IRRS Good Practices

Interface with nuclear security (Module 11)

Regulatory oversight activities

Belgium – Initial Mission

Mission Date: June 2023

Good Practice

The regulatory body oversight approach to regulate the interfaces between safety and security, based on their unique use of "confidentiality and the principle of a need-to-know" and the conduct of dedicated inspections at all NPPs is effective.

Observation

FANC approaches the interfaces between safety and security in accordance with one of the fundamentals of the CPPNM, namely confidentiality and the principle of a "need-to-know". FANC's 3S Strategy Note describes the scope of safety and security interfaces and how a conflict between safety and security interfaces would be addressed.

FANC has developed an inspection guide for all Class I facilities that identifies areas for inspections on the interfaces between safety and security. Potential challenges and impacts are assessed as part of the preparation of these inspections. Bel V performs annual inspections at all NPPs using this guide to identify the impact of the physical protection measures, including cyber security, on nuclear and radiation safety.

Basis

1. GSR Part 1 (Rev. 1) para. 4.52. states that *"Regulatory inspections shall cover all areas of responsibility of the regulatory body, and the regulatory body shall have the authority to carry out independent inspections."*
2. GSR Part 1 (Rev.1) Para 2.39 states that *"Specific responsibilities within the governmental and legal framework shall include: (…) (b) Oversight and enforcement to maintain arrangements for safety, nuclear security and the system of accounting for, and control of, nuclear material…"*
3. GSR Part 1 (Rev.1) Para. 2.40 states that *"Safety measures and nuclear security measures shall be designed and implemented in an integrated manner so that nuclear security measures do not compromise safety and safety measures do not compromise nuclear security"*

IAEA Comments/Highlights

FANC approaches the interfaces between safety and security in accordance with one of the fundamentals of the Convention on the Physical Protection of Nuclear Material (CPPNM), namely "confidentiality and the principle of a "need-to-know". While security Single Points of Contacts (SPOCs – for DOEL and TIHANGE nuclear power plants) are cautious with their security information about the facilities, it does not apply to their safety colleague who is required to work with them. Safety SPOCs who are aware of the security information are not to share with individuals who are not authorised to receive the security information and have no "need to know".

As part of the overall inspection programme, Bel V performs annual inspections on interfaces between safety and security at all NPPs. For other Class I facilities, these inspections are performed every two years. These inspections are not performed in facilities of other classes. At any time, FANC and Bel V inspectors can report any unusual observations or events that may impact interface with nuclear security by using a reporting process.

The purpose of the planned inspections is to confirm scope of the inspections will cover safety and security interface, such as target identification (those components critical to safety aspects), studies related to design basis threats (DBT) (resistance of structures, etc) and changes to installations and facilities. The scope of planned inspections is to identify the impact (complementarities, interferences and antagonisms) of the physical protection measures (including cyber security) on nuclear safety and radiation protection.

Slovenia – Initial Mission

Mission Date: April 2022

Good Practice

SNSA's activities with regards to organising and conducting emergency exercises (KiVA series) based on realistically simulated cyberattacks leading to a safety and nuclear security

event were found remarkable for effective training and management of the interface between safety and nuclear security.

Observation

SNSA has trained and developed its competences in the field of cybersecurity at the interface between safety and nuclear security making available internationally recognized experts. In particular SNSA has engaged all national partners for emergency exercises with cyber scenarios as a mean to raise awareness towards cybersecurity and train the network of collaborating EPR organisations to respond to such events. The IRRS team was informed that the IAEA is following such exercises in Slovenia in order to leverage those experiences for a planned IAEA TECDOC based on the Slovenian exercise series KiVA.

Basis

1. GSR Part 1 (Rev 1) para. 2.40 states "*Safety measures and nuclear security measures shall be designed and implemented in an integrated manner so that nuclear security measures do not compromise safety and safety measures do not compromise nuclear security.*"
2. GSR Part 7 para. 4.10 states "*The government shall establish a national coordinating mechanism to be functional at the preparedness stage, consistent with its emergency management system, with the following functions: …(c) To coordinate and ensure consistency between the emergency arrangements of the various response organizations, operating organizations and the regulatory body at local, regional and national levels under the all-hazards approach, including those arrangements for response to relevant nuclear security events, and, as appropriate, those arrangements of other States and of international organizations;*"
3. GSR Part 7 para. 6.12 states "*Arrangements shall be developed, as appropriate, for the coordination of emergency preparedness and response and of protocols for operational interfaces between operating organizations and authorities at the local, regional and national levels, including those organizations and authorities responsible for the response to conventional emergencies and to nuclear security events.*"

IAEA Comments/Highlights

With respect to cybersecurity, SNSA (Slovenian Nuclear Safety Administration) is putting its expertise at disposal under the umbrella of the Government Information Security Office, acting as liaison for the many national CERTs (Computer Emergency Response Teams) and the nuclear industry as well as the Slovenian civil protection authorities and international EPR (Emergency Preparedness and Response) partners.

In the field of emergency preparedness, SNSA has taken a leading role conducting regular emergency drills with cyber inputs. Furthermore, SNSA has organized a major emergency exercise (postponed to 2022 due to the pandemic) with a cybersecurity scenario at a nuclear facility in order to drill the emergency response staff at the national level (regulators, civil protection authorities, CERTs, nuclear operators and industry), but also testing the international response network. The scenario for the KiVA2022 exercise makes use of real-life hardware and software simulations to be realistic and raise awareness of the responding

staff to the technical, organisational and human factors involved in a cyberattack. Experts from several countries, including from USA, UAE, Germany, Romania and Canada, have confirmed their presence to observe and learn from the unique exercise KiVA2022.