# THE MEANING OF RISK FOR SAFETY, SECURITY, AND SAFEGUARDS IN THE DESIGN OF ADVANCED NUCLEAR REACTORS

D.N. KOVACIC1, F. PARADA1, A. HUNING1, G. RENDA2, G.G.M. COJAZZI3

1Oak Ridge National Laboratory, Oak Ridge, Tennessee, US

2European Commission Joint Research Centre, Ispra (VA), Italy

3European Commission Joint Research Centre, Ispra (VA), Italy, retired

**Abstract**

What is the meaning of risk as it applies to the design of advanced reactors in the disciplines of safety, security, and safeguards? How can we find common terminology for the concept of risk, and how can we find interfaces between these disciplines? These are important questions that should be explored in order that they may be applied in an integrated manner for the most effective and efficient design approaches. Eliminating or minimizing risks is a key design driver that motivates and informs the development of nuclear reactors. For safety, risk is well understood and applied in probabilistic risk assessments. For security, the risk-based concepts of vulnerability assessments and vital areas are all considered in designing security systems. For safeguards, the concept of risk is not formally defined as it relates to the design and operation of nuclear reactors. International nuclear safeguards seek to reduce the risk of proliferation in the nuclear fuel cycle, and as such the concept of risk does exist. Therefore, the current understanding of the “3S” approach, which seeks to find the interfaces and conflicts between safety, security, and safeguards, requires a thorough understanding of the role that the reduction of risk plays in all three disciplines. The intersection of risk for safety and security is now being developed because there is a strong correlation between reactor design and operations and their vulnerability to sabotage. The intersection of risk for security and safeguards has to date chiefly been focused on the nuclear material control and accounting systems, which are relied on by both the operator (State) and the International Atomic Energy Agency. This paper explores the concept of risk in each of the three disciplines, how they interact, potential conflicts and interface sand how they might be addressed and leveraged, and a notional framework for how this could be achieved.

## INTRODUCTION

Advanced reactors that are currently being designed, including small modular reactors, will have to be compliant with the nuclear safety, security, and safeguards (3S) disciplines. While having different origins and implementations, the three disciplines will inevitably interact with each other, with the potential of creating synergies or conflicts that can have a significant effect on the operation of the facility. Safety is always taken into account at a reactor’s design stage, but security usually receives less attention, and international safeguards[[1]](#footnote-2) are often neglected. Building on the very strong “safety by design” culture ubiquitous among nuclear designers, there is now a unique opportunity to consider security and safeguards by design concepts into advanced reactor development from very early design stages. Because safety by design is usually ensured and achieved through risk-informed approaches, it is worth investigating the possibility to extend this approach to a more comprehensive risk-informed approach to 3S. The concept of risk is very well defined for nuclear safety and is internationally agreed upon, whereas, in nuclear security, which is the operator’s responsibility, risk elements have been imported from safety, but no standard definition has been universally recognized. Consequently, a robust risk-informed approach to nuclear security supporting a by-design exercise is still under investigation and has yet to become an internationally accepted best practice. Although nuclear safeguards are not usually considered by designers, proliferation risk at the facility and the State level, primarily related to the International Atomic Energy Agency (IAEA) and other relevant governmental stakeholders, has been discussed, and the issues related to nuclear safeguards are well known and have been studied at length. Although this focus is on the IAEA, the international body overseeing safeguards implementation, is crucial, it is equally important to consider the designer's viewpoint, especially for the deployment of advanced reactors and new fuel cycles. To successfully do this, we need to look at risk from a different perspective.

Implementing safeguards after facilities are constructed can be costly and technically challenging and can often cause project delays. Safeguards are often overlooked by designers because their understanding is that safeguards approaches are developed and implemented by the IAEA and are negotiated with States and operators. As a consequence, “[...] there is little incentive for facility designers to follow the developments in the safeguards arena and to analyse what impact they may have on their design concepts.” [1]. The impact of not considering safeguards in the design in traditional light water reactor (LWR) technology is limited because the technology is well understood by the IAEA; however, new fuel cycles and unique reactor designs may possess characteristics that depart significantly from current LWR designs and, as such the IAEA will have to consider how safeguards will be applied. To educate designers, the IAEA prepared a series of facility-specific guidelines fostering a safeguards-by-design point of view among new nuclear energy systems designers and vendors [2-4].

Additionally, there is the possibility that the required safeguards technologies or approaches are not mature enough to be effectively and efficiently applied to certain reactor designs. If the application of safeguards is not taken into consideration before the reactor design is mature, the safeguards will be left to be wholly implemented during construction, and inherent risks will be posed for all relevant stakeholders in the form of increased costs and project delays.

## THE MEANING OF RISK

Nuclear safety has broad understanding and support within the industry; however, the concept of risk takes on a different meaning for designers when it comes to nuclear security and safeguards. All of the 3S acknowledge the importance of risk and have tools to manage it, albeit at different times and by different stakeholders (e.g., designer, owner/ operator, State, IAEA); however, there is still no consensus on a unified approach to the concept of risk and its assessment, and a unified approach to risk and its assessment within the 3S framework remains an open issue.

### The Meaning of Risk for Safety

For nuclear safety, risk is defined in the context of potential unintended events or system failures that lead to an uncontrolled release of radioactive material threatening workers, the public, and the environment. According to the *IAEA Nuclear Safety and Security Glossary*, nuclear safety is “The achievement of proper operating conditions, prevention of accidents and mitigation of accident consequences, that result in protection of workers, the public and the environment from undue radiation risks” [5]. To achieve proper operating conditions, prevent accidents, and mitigate risk, measures, systems, and procedures are designed to control radiation exposure and lower the likelihood of events that can lead to radiological consequences if they were to occur.

Nuclear safety is comprehensively understood and supported by the nuclear industry. It has developed robust systematic approaches that quantify risk by analysing the likelihood and severity of potential accident scenarios. The objective of a safety analysis, either deterministic safety analysis or probabilistic risk assessment, is to identify and quantify the risks associated with potential nuclear safety accidents. A key concept in safety is the Design Basis Accident (DBA), hypothetical accident scenarios that the facility must withstand and respond to. It is defined in the IAEA Safety glossary as “*A postulated accident leading to accident conditions for which a facility is designed in accordance with established design criteria and conservative methodology, and for which releases of radioactive material are kept within acceptable limits*.” [5]

Safety analysis will cover events that are considered accidental or unintentional (i.e., derived from the failure of components or safety systems, human error, or a natural disaster). These safety accidents are known, and depending on the type of analytical approach, the probability of occurrence can be estimated. Risk is generally expressed as “a set of triplets, , where *S*i is an identification or description of a scenario i, *p*i is the probability (i.e., likelihood) of that scenario, and *X*i is a measure of the consequence of the scenario” [6].

Generally, from extensive global operating experience of nuclear reactors, the safety risks are well known governed by regulations and requirements that are well recognized and understood. This experience is being used for assessing the safety risk of advanced reactor designs and this is a major focus of designers to reduce the costs associated with safety systems, the size of emergency planning zones, and emergency preparedness measures.

### The Meaning of Risk for Security

Unlike the nuclear safety measures and analyses that are designed to prevent known hazards and risks related to the operation of nuclear power plants, security threats are not static and can evolve over time. After the attacks of 9/11, the concept of risk for nuclear security was heavily revised in the United States and internationally. Since then, the details pertaining to nuclear security requirements and the implementation measures to meet them changed drastically as the new level of threat of potential adversaries was being considered.

The *IAEA Safety and Security Glossary* defines nuclear security as “The prevention and detection of, and response to, criminal or intentional unauthorised acts involving or directed at nuclear material, other radioactive material, associated facilities or associated activities” [5]. Although the glossary does not define security risk, it can be considered in terms of the risk that the design has vulnerabilities to potential deliberate malicious acts that could have a negative impact in the operation of the facility. This includes theft, sabotage, or access (physical or cyber) by an individual or a group with the objective to acquire nuclear or radioactive material for malicious purposes. Such individuals or groups can be motivated by different reasons, and they may have the capabilities, knowledge through insider information or other means, and equipment at their disposal to commit a malicious act.

Therefore, a nuclear security system needs to consider malicious events with sophisticated techniques and unpredictable scenarios where the assistance from an insider might exist. The system would be built by integrating security measures that serve to prevent an adversary from completing their objective, and its performance would be analysed to assess whether it complies with national regulatory standards. Overall, the objective of the assessment is to determine the effectiveness of the nuclear security and physical protection system in place, and it should provide information on the performance of the security measures to prevent the completion of a malicious act.

An essential function of a security system is to deter attacks. A robust security system is a success if it discourages potential adversaries from attempting a malicious act. A key challenge in quantifying nuclear security risk lies in the nature of the threat. The 2022 IAEA Safety and Security glossary makes a distinction between threat and an adversary. While a threat consists of “A person or group of persons with motivation, intention and capability to commit a malicious act.” [5] An adversary is considered when the threat takes action and initiates an attempt at a malicious act. Estimating the likelihood and potential success of a threat departs significantly from traditional safety assessment, which focuses on unintentional events.[5] A nuclear security risk is inherently conditioned to an attack and cannot be estimated in absolute terms. In one hand, the intention of a nuclear security threat most likely changes from one event to the other giving unpredictability to the underlying nature of the event. On the other hand, the small quantity of events can create an issue for statistical analysis. Given that a given attack occurs, a success, both the probability of success of the attacker and the consequences of the attack can be estimated as well.

Unlike nuclear safety, security risk does not have an internationally accepted formal definition. Nuclear security is the responsibility of each individual State, and various organizations within the country contribute to shape the overall nuclear security regime. Usually, the nuclear security design basis threats (somewhat analogous to the safety design basis accidents) are classified and different for each State, making an international harmonization of nuclear security risk-informed approaches challenging. There are several ongoing efforts to translate the risk-informed approach used in safety for use in the security domain. The objective is to optimize the design of physical protection systems, the most difficult being to quantify the likelihood of an attack [7].

### The Meaning of Risk for Safeguards

Regarding safety, risk is associated with accidents and unintentional events. Regarding security, risk is associated with the acts of malicious individuals or groups. The concept of risk in nuclear safeguards differs significantly. For safeguards, the potential for a State to divert nuclear material or misuse nuclear technology becomes the primary concern. The IAEA and other regional organizations such as European Atomic Energy Community and Brazilian-Argentine Agency for Accounting and Control of Nuclear Materials, have the right and obligation to design and enforce safeguards measures. These are defined as “the technical means by which the IAEA verifies States undertakings under their safeguards agreements and protocols” [8]. Unlike safety and security systems, which are typically national responsibilities, safeguards are implemented by an international inspectorate. The purpose of safeguards, as defined in the *IAEA Safeguards Glossary* is to “verify the undertakings of States under their respective safeguards agreements with the IAEA. Independent IAEA verification provides assurance to the international community that States are fulfilling their commitments concerning the peaceful use of nuclear energy and deters States, through the *risk of early detection[[2]](#footnote-3)*, from acquiring or using nuclear material, facilities and/or other items subject to safeguards for proscribed purposes” [8]. Thus, the potential misuse of the technology, diversion of material, and the development capabilities and knowledge to proliferate is the risk from a safeguards perspective. There have been several efforts to define nuclear proliferation risk in the past decades, with various degrees of success. One of the most recent and sound attempts to translate the nuclear safety risk triplet to the nuclear proliferation domain defined proliferation risk as made up of the following components: “1) the probability that a host State will choose to proliferate along a particular or multiple pathways (L), 2) the probability of success of that path (P), 3) the consequences of proliferation (C)” [9]. Similarly with security, the risk of proliferation is assumed, and it is not estimated in absolute terms. In the context of nuclear proliferation risk, the variables L, P, and C represent the following:

* L (likelihood): The probability that a State will choose to proliferate encompasses factors such as regional geopolitical tensions, national security concerns, internal dynamics, and other social and political factors that play a role in determining this possibility.
* P (probability of success): This variable represents the chance of a country successfully proliferating after it decides to do so. Factors like the availability of technology, materials and financial resources, technical expertise, and international pressure can affect this probability.
* C (consequences): Consequences are the potential impacts of nuclear proliferation. Their severity depends on the scale of the proliferation and the geopolitical context.

With the envisioned increase of nuclear energy and expansion of nuclear fuel cycles, a new design might incur in the risk of coming to maturity with no proven safeguards technology available in the short term and being expensive to safeguard. Therefore, designers should consider international safeguards when exploring fuel types, the fuel cycle needed, and the reactor and its systems as early in the design stage as possible. In some cases, the potential proliferation risk associated with a particular design might be so high that the vendor’s State might be unlikely to approve its export, potentially jeopardizing the business case for the entire endeavour.

From the designer’s perspective, a key risk lies in the potential need for costly engineering design modifications to meet safeguards obligations. This is because, unlike safety requirements (which are dealt with by design) or the security requirements that are discussed with the operators in which designers can be involved, safeguards approaches are designed by the safeguards inspectorate, which is usually receiving information about the design when it has already been finalized. At that stage, any design modification needed to accommodate the safeguards approach has the potential to become an important source of cost and project delays. From the perspective of the designer, the concept of risk must be translated from a global/ political sphere to a project-based approach. The designer can only control their individual designs and consider where and how it may be deployed by an owner/ operator (i.e., the end user). If the problem is addressed at the time of construction/ operation, it is too late and retrofitting to accommodate IAEA safeguards may be needed. So, although the burdens will fall on the owner/ operator, this will reflect back on the design such that there is a “transfer of risk” back to the designer, which is in a position to do something before it reaches the stage where retrofitting is needed.

#### Proliferation risk, proliferation resistance and. safeguardability

When dealing with special fissionable material, there will always be a degree of proliferation risk. Proliferation in nuclear energy systems can never be eliminated, and any nuclear technology can be potentially misused. Proliferation resistance is a term used to denote the degree to which a specific nuclear facility contributes to proliferation risk.

Proliferation resistance is defined by the IAEA as “characteristic of a nuclear energy system that impedes the diversion or undeclared production of nuclear material, or misuse of technology, by States to acquire nuclear weapons or other explosive devices. The degree of proliferation resistance results from a combination of, inter alia, technical design features, operational modalities, institutional arrangements, and safeguards measures” [10]. The intrinsic features, design characteristics, features to prevent diversion of material and facilitate continuity of knowledge of nuclear energy systems are developed by the designer. Intrinsic features coupled with the extrinsic measures (i.e., the State’s institutional arrangements for safeguards) impact the level of proliferation resistance of a reactor. Extrinsic measures will continue to be essential to control and verify the information provided by the State under its safeguards obligation independently of the proliferation resistance level of a nuclear reactor.

For new fuel cycles and reactor technologies, designers can reduce the proliferation risks by incorporating design features that will facilitate the application of IAEA safeguards such as Design Information Verification, Nuclear Material Accountancy and Containment, and Surveillance. New designs can be evaluated in terms of its “safeguardability,” whose commonly accepted definition is “the ease with which a system can be effectively and efficiently put under international safeguards. Safeguardability is a property of the nuclear system and is estimated for targets on the basis of characteristics related to the involved nuclear material, process implementation, and facility design” [11]. Although robust safeguards cannot eliminate proliferation risk entirely, they increase the ability of the IAEA to detect of any potential diversion attempts. However, if a reactor design requires extensive safeguards measures, it might become very resource-intensive on the safeguards inspectorate and potentially burdensome to the operator.

Safeguards by design (SBD) and safeguardability are closely related. A designer does not “design” safeguards into the reactor, but rather designs the reactor (in collaboration with the IAEA or some other safeguards guidance) such that the IAEA can readily apply safeguards once the reactor is purchased, constructed, and deployed by the owner/ operator. SBD denotes a process whereby the designer takes into consideration the future application of IAEA safeguards to their specific design. The end design will therefore have a degree of “safeguardability” meaning the ease or difficulty that the IAEA will have in designing and implementing a safeguards approach to the specific reactor.

Reactor designers require design guidance that is clearly defined. However, there is currently little or no design guidance for safeguards, and this lack of clarity makes it challenging for designers to consider the need for safeguards and how it should be integrated into their processes. Additionally, designers point out that they respond to shareholders and that, without clear financial benefits and procedures, embracing safeguards by design can be a complex task. Furthermore, solutions that facilitate safeguardability have to be considered along with safety and security so that neither are adversely affected and that an acceptable balance solution can be found. [2-4, 12].

#### The engineering design process to minimize risks as applied to safeguards[[3]](#footnote-4)

During the engineering design process, there are three basic methods to approach to mitigating risks:

1. Engineered solution. Eliminate the unwanted event via the basic design. For example, if an equipment or piping failure will result in loss of coolant or another unwanted event, redesign the system to eliminate that possibility entirely.
2. Mitigation. If the unwanted event cannot be eliminated, then apply design solutions that can mitigate the problem. For example, add or modify other systems that will intervene to mitigate the effects of a piping failure and loss of coolant.
3. Administrative controls. If the costs associated with engineering solutions or mitigation are too high, then apply administrative controls to mitigate them. For example, implement access controls, procedures, and/or operator actions that will mitigate the unwanted event.

Parallels to this thinking can be applied to minimizing risks as applied to safeguards:

1. Engineered solution. Eliminate potential proliferation pathways by designing the fuel, the reactor, and its systems. For example, by consolidating multiple fuel paths, some special fissionable material diversion paths can be eliminated, and the need for verification may be reduced, thereby minimizing the need for the installation of IAEA equipment and other verification activities.
2. Mitigation - If the potential proliferation pathways cannot be eliminated, then design the system to make the proliferation path more difficult to be pursued. For example, the fuel paths can be designed to make diversion more difficult by increasing the proliferation path technical difficulty or by reducing access points and making such attempts readily detectable.
3. Administrative controls. IAEA Safeguards are extrinsic proliferation resistance measures. If the potential proliferation pathways cannot be eliminated, design the system with a high degree of safeguardability so that IAEA equipment and verification activities can be easily accommodated/ facilitated.

In these examples, applied to safeguards, engineered solutions, and mitigation features are considered intrinsic features of the system. The administrative controls are considered extrinsic features, which are implemented by the IAEA as part of international safeguards and can be made more efficient via a safeguards-by-design exercise. Regardless of the solutions being implemented, the IAEA will reserve the right to apply a safeguards approach, including equipment and verification activities, based on the level of risk that it deems appropriate based on the facility type and the acquisition pathways determined for the State.

## INTERFACES BETWEEN THE DIFFERENT DISCIPLINES

In this section, the risks for a select set of topics will be analyzed from the perspective of the interfaces between each of the 2Ss - safety and security, safety and safeguards, and security and safeguards. It is important to note that these topics were chosen for illustrative purposes as other topics exist and should be considered. Additionally, the discussions only represent a portion of the considerations that are needed for each topic and are provided to illustrate the risk-based thinking necessary from a designer’s perspective. Specifically, the risk for the designers is that all relevant safety, security, and safeguards measures are not adequately considered and integrated. This integration should ensure compliance with regulatory requirements and international obligations and address potential vulnerabilities that may arise at the intersection of these interfaces. This risk includes that the design may require costly re-engineering and result in project delays. In this paper, “risk for the designer” is used as a qualitative term and future efforts may be needed to better quantify this concept. These topics are also used in the DRAFT Technical Service Review Guidelines Reference document for the IAEA for the review of safety, security, and safeguards Interfaces currently under development by the IAEA [14].

### Novel Siting and Deployment Scenarios

*Risks from a Safety and Security Perspective*

Some novel siting and deployment scenarios envision that advanced reactors may be deployed in remote areas with limited access. This can result in access delays of mobilizing response forces reaching the site in the time frame required to respond to the threat. This delay could be due to factors like distance, limited infrastructure, or harsh weather conditions. From a physical protection standpoint, site selection should also consider whether the landscape where the advanced reactor will be deployed offers an advantage or disadvantage in relation to the security system and access to the response force.

Conversely, advanced reactor may be deployed closer to populated areas/ urban centers than is the case for conventional LWRs due to reduced emergency protection zones. Deploying reactors near populated areas poses an additional challenge as well. Urban areas can evolve over time, potentially impacting previously established security measures. This would demand the revision of the threat assessment and the evacuation routes during the advanced reactor deployment.

Therefore, the risk to the designers is that added the security costs will increase the deployment costs of the reactor, which will be a burden to the operator. As such, the designers should anticipate various siting and deployment scenarios and engineer systems such that the available security systems and response forces can adequately protect the safety systems both effectively and economically. For example, given resilience to external events such as flooding and severe weather, the optimal combination of inherent system features, mitigation strategies, and administrative controls should be determined to minimize any associated security risks such as communications being disabled, or response forces being delayed due to lack of access to the location.

*Risks from a Safety and Safeguards Perspective*

Accommodations for safeguards inspection access and verification should be considered if the deployment strategy includes remote locations. The IAEA will likely require access and verification activities whenever fresh fuel is received and when reactors are refueled. This could be achieved via remote verification or may require inspectors to access the site and reactor facility. The IAEA will also require the ability to independently verify that the integrity and location of any fresh and spent fuel storage be confirmed. Adequate resources must be provided so that the IAEA can carry out its mission. The transmission of monitoring data from the reactor to the IAEA (off site) may have both a positive and negative impact on operations. The release of operational data may reduce the need for on-site inspections, but it may also create concerns for the operator.

Therefore, the risk to the designer is that the novel siting and deployment will result in safeguards being difficult to apply, which may result in additional time for the IAEA to develop and install the required specialized equipment. To facilitate IAEA verification, the designer should consider aspects of different siting and deployment scenarios that could impede IAEA access and design in solutions that will allow ample time, technology, and access for the IAEA to verify refueling activities at the site and allow visual access to strategic facility areas where fuel is stored. The application of safeguards is considered an extrinsic control.

*Risks from a Security and Safeguards Perspective*

If the reactor is placed in a remote location that is difficult to access, a robust communication infrastructure may be necessary. This infrastructure might require new systems, protocols, or upgrades to existing ones to ensure remote data transmission for safeguards verification. A thorough analysis should identify any potential disruptions, and appropriate design measures should be taken to ensure that the appropriate data can be provided to the IAEA to facilitate their independent verification activities.

Therefore, the risk to the designer is the burden of additional inspector verification due to inability to receive authenticated remote data from the operator may reflect poorly on the design or required costly retrofits for siting in remote locations to address this specific interface issue. As advanced reactors are expected to be deployed under a variety of settings worldwide under a more streamlined supply chain and factory fabrication model, the reactor design should include systems with the necessary communication capability, specify what local infrastructure must exist to support that capability, and consider what data will be needed by the IAEA to minimize the impact on plant security while meeting all legal reporting and verification obligations.

### Reactor Design and Passive Safety Systems

*Risks from a Safety and Security Perspective*

Advanced reactors often utilize passive safety features for inherent accident protection; however, passive safety systems may introduce different security vulnerabilities. These vulnerabilities may need additional security measures, which can burden plant operations. To mitigate this risk, designers should incorporate measures that address credible threats from malicious actors, including insiders, who could compromise plant safety.

Therefore, the risk to the designer is not considering how passive safety systems may introduce new/ different security vulnerabilities that may increase the security measures needed and result in unanticipated costs to the operator. Therefore, the drive to reduce the intrinsic safety risk via the utilization of passive safety systems should be balanced with the impact of the security systems required in the facility.

*Risks from a Safety and Safeguards Perspective*

The passive safety systems may obviate the need for personnel access for operations or maintenance during the lifetime of the reactor. Therefore, major areas of the plant might be restricted or otherwise inaccessible. As such, designs could incorporate inherent features that will facilitate IAEA verification of locations that are hard to access or mitigation strategies that allow for that IAEA to maintain continuity of knowledge throughout the lifecycle of the plant (i.e., construction, operation, decommissioning, and the termination of safeguards).

Therefore, the risk to the designer is that it will be difficult for the IAEA to maintain continuity of knowledge of nuclear material; IAEA might require additional verification activities and equipment that could become burdensome to the operator and to plant operations.

*Risks from a Security and Safeguards Perspective*

When considering what measures must be applied to address any new passive safety systems, the designer should recognize that the IAEA will require independent verification of the nuclear material as well as the design of the plant and its systems. Therefore, similar to the safety and safeguards interface, the design of the security system must not prevent the IAEA from carrying out its verification activities, even for areas that where plant personnel are normally not required to enter or not permitted to enter for security reasons. If sections of the plant are never to be accessed during operation, one possible mitigation strategy would be to allow additional IAEA verification during the construction phase and include provisions for the IAEA to periodically verify that no changes have been made during any operation or maintenance of the plant.

Therefore, the risk to the designer is that, because of certain security restrictions, the IAEA will not be able to access areas of the plant and will require additional verification activities or will install equipment that may place additional burdens on the operator and plant operations.

### Irradiated Fuel Storage Systems

*Risks from a Safety and Security Perspective*

Irradiated fuel storage systems are necessary at all currently operating nuclear power plants to store recently discharged fuel from the reactor. This creates a security risk because adversaries could steal material from the spent fuel pool or sabotage safety systems, leading to a radioactive release. Dry cask storage enhances security by separating fuel assemblies, reducing the amount of accessible material, and providing an additional layer of protection. However, freshly discharged fuel generates significant decay heat, requiring it to be stored in a spent fuel pool for a cooling period before being transferred to dry casks. Some advanced reactor designs may have factory-sealed cores or replaceable cores that would be shipped back to the factory for disposal. Others allow for online refueling or sealed core storage on site. Therefore, the design of new kinds of irradiated fuel storage systems must consider the physical protection systems required to protect it from attacks from outside, as well as from an insider, as they have different means of disabling or tampering with safety systems, such as water pumps, cooling, or heat exchangers, in the short and/or long term.

Therefore, the risk to the designers is that irradiated fuel storage systems employed for safety and economic reasons introduce security vulnerabilities that will require additional response forces or costly security equipment or even a redesign of the storage system.

*Risks from a Safety and Safeguards Perspective*

Novel fuel cycles will have new types and forms of fuel that can challenge safeguards inspections if they are in a bulk or liquid form. The IAEA may require measurements of irradiated fuel materials and verification of containment and surveillance methods such as seals and cameras to ensure continuity of knowledge. When storage systems for these novel irradiated fuel forms are being designed, the IAEA’s ability to apply safeguards measures and technologies to independently verify the quantity and type of nuclear material at all times should be considered along with safety and economics. Because simple item accounting as is used in current LWR and heavy water reactor designs may not be possible, the IAEA may require more robust measurement, containment, and surveillance features.

The risk to the designers is to ignore the safeguardability of new kinds of irradiated fuel storage systems, such as visual inspection compatibility with irradiated fuel, which could result in increased IAEA verification activities and/or installed equipment that my become burdensome to the operator and to operations.

*Risks from a Security and Safeguards Perspective*

After verifying the declaration of data, IAEA inspectors utilize containment and surveillance measures for the spent fuel to ensure the continuity of knowledge. Spent fuel pools are also subject to verification through a variety of non-destructive analysis measurements by safeguards inspectors. While adversaries could acquire nuclear material from a spent fuel pool (diversion), the high radioactivity makes the fuel itself a significant deterrent. An attack aiming to release radioactive material becomes the most likely threat scenario. Therefore, for diversion of nuclear material, containment and surveillance measures would have a natural synergy by serving the dual purposes of deterring unauthorized access and facilitating safeguards verification.

The risk to the designers is that by not considering how IAEA will apply safeguards, they may miss the opportunity to increase both facility security and economics because certain security features (such as the application of tamper-indicating seals) may serve both safeguards and security purposes.

### I&C system design

*Risks from a Safety and Security Perspective*

Instrumentation and control (I&C) systems should be designed bearing in mind that security, whether cyber or physical, should protect nuclear power plants from insider and outside attacks while not hindering the safety operations. Measures include protection of software from cyberattacks, physical aspects of the hardware, and data transmission.

The risk to the designer is that sabotage in the form of unauthorized system access resulting in off-normal operations or gaining access to plant systems for the purpose of stealing data or disrupting operations could occur if the security of hardware and software interfaces are not taken into consideration. Enhancement of computer system security could result in additional security costs and changes to plant operations, both of which could have an economic impact.

*Risks from a Safety and Safeguards Perspective*

As plant digital systems increase in scope and complexity, the storage and transmission of data will likely increase. This could have positive implications for safeguards, especially for some advanced reactor designs that may have complex fuel handling systems (such as continuous on-line fueling) that inherently makes material accounting more difficult and therefore challenging to apply safeguards. The IAEA may have to deploy equipment that is either not tested or that does not exist at the moment and must be developed. Considering the deployment of advanced reactors over the next 5-10 years and the time that may take to develop, test, and approve safeguards equipment, working with the IAEA at that stage of the design process will mitigate the issue by alerting it of future safeguards equipment needs and providing time to think through possible safeguards approaches. Traditional safeguards approaches and measurements may prove costly and time-consuming, and therefore the IAEA may look to supplementary verification methods, such as analysis of operational or process data. Such data may provide confirmation to the IAEA that their installed equipment is operating properly and thus additional confidence that no diversion or misuse has occurred. Thus, the digitization of plant systems could provide unexpected benefits for safeguards.

The risk to the designer is that opportunities to apply efficiencies and economics can be missed if safeguards that include the use of digitized plant data is not considered.

*Risks from a Security and Safeguards Perspective*

All three disciplines involved with nuclear materials need access to nuclear material information. Although sharing this information can improve efficiency, some safeguards and security details will be restricted. The increased digitization of the plant I&C systems provides opportunities to have access to more data, and the data could be shared with the IAEA; however, any data received by the IAEA must be authenticated for both on-site and remotely transmitted data. Remote data transmission could reduce overall safeguards costs and could allow the IAEA to verify compliance with safeguards obligations and ensure that nuclear material is not diverted. However, remotely transmitted may contain sensitive information that is relevant to both security and safeguards. Cybersecurity and physical protection measures can improve both security and safeguards because they can both rely on the same basic infrastructure. However, the independence of the IAEA and its verification activities must be ensured at all times through the lifecycle of the facility. For example, cyber security of I&C systems should not unduly impede or prevent the IAEA from receiving data signals that have been identified as part of the facilities safeguards systems.

The risk to the designer is that the cost of systems required for the IAEA to access the needed data will increase, thereby increasing costs and burdens on the operator and operations if the interface between physical protection, cyber security, and safeguards is not considered.

## Does risk have meaning for safeguards by design?

For safeguards the risk of proliferation is formally determined by the IAEA and drives their safeguards approaches for each facility, taking into account the Acquisition Path Analysis for each country. Proliferation risk can also be determined by a country – e.g., countries will consider proliferation risk before they authorize export licenses for nuclear technology. For a designer, once the basic design features of their reactor have been chosen (i.e., burner vs. breeder, U enrichment, thermal vs. fast, fuel form, quantity, physical form, etc.) this determines tits intrinsic potential for proliferation. And although they can make changes to their basic reactor features, most of their efforts will likely be directed towards optimization of their design from a safety and economic perspective. And this is the point in the design process where safeguards by design plays a key role.

The safeguards part of the 3S focuses on applying IAEA safeguards to a nuclear facility. Proliferation resistance is defined as the combination of intrinsic and extrinsic measures, where the extrinsic measures include IAEA safeguards. Extrinsic measures will always be needed because no nuclear reactor/ fuel cycle is “proliferation proof.” Therefore, this paper is trying to express risk in terms that the designer could both understand and effectively address. If they consider what extrinsic measures (IAEA safeguards) would be applied, they can design their systems to minimize burdens on the operator (and the IAEA) and thus make safeguards easier to apply (safeguardability). This reduces the “risk” to the designer that their design will be difficult to safeguard, and therefore not attractive to potential owner/ operators.

So, although risk is used in terminology such as “proliferation risk” that is too broad of a topic and not entirely within the designer’s control. Proliferation can be used more as a political term than a technical term, so although preventing the proliferation of nuclear weapons is the ultimate goal of safeguards, proliferation risk may not be able to be quantified in terms that is actionable for a designer. Once the basic design features of the reactor are determined, their focus should be on consideration of IAEA safeguards as part of their optimization process for safety and economics (as well as security and other factors).

Designers of novel nuclear energy systems should consider safeguards (i.e., SBD) early in the design process to identify the stakeholders and the challenges, constraints, and mitigation strategies to ensure that their nuclear facility has a high degree of safeguardability. The designer’s risk is in developing a design that hinders the implementation of effective safeguards measures. Impediments could include limited accessibility for inspectors, a lack of clear material flow paths, or a design that makes it difficult to monitor the movement of nuclear material. Such shortcomings can make it challenging for the IAEA to verify the facility's compliance with safeguards agreements.

Safeguards by design improves the safeguardability of the reactor, promotes efficient and effective safeguards throughout a system's life cycle, reduces burdens on owner/operators in the long term, and ensures compliance with national and international obligations. The definition of risk for the different fields may never be unified based on the different mathematical concepts that are behind the calculation and the assessment of what risk is considered for each field. While for safety, the risks are well understood and can be estimated based on experience and methodologies; however, security and safeguards have different, evolving profiles of threat and consequently of risk.

## CONCLUSION

The term “risk” has a different meaning within nuclear safety, security, and safeguards. In safety, risk is inherent in the design and is mitigated through safety margins, fuel design, and overall design principles. The designer’s risk lies solely in miscalculating potential hazards, which then translates to inaccurate risk assessment.

Security risk focuses more on threats and prevention, detection, and the response to them. Quantifying probabilities is more challenging in security than in safety. The terminology often leans toward “likelihood of success,” which can be an analogue of probability but is not mathematically defined as it is in safety. The risk that security poses for the designer is that security measures can become burdensome and expensive later on if security considerations are neglected during the design phase.

In safeguards, proliferation risk refers to the potential for the diversion of nuclear material or misuse of the reactor for unauthorized purposes, and, like security, it is influenced by human actions and intentions. Probabilities play a role in assessing the likelihood of diversion attempts if they take into account the entire fuel cycle infrastructure within a State and the effectiveness of safeguards measures.

The degree of the proliferation risk is inherent for different reactor designs and fuel cycles (intrinsic features), and this is mitigated by the application of IAEA safeguards (extrinsic measures). By considering safeguards early in the design stage, designers can create an energy system that facilitates verification by the IAEA. This not only fulfils regulatory requirements, but also offers several benefits. A design with a high degree of safeguardability can attract interest from countries seeking to add nuclear energy because they know that the design could facilitate international safeguards obligations. Additionally, it simplifies the work for both State authorities and the IAEA, and it enables better collaboration and potentially faster regulatory and license approval.

Therefore, the risk to the designer” approach offers a way to address the interfaces of the three 2S couplets and may be the only way to meaningfully quantify risk when the interfaces between the three disciplines are being discussed.

References

1. STEIN, M., MORICHI, M., VAN DEN DURPEL, L., SAFEGUARDS BY DESIGN – AN INDUSTRIAL VIEW, INMM 51st Annual Meeting, July (2010)
2. INTERNATIONAL ATOMIC ENERGY AGENCY, Safeguards by design, https://www.iaea.org/topics/assistance-for-states/safeguards-by-design
3. INTERNATIONAL ATOMIC INTERNATIONAL ATOMIC ENERGY AGENCY, International Safeguards in Nuclear Facility Design and Construction, IAEA Nuclear Energy Series No. NP-T-2.8, IAEA, Vienna (2013)
4. ENERGY AGENCY, International Safeguards in the Design of Nuclear Reactors, IAEA Nuclear Energy Series No. NP-T-2.9, IAEA, Vienna (2014)
5. INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Nuclear Safety and Security Glossary, (2022).
6. KAPLAN, S., GARRICK J., On the Quantitative Definition of Risk, Risk Analysis, Vol. I, No. I, (1981)
7. INSTITUTE of NUCLEAR MATERIALS MANAGEMENT, Workshop on The Quantification of The Likelihood of Attack, (2021).
8. INTERNATIONAL ATOMIC ENERGY AGENCY, IAEA Safeguards Glossary, (2022)
9. NATIONAL RESEARCH COUNCIL, Improving the Assessment of the Proliferation Risk of Nuclear Fuel Cycles, The National Academies Press, Washington, DC, 2013. https://doi.org/10.17226/1833
10. INTERNATIONAL ATOMIC ENERGY AGENCY, Proliferation resistance fundamentals for future energy systems, IAEA-STR-332, (2002)
11. GENERATION IV, International Forum Proliferation Resistance & Physical Protection Working Group, Evaluation Methodology for Proliferation Resistance and Physical Protection of Generation IV Nuclear Energy Systems, rev. 6, GIF/PRPPWG/2011/003, GIF, 2011. https://www.gen-4.org/gif/upload/docs/application/pdf/2013-09/gif\_prppem\_rev6\_final.pdf
12. IAEA, Facility Design and Plant Operation Features that Facilitate the Implementation of IAEA Safeguards, SGCP-CCA, STR- 360, (2009)
13. UNITED STATES, DEPARTMENT OF LABOR, Occupational Safety and Health Administration, Recommended Practices for Safety and Health Programs, https://www.osha.gov/safety-management/hazard-prevention
14. INTERNATIONAL ATOMIC ENERGY AGENCY, TSR-DS Review Guidelines REFERENCE DOCUMENT FOR THE IAEA REVIEW OF SAFETY, SECURITY AND SAFEGUARDS INTERFACES, (in preparation).

1. The term “international safeguards” refers to the application of IAEA safeguards under agreements such as a Comprehensive Safeguards Agreement. In this paper, the term “safeguards” will be used to refer to international safeguards. [↑](#footnote-ref-2)
2. Note that the definition includes the term “risk,” but here it is used to indicate that the potential risk to the proliferator that they will be caught or their activities detected, thereby thwarting their efforts to divert nuclear material or misuse the nuclear facility. [↑](#footnote-ref-3)
3. U.S. Department of Labor, Occupational Safety and Health Administration, Recommended Practices for Safety and Health Programs, <https://www.osha.gov/safety-management/hazard-prevention> [13] [↑](#footnote-ref-4)