle sequence using vehicle to vehicle communication. In addition to a description of the element technology, a scenario of a virtual nuclear material transport using this system will also be introduced. In conclusion, it is expected that the verification of these scenario will enable us to grasp the advantages and disadvantages of the system, and partially improve the current transportation protection system even if the whole technology is not introduced at once. As such, KINAC conducts various research activities in preparation for future regulatory environments as well as general transport inspection based on APPRE.

Synopsis ID: [261]

Development of Information Security Policy for Thailand Nuclear Regulatory Body

Maneechayangkoon, R.[1], Siripirom, P.[1], Watcharasuragul, V.[1], Srimok, B. [1]

[1] Office Atoms for Peace, Thailand

Corresponding Speaker: R. Maneechayangkoon

Thailand has been a Member State of the International Atomic Energy Agency since 1961 and has just issued a new Nuclear Energy for Peace Act which reflects all stages of licensing process and comply with international legal instruments since February 1, 2017. Therefore, Office of Atoms for Peace (OAP), the only nuclear regulatory body in Thailand, need to review and develop the regulations and also the nuclear policy especially the information security policy since the current policy is out-of-date (last updated: March 2012) and inadequate for protection against Cyber Crime nowadays.

Thailand has taken steps to conduct the sensitive information analysis in accordance with the International standard such as IAEA standard especially the information security by "identifying sensitive information", "classifying and prioritizing the data", etc. It appeared that there are gaps that might be vulnerable to Cyber Crime. Outcome of this paper will provide the OAP with guideline and framework for developing the new information security policy for better confidentiality, integrity and availability of information assets. One of them is to have a clear definition of roles and responsibilities for ensuring information security is effective throughout the organization.

Synopsis ID: [285]

Overview of the International Training Course for Computer Security

Nickerson, C.[1], Solit, J.[2], West, R.[3]

[1] Idaho National Laboratory, Department Of Energy, United States of America

[2] US Department Of Energy, United States of America

[3] Los Alamos National Laboratory, Department Of Energy, United States of America

Corresponding Speaker: C. Nickerson

The United State National Nuclear Security Administration (NNSA) Defense Nuclear Nonprolifer- ation (DNN) has been actively engaged in working with the IAEA to promote and develop policies that mitigates risks to nuclear material. Of recent concern is the risk exposure of digital systems that are used to protect and safely work with nuclear materials. The NNSA has developed a comprehensive joint effort with the IAEA to develop policy recommendations, documentation, training, and technical counsel to enhance the cybersecurity of these systems. The NNSA and IAEA have agreed to continue this effort by collaboratively developing a new training course that will provide participants the opportunity to learn about issues and solutions in an immer- sive environment with practical (hands-on) examples and tools. This new course is called the "International Training Course For Computer Security."

STRAGETIC VISION OF THE COURSE The envisioned outcome of the course is to provide member states with foundational principles, methodologies, and tools from which they can strengthen their nuclear security regimes. The course will provide participants a venue to not only learn about these principles but also give them an opportunity to apply them against real equipment to visualize impacts of their decisions.

CORE IMPLEMENTATION OBJECTIVES To achieve the strategic vision, the NNSA and IAEA are developing a curriculum that will immerse attendees into digital frameworks used at nuclear facilities and demonstrate the challenges and potential solutions to a cyber enabled adversary. The course will be based on 5 core learning objectives: Develop an understanding of the digital ecosystem at a nuclear facility; Raise awareness of digital vulnerabilities and threat exploitation methods; Create familiarity with IAEA guidance, recommendations, and other internationally recognized/accepted resources; Increase risk assessment competencies by integrating cyber equities into existing processes; and Introduce risk mitigation strategies and verification, validation, and acceptance methodologies.

The course will be designed to foster interaction between participants across multiple domains within the nuclear industry to share common practices, discuss realities, and lessons learned. The course will be

predominantly hands-on exercises and demonstrations to maximize the learning opportunity and create a greater awareness of computer security impacts for nuclear facilities.

Synopsis ID: [218]

Computer Forensics and Nuclear Forensics in Uganda

Otim, A.[1]

[1] Atomic Energy Council, Uganda

Corresponding Speaker: A. Otim

The world has witnessed immense computer crimes in the recent past prompting immediate efforts to curb the vices through enhanced computer security techniques. Computer forensics is also needed in recovery as well as identification and prosecution of the perpetrators. With computer aided theft now becoming rampant in the Uganda, forensics expert and forensic laboratory to train Ugandans in cyber security is needed. According to Mr Mustapha Mugisha, one of the consultants at Summit Consulting, there is need for more forensics laboratories to give Ugandans world class specialized training that otherwise would have required them to go and get it from the United States, This is because there is still very little knowledge about computer security among computer users in Uganda, a loophole hackers have taken advantage of to hack into government websites, data bases, banks, mobile telecommunication companies as well as individuals to steal vital information that has led to theft of colossal sums of money. This paper focuses on characterizing what Uganda is doing at the national level and introduces a potential model for developing a national approach to computer forensics at nuclear facilities. Uganda nuclear security regime comprises of; the legislative and administrative systems of associated facilities using nuclear material and radioactive sources Uganda is working towards the implementation of regulatory framework and administrative systems of nu-clear security; nuclear security systems and measure for the prevention of detection and response to nu-clear security events. The purpose of the nuclear security regime is to prevent, detect and respond to nuclear security events (e.g. illicit trafficking of nuclear material or a nuclear terrorism attack). Nuclear forensic analysis is a key technical capability that utilizes signatures inherent to nuclear or other radioactive material to provide information on its source, production and history. It can be used as part of the response to the nuclear security event, as well as to help prevent it. This paper looks at potential challenges to achieve as traditional forensic science laboratories are not designed or designated to handle exhibits contaminated with nuclear or other radioactive material. Equally, analytical laboratories designated to support nuclear forensic analyses are not equipped with the instrumentation or the trained staff to undertake traditional forensic science examinations. The United Kingdom, in response to this technical challenge, has established a purpose built facility, the Conventional Forensic Analysis Capability (CFAC) at a nuclear licensed site to enable the examination of items contaminated with nuclear and other radioactive material using a range of traditional forensic science examination techniques.

Nuclear Forensic Capacity Building Developing and sustaining a nuclear forensic capability is a Uganda's responsibility. Elements such as infrastructure, legal and regulatory frameworks,

operations, human capital and specialized equipment and knowledge are critical to an effective nuclear forensic capability. Key words: Computer Forensic, Nuclear forensic, Forensic Laboratories, Nuclear Facility.

Synopsis ID: [119]

Self-Assessment on Cyber Security within Public Company "Nuclear Facilities of Serbia"

Žarković, D.[1], Mladenovic, M.[1], Arbutina, D.[1]

[1] Public Company Nuclear Facilities of Serbia, Serbia

Corresponding Speaker: D. Žarković

This paper will present results of self-assessment on cyber security of Physical Protection Systems (PPS) within Public Company Nuclear Facilities of Serbia (PC NFS). PC NFS was established in 2009 under Law on Radiation Protection and on Nuclear Safety. PC NFS is the only nuclear operator in the Republic of Serbia and is responsible for operation of heavy water critical assembly RB; decommissioning of the RA research reactor and management of all radioactive waste in Serbia (old hangars H1 and H2 with legacy waste and new hangar H3 for the storage of intermediate and low level radioactive waste). One of the goal of nuclear security is protection of computer systems from the theft or damage to their hardware, software or information, as well as from disruption or misdirection of the services they provide. Cyber security includes controlling physical access to the hardware, as well as protecting against harm that may come via network access, data and code injection. In the context of this publication, computer and cyber systems refer to the communication, instrumentation and control devices that make up functional elements of the PPS. They include not only desktop computers, mainframe systems, servers and network devices, but also lower level components such as embedded systems and programmable logic controllers (PLC). Scope of this paper will be cyber security on PPS in PC NFS. PPS in PC NFS covers Vinca site which includes mentioned research reactors RA and RB, hangars H1, H2 and H3 together with its secure storage as well as two units which operates with cat.1 sources and works under Institute of Nuclear Sciences "Vinca". PPS was upgraded in 2015 by donation from United States Department of Energy. Based on the IAEA guide for conducting computer security assessment at nuclear facilities, after the formal request, expert team was formed to conduct assessment. Part of the expert team Head of Department for nuclear security, systems control engineer and IT specialist (boat from department for nuclear security). At pre-assessment team meeting it was defined that scope will be only Physical protection domain: perimeter monitoring, access control systems, voice and data communication infrastructure, alarm systems and security clearance database. Also, it was defined that assessment will be conducted in 10 days and roles and responsibilities of team members were defined. Techniques used in this assessment were review of documentation, interviews and direct observation. During the assessment common vulnerabilities of computer systems were tested. Per example, software were tested for improper input validation, permission privilege and access control. Network configuration and configuration of computer systems were also tested. In autumn 2015, PC NFS has signed research agreement with IAEA under CRP on Development of Nuclear Security Culture Enhancement Solutions(NSCES). During interview

awareness of cyber threat was examined and level of cyber security culture was evaluated. These results will be used in order to enhance nuclear security culture in PC NFS. One month after the assessment final reported was made. Key finding, recommendation and suggestion from that report will be presented in this paper.

Synopsis ID: [64]

Nuclear Material Accounting and Control (NMAC) by Design at Pebble Bed Modular Reactor in Indonesia

Tri Jatmiko, D.[1]

[1] The GA Siwabessy Multipurpose Research Reactor (PRSG) – (BATAN)

Corresponding Speaker: D. Tri Jatmiko

The design of the Experimental Power Plant (RDE) development as a demo reactor for electricity generation, which will also be a process experiment for process heat applications in the framework of mastering the concept of cogeneration is currently being drafted by the National Nuclear Energy Agency (BATAN) as the authorized body to undertake the construction of non-commercial reactor. The nuclear reactor in the power plant design is a Pebble Bed Modular Reactor (PBMR) type with spherical fuel. The utilization of spherical nuclear fuel must be controlled and accounted for security by the physical protection system in nuclear facility including nuclear material therein. Based on nuclear material owned, the nuclear material in the PBMR facility including class II so that the security is done for 24 hours a day. The legal instruments of the physical protection system of nuclear material is increasingly strengthened by the implementation of various guidelines for the achievement of control system, especially the physical protection system of nuclear material in better nuclear facilities. One of the series of nuclear safety guidelines published by the IAEA in May 2015 is the Use of Nuclear Material Accounting and Control (NMAC) for Nuclear Security Purposes at Facilities (NSS-25-G). With this latest publication, one of the problems that arise related to the implementation of monitoring and security system in PBMR is how to arrange NMAC by design as an effort to effectively and efficiently implement the interface between the physical protection system and safeguards of nuclear material. This paper will describe the preparation of NMAC by design on PBMR beginning with the design of the organizational structure between of security and safeguards collaboration which will synergize in the control and monitoring of nuclear materials inside the nuclear facility so that the reporting of the absence of nuclear materials in the facility to the IAEA can be complete and correctness. Next design of the physical protection systems is implementation at the fresh fuel storage as a Key Measurement Point (KMP) by preparing a design to procedure that contains recordings in the receivement of fresh fuel and the other security aspect include transportation nuclear material therein. NMAC by design to the next are to design of the physical protection system in the application of a layered defense system and the use of Containment and Surveillance (C/S) as part of a control system at certain points outside and inside a fresh fuel storage it could be continue to monitoring by receivement and storage activities fresh fuel in the storage. Another thing that is required in NMAC by design is the design of the application of the physical ptotection systems and the controlling of spent fuel after exiting the reactor core. Nuclear fuel element after burning inside the reactor core consists of 2 types, namely

fuel with low burn up value and will be put back into the reactor, as well as fuel that will be put into second hand fuel storage pool due to burn up high or damaged when burned inside the reactor. NMAC by design activities required to support the physical protection system in PBMR are designed using Flow Counting Monitor (FCM) which measures the amount and flow of fuel out of the reactor and the placement of measuring instruments in the form of spectrometer gamma detector equipment to measure nuclear fuel burn up and C/S devices as a supporter of the physical protection system at certain points of monitoring. The next design is the required by placing barrier and the design of the physical protection system by placing the C/S device in a spent fuel storage to ensure that the control and monitoring of spent fuel can be monitored continuously. NMAC by design is also applied to other locations within nuclear facilities to ensure absence and the use of nuclear material for peaceful purposes only. The NMAC by design result is expected to be used as an effort to effectively and efficiently design the application of the physical protection system at The PBMR in Indonesia. Key words : design, security, reactor

Synopsis ID: [39]

Mexico and International Cooperation

Cruz Reyes, Z.[1]

[1] Ministry of Energy, Mexico

Corresponding Speaker: Z. Cruz Reyes

The Convention of Physical Protection of Nuclear Material and its Amendment is a tool that the Member States of International Atomic Energy Agency (IAEA) have to strengthen their physical protection regime under international recommendations. Since the beginning of the peaceful use of nuclear energy, the Sates seeking to protect nuclear material and nuclear facilities of any kind of actions that can release significant amounts of radioactive material which causes damage to people or to the environment. Nuclear material has a deep impact in human being everywhere, the uses of this materials are in different activities not only for nuclear energy and posterior transformation in electricity but in associated as medical, industrial, and academic uses . Although nuclear material has an important benefit for society worldwide, the nuclear weapons are a threat to the entire world. The nuclear weapons effects are devastators, like blast, thermal and nuclear radiation. To avoid the misused of nuclear material, and to strengthening the physical security regime the States promote mechanism and actions to improve nuclear materials security. Mexico is a Member State of IAEA since 1958, the Government of Mexico deposited with the IAEA its instrument of accession to the CPPNM on April 4, 1988 and deposited its instruments of ratification of the 2005 Amendment to the CPPNM on 1st August 2012. According to the Regulatory Law of Article 27 in Nuclear Matter , in Mexico nuclear energy only be used for peaceful purposes. In this document, it mention that nuclear fuels are property of the State, and only the federal government may authorize their use in accordance with this Law and the Secretariat of Energy (SENER) is responsible of it. Regarding this Law, the purpose of physical protection in nuclear facilities is to avoid intentional acts which harm or may harm public health and safety such as theft or the unauthorized use of nuclear materials. The National Commission of Nuclear Safety and Safeguards (CNSNS), inspects nuclear facilities to account for materials, to control and check the physical protection measures and the application of safeguards. Mexico has two Units BWR reactors with a capacity of 810 MWe each one at Laguna Verde of Federal Electricity Commission (CFE) property . The first unit has been operating since 1990 and the second one since 1995. In addition, National Institute for Nuclear Research (ININ) operates a 1MWe TRIGA MARK III research reactor . Technical support and assistance through bilateral and multilateral cooperation are fundamental steps to achieve a physical protection regime according with the best international recommendations, so, share good practices with other countries and organizations through seminars, training courses and workshop, promote best security practices Mexico actively participated with the different organizations worldwide in the nuclear theme, like IAEA, Nuclear Suppliers Group, Global Initiative to Combat Nuclear Terrorism and World Institute

for Nuclear Security, for mentioned few. The IAEA has developed a concept for the establishment and maintenance of a national Nuclear Security Support Centre (NSSC) as a mean to strengthen the sustainability of nuclear security in a State. The NSSC concept emphasizes the importance of effective processes and proven methodologies such as the Systematic Approach to Training (SAT) to analyzing needs and developing resources for nuclear security sustainability . The Government of Mexico through SENER, seeking to reinforce its capabilities in the human resources development, in promoting excellence in nuclear security through the establishment of high standards for nuclear security training, education, and qualifications, and with support of the Canadian Department of Foreign Affairs, Trade and Development, have signed a working agreement in the development of a sustainable and certified nuclear security training center. One of the scope of this project is to engage Mexican and Central America Region stakeholders to enhance skills development and contributing in the promotion of the physical protection regime. This proposal is aligned with the 2014-2017 National Action Plan for the Implementation of United Nations Security Council Resolution 1540 and its lines of Action called "capacity building measures as part of the strategy to combat the proliferation of weapons of mass destruction" . On the other hand, the Secretariat of Energy published in 2016, the National Electrical System Development Program (PRODESEN), which is a document that contains the planning of the national electrical system and meets the relevant elements of the indicative programs for the installation and decommissioning of power generation electric and expansion programs. This PRODESEN includes new generation projects and mentions three new reactors to enter in commercial operation by 2028, 2029 and 2030. With this in mind, the technical cooperation to develop new capabilities and reinforcement the actuals is necessary for the secure and safe use of nuclear energy in Mexico.

Synopsis ID: [42]

Challenges and Solutions for Sharing Classified Information with Licensees Using, Storing and Transporting High Risk Radioactive Sources

Duguay, R.[1]

[1] CNSC

Corresponding Speaker: M. Beaudette

Licensees and operators are required to implement security measures to address requirements set by the regulatory body or competent authority. These security requirements are generally based on the national threat level and information provided by the relevant law enforcement authority, intelligence agencies and other relevant stakeholders. However, not all States will share this information with radioactive sources holders, especially if they take a more prescriptive approach to regulation on security. The same situation often exists when a performance-based approach is used because there are multiple challenges that restrict the competent authority from sharing threat information with radioactive sources operators. In this paper, the author intends to identify these challenges and explore potential solutions to address these challenges without compromising the need to restrict classified information. The objective is to reflect on current practices to facilitate sharing of information between regulatory bodies and operators and to find innovative solutions to increase awareness about the threats and techniques used by the adversaries and assist stakeholders in being better prepared to address the threats without compromising the security of confidential information

International Atomic Energy Agency
IAEA-CN-254
Vienna International Centre
PO Box 100
1400 Vienna, Austria
Tel: +43 1 2600 (0) plus extension
Fax: +43 1 26007
Email: official.mail@iaea.org

Conference web site:
http://www-pub.iaea.org/iaeameetings/50819/Physical-Protection

CN-254

17-46131