Chapter 11
Technical Synergies Between Safeguards and Security

Elina Martikka, Tapani Hack, Marko Hämäläinen, Tapani Honkamaa, Paula Karhu, Mikael Moring, Olli Okko and Kari Peräjärvi

The objective of the state regulatory authority is to ensure that the use of nuclear energy is implemented in compliance with nuclear safety, security and safeguards. While nuclear safety measures aim to ensure the safety of normal operations, a low probability of accidents, and effective emergency preparedness, nuclear security and safeguards approach the joint fundamental objective from another angle, by combating unlawful and other intentional unauthorized acts. These objectives apply not only to the operating power plants but also to planning, designing, constructing and commissioning of the new nuclear installations and nuclear waste facilities as well as the decommissioning old facilities. Coordination of safety, security, safeguards, their interfaces, synergies and conflicts is essential for achieving the objectives.

New technologies, research and development are supporting verification and other measurement activities by the regulator. Close cooperation between research and development assist in confirming the safe and peaceful use of nuclear energy.

This paper discusses technical synergies between nuclear security and safeguards in the regulatory control of new nuclear power plants and new types of facilities, based on our experiences. Practical examples and possibilities to use new technologies, research, and development to confirm the safe, secure, and peaceful use of nuclear energy are given.

Nuclear energy has played an important role in electricity production in Finland since the beginning of the 1980s. In 2016, one quarter of Finland's electricity production was generated by nuclear power. The nuclear power plants (NPPs) in Finland are operated by Fortum in Loviisa and TVO in Olkiluoto. Each NPP has two operational reactors. TVO's third reactor OL3 is in commissioning. A new nuclear power company, Fennovoima, has also been granted a positive decision in

E. Martikka (✉) · T. Hack · M. Hämäläinen · T. Honkamaa · P. Karhu · M. Moring
O. Okko · K. Peräjärvi
Radiation an Nuclear Safety Authority, Helsinki, Finland
e-mail: elina.martikka@stuk.fi

L. Maiani et al. (eds.), *International Cooperation for Enhancing Nuclear Safety, Security, Safeguards and Non-proliferation–60 Years of IAEA and EURATOM*,
Springer Proceedings in Physics 206, https://doi.org/10.1007/978-3-662-57366-2_11

principle by Parliament for a nuclear power reactor, which it plans to construct in Pyhäjoki in the northern part of Finland.

It was legislated in 1980s that all spent nuclear fuel produced in Finland would be disposed of in Finland. The companies with operating NPPs, TVO and Fortum, cofounded the company Posiva to handle this task. The concept and a site for disposal of spent nuclear fuel was approved by a Decision in Principle in 2001. In November 2015 the Government granted the construction license. It was the first license for a geological repository for spent nuclear fuel in the world. The company Posiva is expected to apply for the operating license in 2020.

STUK is the regulatory authority for nuclear and radiation safety, nuclear security, and nuclear safeguards in Finland. Operators or licensees of a nuclear facility are responsible for fulfilling requirements stipulated in legislation and regulations as well as conditions and regulatory requirements set by STUK. In other words, operators are responsible for the necessary implementation of nuclear safety, security, and safeguards, and for enabling regulatory supervision in their facilities.

According to the IAEA Safeguards Agreement, the State has many responsibilities. In the Agreement, it is noted that the State also has many rights when the IAEA is implementing safeguards in the state. It is a duty of the regulatory authority to enable effective implementation of IAEA safeguards, while also ensuring that national security is not compromised.

Nuclear safety, security, and safeguards share the same fundamental objective: to protect people, society, the environment and future generations from the harmful effects of ionizing radiation.

The objective of nuclear security is to protect nuclear facilities and nuclear materials against unlawful and other unauthorized activities, primarily against theft and sabotage. A graded, risk-informed approach is applied to design, implementation, and assessment of nuclear security. Nuclear materials and facilities, including their systems, structures, and components, are categorized according to their significance to safety and security. The categorization is traditionally safety-based and security-based categorization is a somewhat newer concept, in particular with regard to cyber security considerations, which have become increasingly important.

The Design Basis Threat (DBT) in Finland consists of progressive levels of physical and cyber threats, and includes non-proliferation considerations. The scope of nuclear security in Finland is broad in comparison to the IAEA definitions. For example, nuclear security responsibilities and inspection programs in Finland cover other nuclear items in addition to uranium and plutonium, such as sensitive nuclear technology, including sensitive information.

The objective of nuclear safeguards is the prevention of the proliferation of nuclear weapons. The worldwide basis for safeguards is the Non-Proliferation Treaty (NPT) to which Finland is a party. The practical implementation of safeguards is based on the Safeguards Agreement between the State and the IAEA. Finland was the first state which had a comprehensive safeguards agreement

(INFCIRC/155) with the IAEA. In the European Union, the Euratom Treaty is also part of the overall safeguards structures.

Nuclear safeguards, the regulatory control of nuclear materials, is a prerequisite for the peaceful use of nuclear energy. The national system for the regulatory control of nuclear materials and activities forms the basis of nuclear safeguards. Nuclear safeguards are applied to both large- and medium-sized nuclear industry and to small-scale nuclear material activities. Along with safeguards, the regulatory process for nuclear non-proliferation includes transport control, export control, border control, international cooperation, and monitoring compliance with the Comprehensive Nuclear-Test-Ban Treaty (CTBT).

As mentioned before, safeguards and nuclear security share a common goal. Nuclear security is mainly concerned with the acts of non-state actors such as individuals or groups, while the main concern of safeguards is the actions of the State itself. Often nuclear security measures can be used for both purposes. E.g. compartmentalization of duties may help to protect nuclear material from being diverted from its original purposes, both at State and non-state levels.

For facilities handling nuclear material only as items, such as nuclear power plants, interfaces between safeguards, security and safety should be taken into account when considering possible control measures, such as item monitoring, use of radiation portal monitors and, if appropriate, metal detectors. The systems that are used for mainly one purpose, can be used for other purposes too.

Nuclear security is a national responsibility and binding requirements are not common. Convention of Physical Protection of Nuclear Material, as Amended (CPPNME) is the key document for nuclear security. Safeguards is much more regulated by international agreements and conventions. However, at the national level it should be carefully assessed, how these requirements can be fulfilled to achieve the common goal.

For new nuclear facilities, it is typically easier to design systems, structures, and components taking into account both security and safeguards requirements than for old facilities where modifications may be difficult to implement. In the design process of a new facility, it is important to share information between safety, safeguards and security experts and other stakeholders (e.g. rescue personnel). A need-to-know principle is commonly used, but there is also a need-to-share. If the information is not shared between these two parties, the common objective is more difficult to achieve.

The traditional concept of implementing safeguards is that safeguards measures are put in place by the authorities and international inspectorates, once the facility is built and ready for operation. Our experiences of the current demands on the safety and security of new nuclear power plants and new types of nuclear facilities, show that adding safeguards measures late can become very difficult and costly, so early consideration of safeguards and security is very important. Safeguards and security

measures are now a part of the design process of both the Hanhikivi NPP and Posiva repository projects.

After Parliament has made the Decision in Principle, that states that the construction and operation of a new nuclear facility is for the overall good of Finnish society, the operator can start the planning and the bidding process. During that process, there is classified information, which requires export or import licenses, end user statements, Nuclear Suppliers Group (NSG) obligations, and bilateral agreements on a state level as well as on an operator level. The operator must have an information security management system (ISMS), which also covers the information security of relevant third parties, such as its supply network. This includes contractual measures, such as information classification and handling rules, and non-disclosure agreements. Facility security clearances and personnel security clearances may be performed by authorities. In a case where there is a general security agreement (GSA) between the States, the agreement may cover the clearances to be mutually recognized. In the absence of a GSA, there may be other state-level arrangements. As a general rule, the operator must convert any classified regulatory requirements into its own design specifications. Some of this information remains classified, and is managed by the aforementioned operator's ISMS, contracts, and state-level arrangements. Information security is therefore the earliest encountered task for a State or an operator embarking on a NPP program. This is also the very first stage of nuclear safeguards. During that phase, the operator needs a person responsible for safeguards, who has the required knowledge and who is able to coordinate the process.

An important document at the early planning stage is the IAEA Safety Standards, Safety of Nuclear Power Plants: Design, Requirement 8: Interfaces of safety with security and safeguards. This IAEA Standard supports the states in the coordination of safety, security, and safeguards. The standard is also among the first IAEA document that the nuclear suppliers and vendors read, ensuring that the interactions on safety, security and safeguards start between the State, supplier and IAEA. Thus, nuclear regulations in Finland stipulate that the operators must provide the preliminary design information questionnaire (DIQ) within 30 days of the Decision in Principle. This takes the full spectrum of international nuclear safeguards officially on board at a very early phase.

After receiving the preliminary Design Information Questionnaire (DIQ), the IAEA prepares a Material Balance Area (MBA) code for a new facility, and the Safeguards by Design dialogue with the State can start. This is essential for new nuclear power plants and even more important for new types of nuclear facilities, like the geological repository for spent nuclear fuel in Finland. This process enables the State to discuss national security measures with the IAEA and to take them into account when the IAEA implements its safeguards activities in the facility.

Starting the safeguards measures during the planning and design phase has many benefits: cost efficiency, cabling taken into account, placing the IAEA equipment such as cameras and seals, routes for nuclear material movements, etc. This will

improve the overall quality of safeguards. All stakeholders will also become more familiar with safeguards and its international obligations in a timely manner.

Safeguards by Design is voluntary for the states. A practical example of Safeguards by Design, based on the experiences of Finnish operators, is to get all safeguards requirements included as early as the design phase in the request for tender, and it is necessary to keep regular contact with the authorities (national and international).

In accordance with national requirements and in line with the IAEA Nuclear Security Series (NSS) recommendations and guides, the operator must ensure the security of information, including the cybersecurity of third parties who have potential access to its classified information. This obligation encompasses such systems as safeguards' remote monitoring where, for example, the security of technical interfaces, transmission, and use of information at the recipients' systems are considered. The necessary information and cyber security measures must be implemented following the normal graded, risk-informed approach.

Security and safeguards inspectors should cooperate closely. Security and safeguards inspectors should notify each other of, their findings also from the other S's point of view.

As practical example, STUK's radiation safety, security and safeguards inspectors cooperate when verifying small amounts of nuclear materials. Responsible personnel from these smallholder organizations are usually limited in number and the practical implementation of safety, security and safeguards is the responsibility of just a few persons. It is important to ensure that all aspects of all S's are taken into account as appropriate and required.

Site walk, covering security and safeguards is an activity where safeguards and security experts make observations at the facility. Optimally, safety observations are included. The observations are recorded and assessed, and corrective actions are taken and followed up as necessary. One objective is to increase awareness and knowledge in a multidisciplinary manner.

Technology development has been fast in recent years. This is also evident in safeguards. The goal of using new technology is to make safeguards implementation more effective. A good example is the development of safeguards cameras. The first cameras in the 1970s were film-based. This technology has been replaced by technically advanced digital cameras, which makes the handling and storing of data much easier. On the other hand, digital data and data processing including image analysis can be much more easily manipulated than the original films and printed pictures, which increases the importance of information security and tamper-resistant methods. The storage capacities of digital memories are increasing and costs are falling. Digital imaging also makes it possible to use Remote Data Transmission (RDT), where data from the site under surveillance is sent to the inspectorates by various data transmission means. RDT has been discussed since

the 1990s when the Internet made its breakthrough, and it was implemented in safeguards surveillance systems at Finnish NPPs in recent years.

These safeguards issues must be considered in a balanced manner together with potential security risks. The nuclear operator is in charge of the safety and security of its facility, so the operator must know what kind of electronic systems are being used within the perimeter of its facility. In accordance with national regulation and international nuclear security guidance, the operator is responsible for ensuring appropriate information security levels at third parties that have access to its sensitive information. The safeguard cameras monitor the nuclear materials and their flows, which is sensitive information and as such subject to information security requirements. A surveillance system is also a potential vector for a cyber attack and should be protected accordingly. Espionage and the leaking of confidential commercial information can also occur. In practice, these risks cannot be completely avoided. There are administrative and technical ways to efficiently manage the risks, for example batching the transmission.

Laser 3D scanning has been used by international inspectorates for the Design Information Verification of nuclear facilities. The scanners create point clouds accurate to a level of 1 mm that are processed to present accurate 3D models of the targets scanned. For safeguards, this methodology is very effective and makes it possible to verify and document the built infrastructure of the facility in a reliable and repeatable manner. The point clouds and 3D models are digitally stored for further review. If the scanning is repeated, detection of changes is possible.

However, this data is, again, very sensitive. In the processed 3D models, even the smallest details of the physical protection systems, ventilation, pathways, etc. can be identified and accurately located. From a security point of view, this information must not be leaked to unauthorized persons. One possible technical solution is that the scanned data does not leave the site, but is only assessed during inspections on-site. This, however, limits the usability of the method as an inspection tool and induces additional cost to all parties as a result of keeping inspectors on-site for longer periods.

IAEA inspector access to the declared facilities is clearly mandated in the Comprehensive Safeguards Agreements. The Additional Protocol also grants wider access to the sites and locations outside the facilities where nuclear materials are used. The access of safeguards inspectors to a facility can be limited, if it conflicts with safety or security, for example, if access to areas of high radiation cannot be arranged due to radiation safety. Access by an intoxicated inspector can be restricted for occupational safety and security reasons.

Modern nuclear facilities have many different information systems that have interfaces to other systems, and the chain can only be as strong as its weakest link. For example, to ensure that there are no attack vectors through less important systems to more important systems, information and cyber security must be taken

into account. This is part of the normal information security management, where sensitive information assets are identified, classified and protected according to their significance.

The legislation regarding the documents of the government authorities in Finland stipulates that they are public unless, based on the legislation, there is a reason and need to classify the document. There are four levels of classification with corresponding requirements for information security measures during the lifetime of the document. State security, relationships with international organizations, and facility security arrangements are the most relevant classification reasons within the nuclear safeguards and security regime. Business secrets may also be a valid classification reason.

Radioactive materials out of regulatory control (MORC) have been among the concerns that both international and national institutions have addressed in recent years. Many countries build, operate, and maintain their national nuclear detection architectures. The activities include radioactivity screening at the borders and at major public events. The activity is considered to be a part of nuclear security since the focus is on combating nuclear terrorism and other unlawful activities. However, it also has much to do with nuclear safety and safeguards. When the material is found, an appropriate organization can start to investigate the root cause of the event, which can then lead to corrective actions. The activities within nuclear detection architecture are also an extra layer to verify that there are no undeclared nuclear materials or activities in the state. A considerable part of MORC is nuclear material, which should be under safeguards.

One important aspect of traditional nuclear safeguards is the concept of reverification. All declared nuclear materials can be verified at any point in time and if continuity of knowledge (CoK) or containment and surveillance (C/S) is broken. The disposal of nuclear fuel in bedrock excludes this possibility, as it is not possible or feasible to verify the fuel after it has been placed underground and the access routes, e.g. emplacement holes and tunnels closed. This adds to the challenge and importance of safeguards during the process of encapsulation and disposal. It is imperative that there is knowledge of all nuclear fuel that is being disposed of. From a security point of view, long-term information security needs are an interesting feature related to final disposal. Integrity and availability of information must be ensured through technical, administrative, and cultural solutions.

Application of new technologies can also introduce synergies between safeguards and security. The IAEA safeguards requirement before spent fuel goes to 'difficult to access' storages is that verification should be done at partial defect level. Partial defect means that the diversion of a given percentage (by default 50%) of the nuclear material should be reliably detectable. Recent development in Passive Gamma Emission Tomography (PGET) has shown that pin-level verification is possible. The position of STUK is that the PGET method should be developed to a fully operational level, so that it can be used in the Finnish disposal project from the

very beginning. This kind of technological development is also valuable for security. It is not possible to build a nuclear weapon from a single pin, but a single pin could easily be used for other criminal purposes. With precise verification, the possibility of using irradiated fuel for illegal purposes can be excluded.

In safeguards, sampling and measurements are employed to verify the declarations of the licensee. In nuclear security, detection activities can be divided into two components: (1) preventive surveillance measurements and (2) forensics studies related to nuclear security incidents. Nuclear forensics analysis can also be seen as a preventive measure since one of its goals is to prevent crimes in the future.

Nuclear forensics has greatly benefited from the developments made in safeguards, since many of the techniques used in safeguards can also be employed in nuclear forensics analysis. Detection, sampling, and analysis in safeguards and nuclear security can be further advanced through general scientific developments or through tailor-made developments in either one of the fields. The next chapter presents some trends and developments that may potentially influence both fields in the future.

Integrated digital nuclear electronics is advancing rapidly. New scintillation detector materials are also under intensive development. As an example, a detector capable of simultaneous gamma-ray spectroscopy and neutron counting is now technically possible. Among the drivers behind these developments are the large nuclear security markets. Such new detectors could also be useful for safeguards inspectors during on-site inspections.

Both bulk and individual particle analysis techniques are important for security and safeguards as well as for radiation protection. NDA particle analysis techniques based on multi-detector setups and coincidence analysis have been extensively studied at STUK. Such studies could, for example, be continued with the nanotomographic investigation of isolated particles. Nanotomography produces a 3D density map of a microscopic particle. Nuclear reference materials and nuclear material libraries can serve both safeguards and nuclear security. Coordination of technical developments is important.

In our experience, there are many technical synergies between nuclear safeguards and security. One of the differences is the international framework. Safeguards are based on international agreements. The IAEA and the EC safeguards requirements for Member States are very detailed and are binding. While there are also binding international agreements on nuclear security, the implementation of nuclear security is mostly based on national legislation and regulation. In general, there are no conflicts between safeguards and security. It is essential that we learn from each other, share information and understand each other's needs when implementing nuclear safeguards and security. In practice, it is challenging to find and develop methods to work with confidential information in a flexible way, but it

is possible to find an appropriate way. Novel technologies are available for safeguards and security measures. Research and development efforts are expected to bring us new technical tools, which will provide improved, more efficient and effective implementation for both safeguards and security.