Berg Heinz-Peter

Seidel Freddy
Bundesamt für Strahlenschutz, Salzgitter, Germany

Interface between nuclear safety and security

Keywords

safety, security, defence in depth, integrated approach, risk management, risk models

Abstract

Nuclear power plants benefit from a sophisticated and comprehensive safety regime that has been established over the years. However, the security regime for nuclear power plants is far less developed than the safety regime. Although adopting (and adapting) certain elements of the nuclear safety regime could significantly strengthen the nuclear security regime, at least four challenges are likely to surface: national sovereignty, information transparency, lack of policy consensus, and challenges of regime harmonization. Seek an optimal balance between mandatory international standards and voluntary actions and endorse consideration of additional binding and non-binding international safety and security requirements.

1. Introduction

In general, nuclear safety and nuclear security have a common purpose — the protection of people, society and the environment from unintended releases of radiation. In both cases, such protection is achieved by preventing a large release of radioactive material. Many of the principles to ensure protection are common, although their implementation may differ.

For nuclear safety or security reasons protection shall be ensured by good design, appropriate operational practices, including transportation waste disposal. This is necessary not just for nuclear material and facilities but also for radiological materials used at medical, agricultural, and industrial sites.

Many elements or actions serve to enhance both safety and security simultaneously. For example, the containment structure at a nuclear power plant serves to prevent a significant release of radioactive material to the environment in the event of an accident, while simultaneously providing a robust structure that protects the reactor from a terrorist assault.

Similarly, controls to limit access to vital areas not only serve a safety function by preventing or limiting exposures of workers and controlling access for maintenance to qualified personnel, but also serve a security purpose by inhibiting unauthorized access by intruders. Such controls may be of particular importance in the security context because the high radiation doses that might be encountered in a vital area may not be a significant deterrent given the apparent willingness of terrorists to loose their lives to achieve their objectives

These facts highlight the importance of a coordinated approach to nuclear safety and security in a way that they complement each other. The aim is to ensure that safety and security are dealt with together in a seamless and effective way.

The following definitions of nuclear safety and security are provided in [10]:

- nuclear safety as “the achievement of proper operating conditions, prevention of accidents and mitigation of accident consequences, resulting in protection of workers, the public and the environment from undue radiation hazards”.
- nuclear security, on the other hand, as, “the prevention and detection of and response to theft, sabotage, unauthorized access, illegal transfer, or other malicious acts involving nuclear material, and other radioactive substances, or their associated facilities”.

The events taken into account differ in each sphere. Safety evaluations focus on risks arising from unintended events initiated by natural occurrences (such as earthquakes, tornadoes, or flooding), hardware failures, other internal events or interruptions (such as fire, pipe breakage, or loss of electric power supply), or human mistakes (such as the incorrect application of procedures, or incorrect alignment of circuits). In the case of security, the risks, or events, feared arise from malicious acts carried out with the intent to steal material or to cause damage. Security events are therefore based on ‘intelligent’ or ‘deliberate’ actions carried out purposely for theft or sabotage and with the intention to circumvent protective measures.

The acceptable risk is presumptively the same whether the initiating cause is a safety or a security event. Moreover, the philosophy that is applied to achieve this fundamental objective is similar. Both safety and security typically follow the strategy of defence in depth — that is, the employment of layers of protection.

The fundamental nature of the layers is similar. Priority is given to prevention. Secondly, abnormal situations need to be detected early and acted on promptly to avoid consequential damage. Mitigation is the third part of an effective strategy. Finally, extensive emergency planning should be in place in the event of the failure of prevention, protection and mitigation systems.

Although a popular conception is that nuclear safety is primarily concerned with facilities while security focuses on material, the operational intersection has always been extensive.

Physical protection system should take into account a state’s system of accounting and control of nuclear material (commonly known as “safeguards”) and that all measures are in addition to, and not a substitute for, other measures established for safety purposes for material in use, transit, and storage.

Likewise, nuclear safety is much broader than just the safety of facilities – it also covers radiation, waste, and transportation safety.

Although safety and security are considered complementary, typical differences exist and are shown in *Table 1*.

In addition, further aspects where safety and security diverge are pointed out in [20]. One key difference is in risk assessment. For nuclear safety experts, an unintended release is the result of an unintentional incident. This can happen as a result of a natural occurrence (like the earthquake and tsunami in Japan), hardware failures, internal events or disruptions, or human error. Nuclear security experts, on the other hand, are most concerned with releases of radiation that result from intentionally destructive acts, including those designed to circumvent protective measures.

There are certainly similarities in the approaches to protection under safety and under security: both rely on in-depth defences; both place priority on prevention, early detection, and prompt action; and both require extensive emergency planning.

Table 1. Typical differences between safety and security

SAFETY	SECURITY
The nature of an incident is an inherent risk	The nature of an incident is caused by a human act
Non intentional	Intentional
No human aggressor	Human aggressor
Quantitative probabilities and frequencies of safety-related risks are available	Only qualitative (expert-opinion based) likelihood of security-related risks may be available
Risks are of a rational nature	Threats may be of a symbolic nature
Information is generally open	Information must be kept confidential

However, the different starting points of safety and security at times have implications for how measures are implemented and who implements them. For example, before Fukushima, probabilistic risk assessments for safety did not consider more than one “beyond design basis” event occurring (such as an earthquake and tsunami). On the other hand, nuclear security assessments must struggle with the attacker’s intention to defeat the system, potentially including a multi-pronged approach.

Another key difference is the approach to information sharing and transparency. In nuclear safety, information sharing is critical to the safe operation of plants, and the general inclination is to share information to avoid mistakes being repeated, including at other plants. For nuclear security, information is generally shared among a restricted group in order to maximize information security. Moreover, there may be kinds of information, for example, intelligence reports, which can be crucial to preventing sabotage, which lie outside the operators’ control. In fact, the role of the state in defining rules for confidentiality is much greater in the case of nuclear security than it is in nuclear safety.

Moreover, nuclear security often is implemented by law enforcement personnel, while nuclear safety is the purview primarily of engineers and radiation health experts. These experts approach problems in different ways and may work in different organizational structures with different incentives. Safety and security can also sometimes have contradictory imperatives. For example, a security incident could require a lock-down of the facility, whereas an accident would require easy access for operators and emergency personnel. Ensuring that measures are complementary rather than contradictory is important in the design, regulation, and operation of the facility.

2. The relationship between safety and security

Safety and security have traditionally been regulated and managed in isolation from each other. Safety management [2] has been the responsibility of operators, engineers, safety managers and scientists whereas security tends to be the responsibility of a separate function frequently led by ex-military and police personnel with a different professional background and range of competencies. Similarly, regulators for safety and security have traditionally been located in separate organisations [32].

This situation must change. The complex, interconnected nature of safety, security and emergency management requires convergence. Otherwise, gaps in capability and response will persist. Therefore, security needs to be integrated into the overall organisational management and development. An integration of the regulator bodies of the two fields would also be desirable.

Crises are, like the world in which nuclear sites operate, increasingly complex, networked, dynamic and fast moving. Convergence requires the adoption of an all hazards approach that concentrates on what needs to be done before and during a crisis. For this reason, assessing, mitigating and managing risk is a challenging task that cannot be done in isolation.

It also requires a fully integrated emergency planning that covers emergency arrangements as well as a proactive, trustworthy, empowered crisis communication mechanism that understands the unique requirements of both safety and security [7].

Moreover, it is necessary to fully integrate the response to an event into both safety and security arrangements.

On this background the adoption of an all hazards approach is required that concentrates on what needs to be done before and during a crisis.

It also requires an integrated response that covers emergency arrangements and a proactive, trustworthy, empowered crisis communication mechanism that understands both safety and security [32].

Moreover, nuclear safety and security management must be considered throughout the lifetime of the facility, which begins with the facility design and continues through commissioning, operation, decommissioning and dismantling [22].

The key difference is the intent of the actor that produced the loss event. It may never be possible to determine this intent but if the majority of activities is refocused on building better loss prevention strategies (regardless of actor intent), then this aspect may not matter anymore.

Note the common goal of mission assurance here, that is, the ability to complete a mission while enforcing constraints on how the mission can be achieved. In a nuclear power plant, for example, the goal is to produce power while preventing the release of radioactivity. The causes for not producing the power or for releasing radioactivity may be due to accidental or malicious reasons, but the high-level goal of preventing these events is the same.

The concept of defence in depth applies as much to nuclear security as to nuclear safety. At the design level of nuclear facilities, defence in depth relates to physical protection that reflects "a concept of several layers and methods of protection (structural, other technical, personnel and organizational) that have to be overcome or circumvented by an adversary in order to achieve his objectives" [13]. Such a defence involves a mixture of hardware (security devices), procedures (including the organization of guards and their performance), and facility design (including layout).

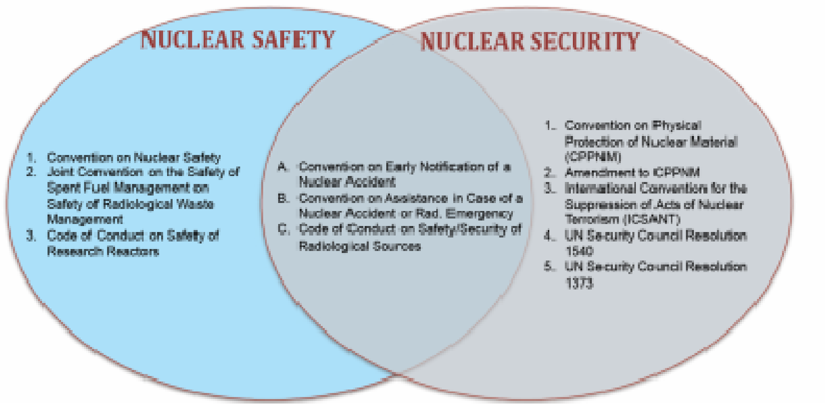
NUCLEAR SAFETY
NUCLEAR SECURITY
1. Convention on Nuclear Safety
2. Joint Convention on the Safety of Spent Fuel Management on Safety of Radiological Waste Management
3. Code of Conduct on Safety of Research Reactors
A. Convention on Early Notification of a Nuclear Accident
B. Convention on Assistance in Case of a Nuclear Accident or Rad. Emergency
C. Code of Conduct on Safety/Security of Radiological Sources
1. Convention on Physical Protection of Nuclear Material (CPPNM)
2. Amendment to CPPNM
3. International Convention for the Suppression of Acts of Nuclear Terrorism (ICSANT)
4. UN Security Council Resolution 1540
5. UN Security Council Resolution 1373

Figure 1. Intersection of nuclear safety and security regime elements according to [30]

Defence in depth in nuclear security should be based on the physical protection system, which serves to detect, delay, and respond effectively to attempts to harm a nuclear facility, and on the system for nuclear material accountancy and control to protect against insider and outsider threats [13].

An interaction between safety and security is necessary before making changes to plant configurations, facility conditions or security to ensure that potential adverse effects have been adequately considered and managed.

Factors which have to be taken into account in determining if a planned change will adversely affect safety or security are in particular [7]:

- Decrease system reliability or availability,
- Increase response times of emergency or security personnel,
- Interfere with the detection and assessment function, and
- Decrease the effectiveness of security plans.

Ineffective management of a safety and security interface could potentially result in:

- Delays of scheduled activities,
- Unintended security vulnerabilities,
- Unintended impacts to safety systems,
- Unintended impacts to emergency response activities, and
- Any cyber-related change.

Nuclear safety, like nuclear security, relies on guidance promulgated by the IAEA and published in a series of guidance documents. These include fundamental safety principles and objectives, general safety requirements and guides, and general and specific safety guides for particular types of facilities and activities. The safety standards help guide national requirements and serve as the basis for peer reviews. Guidance documents for nuclear security are less comprehensive.

The pace and scope of development of the nuclear security and nuclear safety regimes is in many ways tied to international attention to the "problem." Crises focus energy and attention on "fixing" deficiencies in systems and regimes. To date, there has not been a nuclear security crisis on the order of those in nuclear safety (Three Mile Island, Chernobyl, and Fukushima).

In many respects, agreement by world leaders to hold nuclear security summits is an acknowledgement of the need to act now to avert potential crises. The nuclear security summit process has transformed the global dialogue on nuclear security, also with respect to the interface between safety and security. Issues that were preciously handled by office directors have been elevated to the level of presidents and prime ministers. This has forced countries to establish interagency cooperation on nuclear security that in many cases was absent before; it has greatly broadened understanding and perception of the threat and leaders' desire for deliverables to announce forced through many decisions that might otherwise have delayed for years [5].

The decision of the last Nuclear Security Summit in March 2014 in Den Haag was to continue its activities with a further meeting in 2016 and – in parallel – to find some form of a continued high-level dialogue, maybe to get international support to integrate these activities in the framework of the International Atomic Energy Agency (IAEA).

In the meantime, the development of a strong nuclear security regime has lagged in comparison to that of nuclear safety [30].

Given the complementary nature of safety and security, a key question is whether one regime can learn lessons from the other. Given that nuclear safety crises have spawned new organizations, international legal instruments, and new approaches, does it make sense to move forward in a similar fashion for nuclear security even in the absence of a crisis? If so, what existing barriers to new organizations, instruments, and approaches would need to be overcome?

One possibility of a unified approach is shown in *Figure 2*.

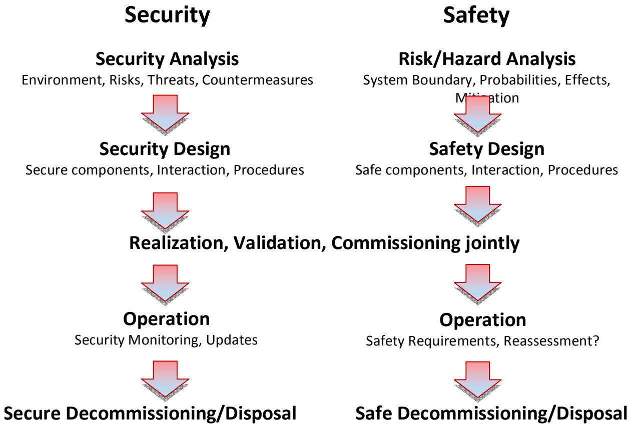
Security
Safety
Security Analysis
Environment, Risks, Threats, Countermeasures
Risk/Hazard Analysis
System Boundary, Probabilities, Effects, Mitigation
Security Design
Secure components, Interaction, Procedures
Safety Design
Safe components, Interaction, Procedures
Realization, Validation, Commissioning jointly
Operation
Security Monitoring, Updates
Operation
Safety Requirements, Reassessment?
Secure Decommissioning/Disposal
Safe Decommissioning/Disposal

Figure 2. One possible unified approach according to [27]

3. Interface between nuclear safety and cyber security

Observations from the near past show the evidence that cyber threats have been also directed on software-based instrumentation and control (SB I&C) systems of industrial processing plants. For instance, the Stuxnet attack [28] targeted the instrumentation and control of a nuclear facility. As a consequence, there is an urgent need to analyze and protect SB I&C performing functions important to safety according to cyber security. This is necessary in addition and in close correspondence to the well-established means and precautions used to provide a dependable SB I&C safety application.

New documents such as [12] and [18] as well as the national German guidance [4] provide assistance to establish a cyber security framework for nuclear facilities describing the fundamental objectives, guidance, requirements and recommendations on how to perform cyber security tasks in a systematic and comprehensive manner. For instance, these documents give generic guidance to develop a national design basic threat (DBT), a cyber security policy, as well as a facility specific cyber security plan.

To illustrate the previous chapter 2, exemplarily some particularly aspects are discussed both from the cyber security and safety point of view. This (non-complete) synopsis is mainly based on the guidance given in [12] and [18].

The state authority is responsible for defining the cyber security objectives and to derive a design basis threat (DBT) from the actual global and local threat situation. In comparison to safety objectives the cyber security objectives might additionally include the prevention of theft and intentional misuse of radioactive material. Because the threat situation is changing in time the DBT should be updated more often than the basis for the safety basis which particularly includes the design basis accidents (DBA). The set of DBA is typically defined by all the involved parties (authority and industry) but the final responsibility on safety bears the licensee.

In order to implement and maintain cyber security a plant specific cyber security plan is to be developed which involves e.g. prescriptions to following aspects:

- The high level documents such as on DBT and the plant security policy the cyber security plan is to be embedded,
- Roles and responsibilities for cyber security,
- Reporting and documentation requirements,
- Interfaces of the cyber security plan to other documents on plant specification,
- SB I&C asset management,
- Graded approach to SB I&C security and risk assessment,
- Implementation of cyber security controls (these are protective measures of technical or administrative nature), and
- Lifecycle qualification procedure.

Such plan prescribes the details to implement and maintain measures, such as [18]:

- Logical Access Control for human-machine interface in control rooms,
- Software update and patching,
- Logging and audit capability,
- Use of cryptography in I&C architectures and systems,
- System security hardening,
- System availability and function continuity,
- Emergency response & crisis management communication systems.

On the other hand, a safety plan is well established to develop and operate SB I&C according to a systematic approach, see e.g. [16] and [17]. Such safety plan comprises elements such as

- Graded approach for SB I&C development and licensing, and
- Qualification procedure covering the whole lifecycle of the SB I&C.

The above mentioned lists could easily completed to better show that there are similar approaches used for nuclear safety and cyber security, but it is worth to highlight the similarity of the lifecycle models. Systematic procedures with milestones or phases can be derived from the lifecycle model to perform both safety and security measures in parallel and in tight cooperation of the associated experts.

In principle following phase structure is common:

- Requirements specification,
- Design,
- Implementation,
- Integration/ commissioning,
- Operation, Maintenance, and
- Decommissioning/ retirement.

Generally, a lifecycle procedure requires a phase by phase development while a distinct phase cannot be finished until a verification step – or in the case of the integration/ commissioning phase the validation step - shows compliance with the requirements set before the phase was started. This is to ensure traceability over the whole lifecycle. Special tasks, such coding or testing, are allocated to the distinct phases.

For safety SB I&C modification there is the special request to follow most of the steps of the lifecycle phase again, because the impact range of a single software modification on the whole system cannot easily be assumed to be limited to the modified module. This request is reinforced for the modification of large distributed computer networks and particularly valid also from the cyber security perspective.

The change management based on a comprehensive asset analysis takes a crucial role to maintain safety and security. The asset analysis comprises in particular:

- Functions/tasks and operational modes of all SB I&C implemented at plant,

- Identification of relevant interconnections including power supplies,
- Dataflow analysis, to determine what communicates with what, and how and why,
- Procedures that initiate communication, frequency of communication, protocols,
- Computer systems and equipment location,
- Analysis of user groups,
- Ownership (for data and computerized systems), and
- Corresponding security level.

If a safety plan already has been followed most information needed for a security asset analysis should already be available. The asset analysis is followed by the analysis of the plant overall SB I&C architecture and the categorization of each of the asset elements according to its cyber security protection demand (defence in depth).

When all assets are categorized they will be assigned to security zones, where, e.g., the highest security level is assigned to systems, which are vital to meet the security objections of the facility. This approach can be compared with the safety classification of structures, systems and components applied in safety assessments.

Categorization is an important measure to implement the security defence in depth concept, e.g. to define interfaces between zones of different security level. According to a threat analysis the interfaces are to be protected by specifically selected and qualified security controls.

The following requirements commonly apply to zones of the highest security level [12]:

- No networked data flow of any kind (e.g. acknowledgment, signalization) should be authorized to enter this level. Only strictly outward communication should be possible. Note that this kind of strict one-way communication does not ensure reliability and integrity natively (redundancy/error corrections may be considered). Note also that this excludes any sort of ‘handshake’ protocols, even with controlled connection directions. Exceptions may only be considered on a strict case-by-case basis and if supported by a complete justification and security risk-analysis [12].
- Measures to ensure the integrity and availability of the systems are typically also required to be proved as a part of the safety case.
- No remote maintenance access is allowed.
- Physical access to systems is strictly controlled.
- The number of staff given access to the systems is limited to an absolute minimum.
- The two-person rule is applied to any approved modifications made within the computer systems.
- All activities should be logged and monitored.
- Every data entry to the systems is approved and verified on a case-by-case basis.
- Strict organizational and administrative procedures apply to any modifications, including hardware maintenance, updates and software modifications.

It is obvious that the implementation of a cyber security feature (a SB I&C system internal property to support cyber security) or control some of the above mentioned security requirements needs a strategy to meet the above mentioned requirements and recommendations in accordance with the safety objectives.

Therefore the mutual impact on safety and security has to be analyze and if necessary resolved. Some examples where a potential conflict has to be resolved might be the following [18]:

- The implementation of a cyber security feature or control shall not adversely impact the performance, effectiveness, reliability or operation of safety functions supported by SB I&C systems.
- The implementation of a cyber security feature directly in a pre-developed SB I&C system should be justified and otherwise avoided because of adding complexity and introducing new potential failure modes.
- Implementation of cyber security within or between safety systems shall be justified from both the safety and security side.
- If cyber security features are implemented in safety system displays and controls, they shall not adversely impact the operator’s ability to maintain the safety of the plant.
- Cyber security features and controls included in safety systems should be developed and qualified to the same level of qualification as the systems.
- Cyber security features should not significantly increase diagnostic and reparation time of safety functions.

On the other hand, a modification of the SB I&C might have an unintended impact on cyber security that also has to be resolved:

- The failure modes and effects of the changed SB I&C might have an unintended impact on cyber security (e.g. due to the change of transfer protocols, architecture, internal SB I&C safety properties such as self-diagnostic).
- When a required cyber security feature dedicated to a safety system cannot be

implemented because it is not compliant with the safety requirements, the compensating cyber security measures and/or equipment shall provide an equivalent level of cyber security protection for the safety system as the omitted feature would have provided.

A distinct cyber security issue is to develop and maintain a common SB I&C procurement strategy for the system vender and the component suppliers. This strategy should cover software and hardware development taking into account software or logic patterns embedded in pre-developed components such as complex programmed logic devices (CPLC), field programmed gate arrays (FPGA), or application specific integrated circuits (ASIC). Suppliers should meet the same security requirements as the vendor responsible for final product, the SB I&C system. It should be taken into account that a FPGA may be supplied without a separate software package, but be developed with software tools. Such tools should also be covered under distinct cyber security provisions.

As a last example, it should be noted that tools applied for development and qualification tools of SB I&C should be both under safety and security control according to the category the target system is assigned to. An appropriate safety qualification is either required for the tool or for the developed software. Similar strategies might be useful to prove the tool application from the security prospective.

Tool categorization according to the target system’s security level is still an open issue. The lack of demonstration tool dependability might be compensated by administrative measures (e.g. restricted facility and/or I&C operation mode during tool application) in combination with testing of the finalized target system.

4. Risk models

By taking a common top-down, system engineering approach to security and safety, several benefits accrue. One is that the overall role of the entire socio-technical system as a whole in achieving security and safety can be considered, not just low-level hardware or operator behaviour. Others include more efficient use of resources and the potential for resolving conflicts between safety and security early in the development process [35].

Today’s increasingly complex, software-intensive systems, however, are exhibiting new causes of losses, such as accidents caused by unsafe interactions among components (none of which may have failed), system requirements and design errors, and indirect interactions and systemic factors leading to unidentified common-cause failures of barriers and protection devices. Linear causality models and the tools built upon them, like fault trees, simply lack the power to include these new causes of losses [35].

STAMP (System-Theoretic Accident Model and Processes) is a new systems-theoretic model of causality related to emergent system properties. It was originally created to act as a foundation for more powerful approaches to safety (see [29] and [31]). Security, however, is also an emergent system property, and STAMP and its associated analysis tools are equally applicable to security [35].

STAMP is based on the observation that there are four types of hazardous control actions that need to be eliminated or controlled to prevent accidents (see [31] and [35]:

- A control action required for safety is not provided or is not followed.
- An unsafe control action is provided that leads to a hazard.
- A potentially safe control action is provided too late, too early, or out of sequence.
- A safe control action is stopped too soon or applied too long.

One potential cause of a hazardous control action in STAMP is an inadequate process model used by human or automated controllers.

In software, this process model is usually implemented in variables and embedded in the program algorithms. Accidents or intended attacks can therefore occur when an incorrect or incomplete process model causes a controller to provide control actions that are hazardous.

New and more powerful techniques for safety analysis and design have been created on this theoretical foundation. STPA (System-Theoretic Process Analysis), for example, is a new analysis technique built on the STAMP [1]. The analysis is performed on the system functional control structure. STPA is currently being used for safety and security problems in a wide variety of industries.

The security in nuclear power plants can be also investigated by dynamical assessment One example is given in [36], where a nonlinear dynamic algorithm is applied to the advanced security assessment, which is called the systems thinking analysis. The cyber security evaluation tool [8] gives the user operators a repeatable and systematic ways for assessing the cyber security state of the industrial control system networks.

Risk models define the risk factors to be assessed and the relationships among those factors. Risk factors are characteristics used in risk models as inputs to determining levels of risk in risk assessments. Risk factors are also used extensively in risk communications to highlight what strongly affects the levels of risk in particular situations, circumstances, or contexts. Typical risk factors include threat, vulnerability, impact, likelihood, and predisposing condition [26].

Figure 3 illustrates an example of a risk model including key risk factors and the relationship among the factors.

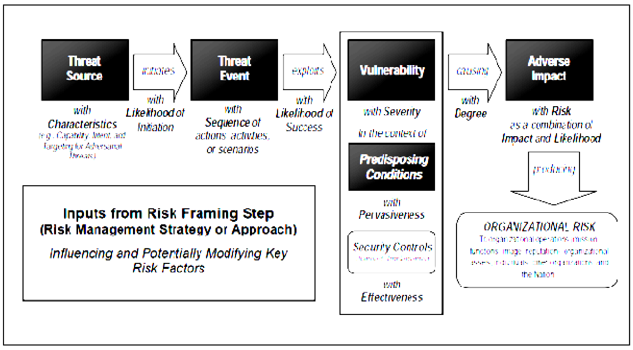
Threat Source
initiates
with Likelihood of Initiation
with Characteristics
(e.g., Capability, Intent, and Targeting for Adversarial Threats)
Threat Event
with Sequence of actions, activities, or scenarios
exploits
with Likelihood of Success
Vulnerability
with Severity
In the context of
Predisposing Conditions
with Pervasiveness
Security Controls
with Effectiveness
causing
with Degree
Adverse Impact
with Risk
as a combination of
Impact and Likelihood
producing
ORGANIZATIONAL RISK
To organizational operations (mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation
Inputs from Risk Framing Step
(Risk Management Strategy or Approach)
Influencing and Potentially Modifying Key Risk Factors

Figure 3. Generic risk model with key risk factors according to [26]

Physical security involves measures undertaken to protect personnel, equipment and property against anticipated threats. It includes both passive and active measures.

Passive measures include the effective use of architecture, landscaping and lighting to achieve improved security by deterring, disrupting or mitigating potential threats.

Active measures include the use of proven systems and technologies designed to deter, detect, report and react against threats.

Information security is the process of protecting the confidentiality, integrity and availability of data from accidental or intentional misuse by people inside or outside an organization or facility. Key elements of information security include limiting information exclusively to authorized entities; preventing unauthorized changes to or the corruption of proprietary data; guaranteeing authorized individuals the appropriate access to critical information and systems; ensuring that data is transmitted to, received by or shared with only the intended party; and providing security for ownership of information.

A security risk assessment should identify which assets need to be protected and how critical each asset is. This requires looking at each asset with regard to human resources and infrastructure. Facility executives should also determine the extent to which core business activities rely on continuous and uncorrupted operations.

A security risk assessment should also identify and characterize threats. These should be viewed as potential occurrences with a hostile intent that will directly affect the host building or organization and be capable of causing damage to others. Methods and approaches are provided in [15].

The current thinking on threat assessment at nuclear facilities in the United States is illustrated in [24].

An assessment of vulnerabilities is critical as well, derived from a systematic survey approach that considers physical, informational and operational features, as well as assets and threats to the building or company.

There are three levels of risk. The first involves the damage resulting from the failure to protect confidential data or from unscheduled downtime. This affects the short-term performance of an organization.

The second risk level is the failure to protect confidential data that can have a ripple effect beyond the company's organization - suppliers, customers and partners, for example. Losses in this instance could be extensive with both temporary and permanent damage to business operations and organizational assets.

The third level of risk is the failure to protect confidential data or to prevent unscheduled downtime that has a cascading effect with potentially devastating consequences felt well beyond the host organization. The resulting damage and losses may be enormous with potential global implications. Unscheduled downtime can potentially threaten public safety, financial stability, and regulatory compliance and even cause loss of life.

Once risks and vulnerabilities are assessed, they should be prioritized along with means to counter and respond to them. This final step allows particular weaknesses to be identified and addressed accordingly.

Senior management must have a thorough analysis of all risks and vulnerabilities to make risk-informed decisions.

5. Safety and security culture

Nuclear safety and security culture are defined as:

- nuclear safety culture as. "that assembly of characteristics and attitudes in organisations and individuals which establishes that, as an overriding priority, protection and safety issues receive the attention warranted by their significance".
- 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".

Achieving effective nuclear security requires a strong security culture in which all staff takes security seriously and gives it the priority which it requires. Organizational culture is equally critical in nuclear safety, and a vast literature has developed on practices to strengthen safety culture (see, e.g. [3] and [14]).

What can be done to build a security culture [11] where all key staff take security seriously and are always on the lookout for vulnerabilities and ways to fix them? The IAEA [19] and the World Institute for Nuclear Security (WINS) [34] have each published guides to strengthening security culture. The key to a strong security culture is belief in the threat "never forgetting to be afraid" as the saying goes. In addition, it is crucial to structure incentives to motivate key staff to take security seriously and invest their time and effort in it.

For a safety culture, great emphasis is placed on sharing information openly, because of an overriding concern for transparency and dialogue wherever possible. A strong security culture places responsibility on the respective organization to respond immediately to confirmed or perceived threats/incidents and to restrict associated communication to authorised persons on a strict 'need-to-know' basis.

Although there is a difference in the approach in some areas, both safety and security cultures need to coexist and should – wherever possible – reinforce the goals of each, because they share a common objective by limiting nuclear risk. This objective is also largely based on similar principles, for example, of adopting a questioning attitude, rigorous and prudent approaches, and effective and open two way communication.

It should be noted that a security culture will require different attitudes and behaviour, compared with a safety culture, such as, when appropriate, the confidentiality of information and efforts to deter, detect, delay and respond to malicious capabilities. On occasions when there are differences between safety and security requirements, any conflict should be identified as soon as possible.

6. Regulations

The nuclear safety and security regimes rely principally on national decision-making, laws, and regulations. This is supplemented by international agreements and organizations that largely offer voluntary guidance. In general, the implementation of the regimes is incentive based and many believe that this is preferable to mandatory requirements.

Four elements central to the nuclear safety regime have direct applicability to the nuclear security regime but are not yet integrated into it. These include:

- regularized assessments,
- information sharing,
- peer review, and
- review of the implementation of relevant international conventions.

These elements are embodied in the Convention on Nuclear Safety (CNS) and have been critical to the improvement of nuclear safety over time. Neither of the nuclear security regime's key international conventions – the Convention on the Physical Protection of Nuclear Materials (CPPNM) and its amendment nor the International Convention for the Suppression of Actions of Nuclear Terrorism (ICSANT) includes provisions for assessment, information sharing or peer review [25].

In nuclear safety, regulators require that people and companies undertaking certain roles have certified competence to fulfil their duties.. Extensive training programmes exist that allow participants to achieve the necessary certification if they pass tests demonstrating their knowledge of the needed material. Nothing similar yet exists for nuclear security – either for the people or for the equipment.

Nuclear security training is now very much in vogue. An increasing number of countries are establishing nuclear security training and support centres; the IAEA is offering an expanded set of relevant training courses, and seeking to coordinate the work of the national centres; and the IAEA and a group of universities have established a new master's degree program in nuclear security.

But it is less clear whether all this training will be of the type and quality that is needed; in-depth needs assessments and tailoring of training to those needs are steps that remain to be taken, in most cases [5].

Although adopting (and adapting) certain elements of the nuclear safety regime could significantly strengthen the nuclear security regime, at least four challenges are likely to surface: national sovereignty, information transparency, lack of policy consensus, and problems of regime harmonization [25].

Introducing more binding international standards however, could address concerns about weak links in national nuclear safety and security regulation and implementation. They could supplement the current regimes without dismantling the incentives in place. The objective would be to have greater uniformity of safety and security standards and to encourage countries and operators that are lagging to improve up to the highest standards. One option for international standards could include negotiating a baseline for nuclear security, or states could provide advance consent to the IAEA for periodic evaluations of their security measures such as in case of nuclear safety.

7. Concluding remarks and outlook

There has been remarkable consistency in the identification of the four key governance improvements that are needed. The regime needs to be more cohesive and its current components universalized and maximally utilized. There needs to be greater cross-border communication of non-sensitive information for the purpose of building international confidence in the system.

The system requires the institution of a peer review process similar to that employed in the nuclear safety regime. Moreover, best practices need to be disseminated, but allowed to be implemented in a flexible and culturally sensitive manner. These improvements can be made through both soft and hard governance approaches on a continuum. But, to be effective over the long term, there ultimately needs to be specific benchmarks that nations must meet.

In developing best practice, WINS [33] uses the following criteria to guide us:

- Impact/Effectiveness:
  The practice has demonstrated impact, applicability and benefits to the nuclear security programme.
- Efficiency:
  The practice has demonstrated cost and resource efficiency, where the expense is appropriate to the benefits.
- Sustainability:
  The practice has demonstrated sustainable benefits and/or is sustainable within nuclear and related organisations.
- Collaboration/Integration:
  The practice builds effective partnerships among various organisations and integrates nuclear security with other functions such as nuclear safety, emergency planning and design.

Strengthening the safety-security interface will be a complex undertaking. Systems that prevent and respond to nuclear accidents and nuclear terrorism must be improved and, where they overlap, made to work seamlessly with one another. They must also take into account a third type of possible nuclear catastrophe: the combined disaster, in which opportunistic antagonists time their malicious activity to take advantage of natural disasters that weaken nuclear safety systems (see [21] and [22]). The apparent lack of security in the immediate aftermath of the Fukushima meltdowns highlights the need for planning for such combined nuclear dangers.

Nuclear security, like nuclear safety, requires a focus on continual improvement and striving for excellence that stretches decades into the future.

In the field of nuclear safety, when an incident occurs, the plant performs a root cause analysis and develops lessons learned to prevent similar incidents from occurring again. These incident reports and lessons learned are then shared on national and international level. Moreover, regulators inspect plants to assess how well reactor operators are implementing the lessons learned [5].

Nothing remotely resembling this approach exists in the security world. It is time to begin such an effort – assessing security-related incidents in depth, exploring lessons learned, and distributing as much of this information among nuclear security operators as necessary secrecy will allow; non-nuclear incidents that reveal types of tactics against which nuclear materials and facilities should also be included. Information about incidents and how to protect against them could be a major driver of nuclear security improvement, as it has been in safety; in a recent survey of nuclear security experts in 18 countries with weapons-usable nuclear material, incidents were cited far more often than any other factor as a dominant or very important driver of countries’ recent changes in nuclear security policies [6].

States could begin with internal assessments of events within their territory, and then provide as much information as can reasonably be exchanged to an international collection of information.

Unlike other major accidents, the Fukushima crisis also highlighted the vulnerability of spent fuel pools. A re-evaluation of their design and permissible loading limits is likely. This could also prompt more support for moving spent nuclear fuel out of wet storage and into dry cask storage away from the reactor more quickly. Such improvements would benefit both safety and security.

More broadly, the Fukushima crisis highlighted the vulnerability of the infrastructure needed to support nuclear power by demonstrating just how disruptive a major accident can be. Efforts to strengthen that infrastructure will have both safety and security benefits.

A Fukushima-like nuclear accident does not have to be caused by nature. Similar results could be wrought by a dedicated terrorist group that gained access to a nuclear power plant and disabled its safety systems. To guard against natural accidents, terrorist sabotage, and possible combinations of these two classes of events, nuclear plant operators and regulators should consider a combined approach [23].

Although safety and security programs have different requirements, they overlap in key areas and could support and enhance one another. Nuclear facilities could improve safety-security in technical ways, including more secure emergency electrical supplies, better security for control rooms, and, at new plants, reactor containment structures built to survive attacks by terrorist-flown airplanes. At the institutional level, regulators could strengthen the safety-security interface by requiring that it be built into the life cycle of nuclear plants, from design to dismantlement.

A focus on performance – achieving a very low risk of accident, rather than just following a set of safety rules – has been a critical element in the nuclear safety progress of recent decades. Nuclear security should move in the same direction. A performance-based approach is far more complex in the case of security, however, because adversaries adapt to the defensive measures, choosing to strike at the weakest point as best they can, in a way that earthquakes and human errors do not.

As with nuclear safety, in nuclear security states not only need to establish clear performance objectives, they need to develop means to assure themselves (and to assure others) that those objectives are being met. Yet in the case of nuclear security, it is equally important to keep the details of the security in place for each operation secret. No one wants potential terrorists or thieves to know the details of the security systems they will have to defeat.

Internally, performance assurance should begin with regular self-assessment by the operators, including in-depth vulnerability assessments. This must then be followed by in-depth inspection by the regulator, focused not just on a checklist of items in place but on a detailed judgment of whether the overall system is providing the required performance.

Finally it should be underlined that the aspects of a necessary interface between safety and security is not only a topic in the nuclear field but also, e.g., in aviation, maritime and rail transport.

References

[1] Asplund, F. (2012). Safety and Tool Integration, A System-Theoretic Process Analysis, TRITA–MMK 2012:01.

[2] Berg, H. P. (2010). Risk based safety management to enhance technical safety and safety culture. *Transactions ENC 2010 – European Nuclear Conference*.

[3] Berg, H.P. & Kopisch, C. (2013). Safety culture and its influence on safety. *Journal of KONBiN* 23, 1, 17–28.

[4] Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit (BMU). (2013). Richtlinie für den Schutz von IT-Systemen in kerntechnischen Anlagen und Einrichtungen der Sicherungs-kategorien I und II gegen Störmaßnahmen oder sonstige Einwirkungen Dritter (SEWD-Richtlinie IT). Announcement of July 8th, GMBl, 36, 711. (without text).

[5] Bunn, M. (2012). Strengthening global approaches to nuclear security. *International Conference on Nuclear Security: Enhancing Global Efforts* - International Atomic Energy Agency, Vienna, July 1, 2013.

[6] Bunn, M. & Harrell, E. (2013). *Threat Perceptions and Changes in Nuclear Security around the World: Results of a Survey, Project on Managing the Atom.* Harvard University, Cambridge, Mass.

[7] Dapas, M.L. (2012). An integrated approach to managing the safety / security interface. *International Regulators Conference on Nuclear Security*, Rockville, Maryland, USA, December 4 - 6.

[8] Department of Homeland Security (2011). Cyber Security Evaluation Tool (CSET), Performing a Self-Assessment, Washington, DC, USA.

[9] Howsley, R. (2012). Best practices in nuclear security and the role of the World Institute for Nuclear Security (WINS). *2012 Seoul Nuclear Industry Summit*.

[10] International Atomic Energy Agency (IAEA). (2007). IAEA Safety Glossary: Terminology Used in Nuclear Safety and Radiation Protection. Vienna, Austria.

[11] International Atomic Energy Agency (IAEA). (2008). Nuclear Security Culture. Nuclear Security Series,7, Vienna, Austria.

[12] International Atomic Energy Agency (IAEA). (2011). Computer Security at Nuclear Facilities – Reference Manual, IAEA Nuclear Security Series, 17, Technical Guidance, Vienna, Austria.

[13] International Atomic Energy Agency (IAEA). (2011). Nuclear Security Recommendations on Physical protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5). IAEA Nuclear Security Series, 13, Vienna, Austria.

[14] International Atomic Energy Agency (IAEA). (2013). Regulatory Oversight of Safety Culture in Nuclear Installations. IAEA-TECDOC-1707, IAEA, Vienna, Austria.

[15] International Atomic Energy Agency (IAEA). (2013). Threat assessment and risk-informed approach for implementation of nuclear security measures for nuclear and other radioactive material out of regulatory control. Nuclear Security Series, Draft.

[16] International Electrotechnical Commission. (2009). Nuclear power plants – Instrumentation and control systems important to safety – Classification of instrumentation and control functions. IEC 61226, Ed. 3.0.

[17] International Electrotechnical Commission. (2011). Nuclear power plants – Instrumentation and control systems important to safety – General requirements. IEC 61513, Ed. 2.0.

[18] International Electrotechnical Commission. (2013). Nuclear power plants – Instrumentation and control systems important to safety – Requirements for coordinating safety and security., IEC 62859, Committee draft 1, under development.

[19] International Nuclear Safety Advisory Group (INSAG). (2002). Key Practical Issues in Strengthening Safety Culture. INSAG-15, International Atomic Energy Agency, Vienna, Austria.

[20] International Nuclear Safety Advisory Group (INSAG). (2010). The Interface between Safety and Security at Nuclear Power Plants. INSAG-24, International Atomic Energy Agency, Vienna, Austria.

[21] Khripunov, I. & Kim, D. (2011). Nature and malice: confronting multiple hazards to nuclear power infrastructure. *Bulletin of the Atomic Scientists*.

[22] Khripunov, I. & Kim, D. (2011). Time to think safety-security. *The Korea Times*.

[23] Kim, D. & Kang, J. (2012). Where nuclear safety and security meet. *Bulletin of the Atomic Scientists* 68, 1, 86–93.

[24] Kuperman, A.J. & Kirkham, L. (2013). Protecting U.S. Nuclear Facilities from Terrorist Attack: Re-assessing the Current “Design Basis Threat” Approach. *Institute of Nuclear Materials Management 54t^{h} Annual Meeting*, Palm Desert, CA.

[25] Luongo, K., Squassoni, S. & Wit, J. (2011). *Integrating Nuclear Safety and Security: Policy Recommendations*. Center for Strategic and International Studies.

[26] National Institute of Standards and Technology (NIST) (2012). Guide for Conducting Risk Assessments. NIST Special Publication 800-30, Revision 1.

[27] Schoitsch, E. & Bleier, T. (2013). *Safety vs. Security*. Available: www.fh-campuswien.ac.at/ index.php?downloadSemantec Security Response (2011). *W32.Stuxnet Dossier, Version 1.4*.

[28] Song, Y. (2012). *Applying system-theoretic accident model and processes (STAMP) to hazard analysis*. Thesis.

[29] Squassoni, S. (2012). Nuclear safety and security. *2012 Seoul Nuclear Security Summit*.

[30] Thomas, J. (2012). *Extending and Automating a Systems-Theoretic Hazard Analysis for Requirements Generation and Analysis*. Sandia Report SAND2012-4080.

[31] World Institute for Nuclear Security (WINS). (2009). Nuclear Security Culture: A WINS Best Practices Guide for Your Organization.

[32] World Institute for Nuclear Security (WINS) (2011). An Integrated Approach to Nuclear Safety and Nuclear Security, International Best Practice Guide.

[33] World Institute for Nuclear Security (WINS) (2011). Time for an Integrated Approach to Nuclear Risk Management, Governance and Safety/Security/Emergency Arrangements.

[34] Young, W. & Leveson, N.G. (2014). Inside risks, an integrated approach to safety and security based on systems theory. *Communications of the ACM*, 57, 2, 31–35.

[35] Woo, T.H. (2013). System thinking safety analysis: nuclear security assessment of physical protection system in nuclear power plants. *Science and Technology of Nuclear Installations*, Hindawi Publishing.