# MANAGEMENT OF THE INTERFACE OF

# NUCLEAR SECURITY AND NUCLEAR SAFETY:

# WHAT, WHY AND HOW

P. KARHU

Radiation and Nuclear Safety Authority (STUK)

Helsinki, Finland

Email: paula.karhu@stuk.fi

M. SCHRAVER

Authority for Nuclear Safety and Radiation Protection (ANVS)

Den Haag, The Netherlands

B. STAUFFER

Swiss Federal Nuclear Safety Inspectorate (ENSI)

Brugg, Switzerland

T. HACK

Radiation and Nuclear Safety Authority (STUK)

Helsinki, Finland

**Abstract**

What is safety-security interface and interface management and why is it important? Security-safety interface is a decision point where both safety and security issues should be taken into consideration. If the consideration is done in a risk-informed, balanced manner, it should result in an informed decision and the best possible overall state of safety and security. Ensuring this—by effective processes and procedures—is safety-security interface management. The paper explains why nu-clear safety and security regimes are different and points out areas where they are similar. In addressing the “how”, the paper describes areas where the interfaces are abundant, important, or obvious, and presents practical examples related to regulatory requirements, oversight, inspections, and site-walks. The paper discusses challenges and suggests solutions.

## SETTING THE SCENE

Security-safety interface is a decision point—any decision—where both safety and security issues should be taken into consideration. The “issues” include potential consequences of both unintentional events and intentional acts, and security and safety interests in providing preventive and protective elements against those events and acts. If the consideration is done in a risk-informed, balanced manner, it should result in an informed decision and the best possible overall state of safety and security. Ensuring this—by effective processes and procedures—is safety-security interface management.

Safety-security interface management is relevant at State level in the legal and regulatory framework. Safety-security interfaces should be considered in the licensing process and in the inspection programmes of the regulatory authority/authorities. Coordination with other authorities who have a role in nuclear safety and security should take place. Those authorities may include intelligence, law enforcement, investigation, rescue, defence forces, border guard, and information security authorities, possibly specific counter-terrorism and/or CBRNE authorities and crisis management agencies, depending on the government administrative structure. Regardless of whether there are one or several competent regulatory authorities, coordination and cooperation is essential, to ensure a balanced, risk-informed approach, appropriate coverage and completeness of assessments, and to avoid conflicting requirements and end-results. The operator level is crucial, as the operator is responsible for the design and implementation of nuclear security and safety measures and for integrating these into an effective system.

In addition to the national level it should be considered, whether and how the interface management should be part of international peer reviews, and whether there is room for improvement in that regard.

The processes relevant to interface management are any activities where the decision points exist. They are related to regulated materials, facilities, and activities as well as materials out of regulatory control. Some of the decisions take place at strategic levels and some at operative levels. Policy making and risk management are examples of high-level processes. Risks should be identified, assessed, and managed considering both unintentional events and intentional acts.

The procedures are for example instructions on who, how, where and when should consider security and safety issues. For example, how to manage interfaces when the regulatory authority reviews operator’s documents and plans, e.g. preliminary and final safety analysis report, PSAR and FSAR. For example, who should participate/be consulted in which stage and in what capacity in change management of a system in a nuclear facility. Procedures/instructions should be written and executed in a manner to ensure the risk-informed, balanced decision making takes place.

## JOINT OBJECTIVE AND THE “FUNDAMENTAL 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 (and nuclear safeguards) measures aim to combat unlawful and other intentional unauthorized acts, we can see that nuclear security and nuclear safety regimes approach their joint objective from different angles and that both regimes are equally necessary to achieve the overall objective.

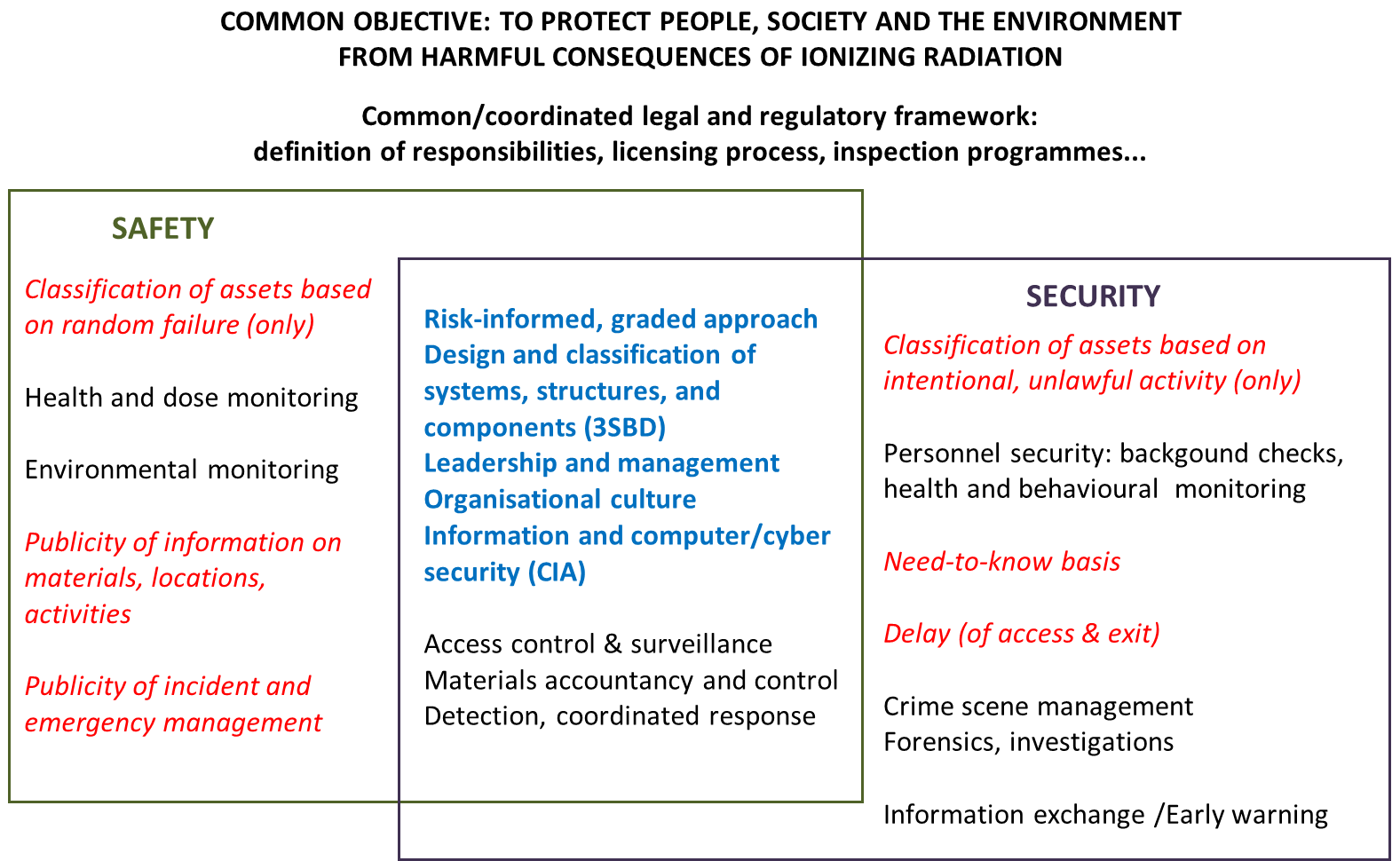
We often say that both regimes are equally important, but one still sees “safety overrides” or “security should not compromise safety” type expressions. This is silo thinking. For the sake of best possible overall safe-ty and security, this thinking should be changed to a risk-informed, balanced approach. It seems that in order to succeed in this, we may still need to improve our communication and have a genuine will to understand each other. Notwithstanding the hectic pace at work we should dedicate some time to dialogue between safety and security professionals, in appropriate groups and at appropriate levels to achieve organizational alignment—to move forward together.

The big difference, one could say the fundamental difference, is the “opponent”. Safety measures are designed to be effective against unintentional events and their unwanted consequences. Security measures are designed to deal with active adversaries, who adapt their actions based on their knowledge of the defences. This results in some conflict potential between the two regimes: in accident management it is good that instructions and procedures are widely known, and the plant controls are easily accessed—in a security event the adversary would use that information and access to defeat the response, and a need-to-know principle (confidentiality) is applied. For the response to be effective, however, we also need to take care of the rest of information security—availability and integrity—and find a good balance between them and confidentiality. A “fundamental difference” seems to be often mentioned without explaining what is meant, which creates unnecessary mystery over a simple matter (the related practical solutions to which may not always be simple, but nevertheless should be dealt with as well as can be).

Through the joint objective and the big difference the two regimes are interdependent.

## SIMILARITIES AND DIFFERENCES

### There are synergies between safety and security regimes, as many safety and security measures contribute to both regimes and complement one another. As explained in the previous section, there is also potential for conflicting requirements. Figure 1 presents one way to look at these. One goal of managing the safety-security interfaces is to take advantage of the synergies and to resolve the possible conflicts.



*FIG. 1. Synergistic (bold blue font), neutral (regular font), and potentially conflicting (red italics font) elements of safety and security. Safeguards/NMAC can be added as a third box. It, too, overlaps with security and safety.*

## SOME KEY AREAS WHERE INTERDEPENDENCIES BETWEEN SAFETY AND SECURITY ARE STRONG

Some of the areas and elements of interest—where the interface management decision points are abundant, important, or obvious—are “high level” (strategic) in nature and some are related to more practical matters.

In regulated activities the interface management takes place at the government level: coordination between responsible competent authorities, maintenance of regulatory requirements and guides, coordination within/between inspection programmes, and at the level of the licensee: the primary responsibility of safety and security and the implementation of regulatory requirements. Regulated activities/regulation of activities provide for prevention of nuclear or other radioactive material getting out of regulatory control (becoming MORC). In detection and response to MORC, interface management takes place for instance in ensuring efficient and secure data transfer and other communications (confidentiality, integrity, availability), taking care of both radiation safety and forensics needs in crime scene management, and coordinating the whole response: rescue and accident management and response to criminal activity.

### Leadership, management, and organizational culture

How (nuclear) safety and security are addressed in the overall integrated management system of an organization, is a top-level interface management decision. A strategic alignment. People should be able to recognize those decision points in everyday life where safety and security considerations should take place. They should understand the effect of their actions and omissions to safety and security. They should be encouraged to identify good practices and to observe non-conformances and report them. In addition to specific safety and security experts and technical solutions, all staff should contribute to early detection. In addition to awareness, attitudes, and understanding, appropriate technology and tools are required to achieve good overall safety and security. The integrated management system should extend these practices also to the supply chain.

### Information security and computer security

In nuclear security, the concept of confidentiality is well established—and essential. However, it is only one of the three main components of information security, and not worth a lot without the other two: integrity and availability of information. Information security links safety and security together in a very concrete way: integrity and availability are essential to the safe and secure use of nuclear energy, and the use of radiation, as well as for management of incidents related to MORC. Integrity aims to ensure that the information at hand is accurate and complete. The objective of the availability component is to have the right information at the disposal of the right people at the right time. Both are very important for effective response to accidents and security events. The availability component is sometimes referred to as the need-to-share principle, complementing the need-to-know.

The interface and interdependence between computer security, physical security, and safety has grown in importance, due to the increased use of programmable and networked systems in information technology and industrial processes (IT and ICS/I&C systems), and the phenomenon of internet of things (IoT).

One potentially noteworthy safety-security interface consideration are the principles of redundancy and diversity. They, along with separation, relate to the defence in depth concept, which is in both safety and security toolboxes. Redundancy of components or controls will not improve computer security, as a single malware will affect any component or control with the same vulnerability, if networked or otherwise accessible to the attacker, and diversity is only effective if diverse systems do not introduce too severe diverse (or unknown) vulnerabilities. Physical separation is effective against outsiders, and together with separation/limitation of duties/access/privileges of persons and segmentation and hardening of networks it is effective also against in-siders.

### Design and change management

The most efficient life cycle phase of a nuclear facility to pursue safety and security is in the design. Suppliers should incorporate security as well as safety in the design of systems and equipment. I&C systems also should have “hard-to-hack” as a design paradigm. The buyer, e.g. a licensee of a facility should have adequate awareness and competence to require security by design. As a single or few buyers have limited influence, the global nuclear community (together with other critical infrastructure) should cooperate in this issue to achieve good results.

Safety and security of the systems, structures, and components (of a nuclear facility or otherwise significant to nuclear safety and security) should be ensured during their whole life cycle from design through manufacturing, installation, commissioning, and operation to decommissioning. Along the way, one safety-security interface exists in maintenance and modifications. Firstly, the designers should have enough knowledge of the boundary conditions related to security when designing modifications. Secondly, security measures appropriate to the safety-security significance of the system, structure, or component should be applied during maintenance or modifications. Additional or compensatory security measures may also be necessary. There should be steps in the maintenance and modification procedures to trigger coordination and identification of safety-security interface management decision points and who should participate/be consulted.

### Response

An emergency may be caused by an unintentional event or by an intentional act or a combination of both or series thereof. Response to incidents is one of the tests for safety-security interface management. Who is responsible for which response activity must be clear to all involved parties. Accident/emergency response plans and nuclear security response plans should be designed and implemented in a coordinated manner. The plans for on-site response should be coordinated with those of the off-site response forces. The plans of different authorities or other entities responsible for off-site response should be coordinated with one another. All plans should be exercised to evaluate the effectiveness and in order to learn, by organizing emergency exercises, security event exercises, and combinations thereof. The overall response is likely to involve a joint command and control structure. In addition to getting the situation under control, minimizing and mitigating the consequences, it has become more and more essential to communicate about the incidents. This includes internal communication within the joint command and control as well as with other government agencies and the public, in order to provide accurate, relevant information. Otherwise the void will be filled with disinformation.

It is important to recognise the possibility of intentional activity, such as sabotage, as a potential cause for anomalies. Security measures and the security organisation may be needed to provide extra protection to those responsible for accident management and the assets required for it. In order to be able to execute the response effectively based on the significance of events to the overall safety and security, knowledge of the facility, its assets—or the MORC, as the case may be—and potential consequences, should be at the disposal of the response forces, the off-site component of which typically may not be experts in nuclear facility operations or radioactive materials.

## Practical examples

### Regulatory requirements

In the regulatory framework in the Netherlands, in terms of policy, safety and security are equivalent. For both domains, the nuclear licensee must comply with legislation and regulations in the Netherlands. Possible conflicts between safety and security must be analysed and resolved at site level.

For the nuclear site (or the nuclear object), the licensee must elaborate the most optimal configuration, whereby the licensee must take compensatory measures for safety or security issues in order to comply fully with Dutch legislation and regulations.

Therefore, if the nuclear licensee opts for a safety solution in safety-security conflict situations, he must take compensatory security measures for that problem and vice versa. Naturally, the licensee must ensure that sensitive security information is not distributed.

Finally, the licensee must substantiate the chosen solution and the inspectorate will test this solution for adequacy and robustness [1].

### Review and inspection by the regulatory authority

#### Review of plans and programme management

In the regulatory control of nuclear facilities in Finland, we have regular meetings among the experts from the various safety oversight sections and the security section, and a system for following up the different areas that contribute to the overall safety and security status of the nuclear facilities.

When nuclear facility licensees send in documentation for review, the review lead is assigned to the relevant oversight section and inspector according to the topic. The lead inspector of the case shall assign more inspectors to the case from other sections, including different safety sections and the security section. In order to do this successfully, all sections need the basic awareness of each other’s’ area of expertise. The documentation that should be reviewed from safety angle and from security angle, and would be coordinated by safety oversight sections, may include, for example, layouts and building plans, structural plans, MCR operations plans, I&C designs, organizational culture assessment, competence management plans, and many more. Similarly, the security oversight section should assign “safety colleagues” to co-inspect certain security focussed documentation, such as physical and logical access management.

#### Separate vs. joint on-site inspections

In the Finnish regime for nuclear facilities the on-site security inspection programme is a sub-element of the overall on-site inspection programme, during the phases of construction, commissioning, operations, and decommissioning. The security oversight section is in charge of it, and there are several safety sections in charge of safety inspections. We—the security—have sometimes joined in the inspections on organization, leadership, management, and culture. A few times we have led the inspections on the management system topic, assessing how nuclear security is understood and dealt with by top management and how it is integrated in the management system. Our national nuclear safeguards/NMAC section’s inspectors have joined in on those occasions, as have the experts from the organization and leadership oversight section. We have carried out joint inspections by the security section and the I&C oversight section. We have joined inspections of the section in charge of the oversight of the licensee’s emergency management.

Due to the complexity of a nuclear facility and the required multi-disciplined expertise, there is a section specialized in nuclear security, and the interfaces must be managed with other sections in charge of other aspects of the regulatory control. In developing risk-informed oversight and optimising resources one challenge is finding a way to compare the significance of the “oversight targets” between the safety and security regimes, not only within each one, in order to avoid the silo effect.

In the regulatory control of the use of radiation—radioactive materials and radiation devices in health care, industry and research—the inspectors of STUK include both safety and security aspects in their inspections. There are so many licence holders that it was not considered feasible to hire many enough specialized security inspectors. Instead many enough inspectors were trained on security inspections as well as safety. Internal instructions on requirements and assessment criteria were updated. One benefit is that potentially conflicting requirements to the licence holders are avoided—for example a case where a safety inspector would require markings on radioactive sources’ facilities and a security inspector would have the markings removed. The authority is a one-stop-shop from the viewpoint of the licence holder [2]. Some cultural shift is required, however, to assume responsibility for security inspections in addition to the more mature safety regime.

The regime is risk-informed based on potential consequences associated with the radiation sources, in terms of inspection depth and frequencies. Security requirements are based on three security levels of sources: A corresponds to IAEA category 1, B to 2-3, and C to 4-5. Transportable industrial radiography x-ray devices belong to level B. Security levels are considered in planning and executing the inspection programme. The nuclear security section experts from the nuclear facilities’ oversight participate on these inspections from time to time “as consultants”—again based on a risk-informed approach. The same is done on inspections of “small nuclear material holders”, for example in research institutes.

### The concept of site walks

One concept that has been found useful in interface management and continuous improvement is site walks. While all staff are encouraged to make and report observations relevant to safety and security, site walks are the responsibility of a dedicated multidisciplinary team. The idea is to have a pool of team members from the areas of nuclear safety, physical security, information and computer/cyber security, operations, maintenance, quality, workplace safety, organizational culture, fire & rescue forces, etc, so that observations can be made on a comprehensive basis. The actual composition of a team may vary from walk to walk. The observation findings are recorded, and they may be classified for example to good practices, minor non-conformances, and major non-conformances. The ones requiring corrective actions are assigned to responsible persons and followed up. Results are reported according to the rules of integrated management system.

The site-walk concept is a part of the situational awareness programme relevant to nuclear security. It is a way to raise awareness of the significance of the different disciplines contributing to overall safety and security. It is a means to drive continuous improvement, good organizational culture, and considering safety and security in decision making in a balanced manner. The site-walk concept is applicable in all organizations—for the authorities and for the operators.

### Transport of nuclear material

When transporting nuclear material, especially in an international environment, safety requirements meet different national security requirements. In addition, the confidentiality of the security arrangements is a challenge for both the license holder and the authorities.

Switzerland as an example, being an island in the middle of Europe without direct access to sea ports, can perform international shipments only by crossing countries in transit to sea ports of a neighbouring country. Based on this situation Swiss operators are usually challenged with multiple different national safety and security requirements.

In order to enable the implementation of the safety and security requirements, integrated involvement of the relevant supervisory authorities is mandatory. The Swiss supervisory authorities and the license holders therefore brought the responsible persons for safety and security together and exchanged the respective requirements openly with each other. At international coordination meetings, also responsible people from safe-ty and security regimes were present. Emerging conflicts between safety and security requirements could be clarified and satisfactory and balanced solutions could be found. This concept requires openness and under-standing of the interface and the mutual influence of the requirements and measures from all involved people. It also requires that the respective parties are professionally competent and authorized to give instructions.

It was not always possible to fully implement all requirements for all transports of nuclear material, but in each case the measures could be designed in such a way that the safety and security measures were balanced. From a Swiss perspective, a non-integrated approach is unthinkable.

## SOME (ADDITIONAL) TOPICS FOR FURTHER WORK

Classical safety classification of systems, structures and components does not necessarily account for intentional unauthorized acts, as it is mostly based on random failures and events. 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. In digital systems one cannot have safety without security, because availability and integrity of systems require security controls, to make sure the systems are doing their important functions for operations and safety when they should, and reliably. The controls should be applied according to significance of the system. Also, the possibility of using less significant (low-impact) systems as attack vectors to the actual target (high-impact) system should be considered.

Methods for application of Probabilistic Risk Assessment (PRA) in security analyses and design have been and are being developed. The goals may be, for example, to assess the efficiency of different protection strategies and to identify important locations or controls that, when added to a protection strategy, would improve its efficiency considerably. The aim would not be to produce absolute values of risk, but to provide practical comparisons of the efficiencies of different protection scenarios. According to studies by STUK and VTT Technical Research Centre of Finland Ltd a significant potential exists in using the logic model of PRA, supplemented by different dependency databases developed during different phases of PRA work. The logic model of the PRA identifies critical failure combinations that shall be prevented. The dependency databases identify all locations where the operation of critical components may be influenced. Considering that the possibilities for an adversary to cause some events and failures are greater than others, the security PRA may use reliability data tailored accordingly [3].

## CONCLUSIONS

Security-safety interface is a decision point where both safety and security issues should be taken into consideration. If the consideration is done in a risk-informed, balanced manner, it should result in an informed decision and the best possible overall state of safety and security. An intermediate goal is to take advantage of the synergies and to resolve the possible conflicts between safety and security interests.

Interface management takes place at the State level in the legal and regulatory framework, in the activities of the regulatory authority/authorities and other competent authorities, and in the activities of the operator of a nuclear facility or a facility using (or manufacturing or trading or handling) radioactive sources or in transport of radioactive material.

There should be steps in relevant procedures to trigger identification of safety-security interface decision points and to address coordination: who should participate/be consulted in the decision making. Establishing and maintaining a process to ensure this, is safety-security interface management.

In many cases the interface management is a question of terminology and putting the common under-standing into words that would be commonly understandable—in the same way. In some cases the established concepts would benefit from some rethinking. Change and improvement requires good communication and a will to understand each other.

References

1. “Policy on Security and Safeguards” (Chapter 4, in Dutch), National Policy on Radiation Protection and Nuclear Safety, Ministry of Economic Affairs, the Netherlands (2014).
2. KARHU P., LAHKOLA A., MARKKANEN M., HELLSTÉN S., Example of a single national regulator responsible for both transport safety and security, invited paper to the IAEA International Conference on the Safe and Secure Transport of Radioactive Materials: the Next Fifty Years, Creating a Safe, Secure and Sustainable Framework, IAEA, Vienna, Austria (2011).
3. JOHANSSON, M., JÄRVINEN, M.-L., KARHU, P., NIEMELÄ, I. AND ROUTAMO, T, Use of nuclear energy and safety-security interface in the Finnish regulatory framework, IAEA Technical Meeting on the Safety and Security Interface – Approaches and National Experiences, IAEA, Vienna, Austria (2018).