Contribution ID: **185** Type: **Paper**

Management of nuclear security-safety interface: what, why and how

What is safety-security interface and interface management

Security-safety interface is a decision point where both safety and security issues should be taken into consideration. When done in a risk-informed, balanced manner, this should result in best possible overall safety and security. Doing this—by effective processes and procedures—is safety-security interface management.

Interface management takes place at the government level: coordination between authorities, licens-ing, regulatory requirements, inspection programmes, and at the licensee level: primary responsibility of safety and security and implementation of regulatory requirements. In detection of and response to material out of regulatory control interface management enables efficient and secure communications, and fits together radiation safety and forensics procedures in crime scene management.

We endeavour to manage the safety-security interfaces in order to take advantage of synergies and to resolve possible conflicts.

Joint fundamental objective and difference

It is widely recognized that nuclear safety and nuclear security share a joint fundamental objective to protect people and the environment from harmful effects of ionizing radiation. If we consider that nuclear safety measures aim to ensure the safety of normal operations, a low probability of accidents, and effective emergency preparedness, and that nuclear security measures aim to combat intentional unauthorized acts, we can see that they approach their joint objective with different risk assessments and that both are equally necessary to achieve the overall objective.

The big difference is the "opponent". Safety measures are designed against unintentional events. Security measures are designed to deal with active adversaries, who may adapt their actions based on their knowledge of the defences. In accident management it is good that procedures are widely known and that controls are easily accessible—in a security event the adversary would use that information and access to defeat the response.

Similarities and differences in practice

Many safety and security measures contribute to both regimes and complement one another. There is also potential for conflict.

Complementing elements include:

- Coordinated legal and regulatory framework
- Risk-informed, graded approach
- Safety and security by design of systems, structures, and components
- Integrated management system
- Human factors
- Organisational culture
- Information and computer security
- Access control and surveillance
- Materials accountancy
- Coordinated response

Potentially conflicting elements include:

- Transparency vs. confidentiality
- Control and delay of access & exit vs. unobstructed passage

There are also neutral elements that do not particularly contribute to or interfere with the other regime.

Some areas where interdependencies between safety and security are strong

Leadership, management and organizational culture

How nuclear safety and security are addressed in the integrated management system of an organiza-tion, is a top level interface management decision. Risk management is an example of a cross-cutting process where balanced approach to security, safety, and other risks should serve informed decision making. People should recognize the decision points where safety and security considerations matter.

Information and computer security

Information security—confidentiality, integrity and availability of information—links safety and security to-gether in a concrete way: to ensure the information is accurate and complete, at the disposal of the right people at the right time, and not at the disposal of the wrong people. All three are essential for safe and secure use of nuclear energy and use of radiation in health care, industry and research as well as for effective response to accidents and security events, including MORC incidents.

The interdependence between computer security, physical security, and safety has grown in im-portance due to the increased use of digital, programmable, and networked systems, in OT as in IT.

Design and change management

The most efficient life cycle phase to pursue safety and security is the design. Industrial control sys-tems should also have "hard-to-hack"as a design paradigm. Along the life cycles there are modifica-tions. There should be steps in the procedures to flag safety-security decision points and who should participate in decision making.

Response

Response to anomalies is a test for safety-security interface management. The following activities should be implemented in a coordinated manner:

- accident/emergency response and nuclear security response
- on-site response and off-site response
- activities of all entities responsible for off-site response
- emergency exercises, security event exercises, and combinations thereof, including cyber and physical threats.

Some potential for further work

Classical safety classification of systems, structures and components does not necessarily account for inten-tional unauthorized acts. On the other hand, a balance should be found between security controls and usability. A holistic risk-informed approach for significance evaluation might be a good basis for further development.

Methods for application of probabilistic risk assessment (PRA) in security analyses and design have been and are being developed. The aim need not be to produce absolute values of risk, but, for exam-ple, to compare the effectiveness of different nuclear security systems, and to balance safety and security aspects in the assessment.

Gender

Female

State

Finland

Author: KARHU, Paula (Radiation and Nuclear Safety Authority (STUK))

Co-authors: STAUFFER, Bernard (Swiss Federal Nuclear Safety Inspectorate (ENSI)); SCHRAVER, Marco (Authority for Nuclear Safety and Radiation Protection (ANVS)); HACK, Tapani (Radiation and Nuclear Safety Authority (STUK))

Presenter: KARHU, Paula (Radiation and Nuclear Safety Authority (STUK))

Track Classification: CC: Nuclear safety and security interfaces