# SECURITY BY DESIGN: UNDERSTANDING

# HOW TO APPLY IT TO SMR, ILLUSTRATED

# BY THE HISTORIC EXAMPLE OF THE

# OPÉRA GARNIER (PARIS)

Mélissa KOPPE

Ministry of Ecological Transition and Territorial Cohesion

French Nuclear Security Authority

Paris, France

melissa.koppe@developpement-durable.gouv.fr

Thomas LANGUIN

Ministry of Ecological Transition and Territorial Cohesion

French Nuclear Security Authority

Paris, France

Justine LAUNAY

Ministry of Ecological Transition and Territorial Cohesion

French Nuclear Security Authority

Paris, France

Antoine MALABIRADE

Ministry of Ecological Transition and Territorial Cohesion

French Nuclear Security Authority

Paris, France

**Abstract**

Security by design is of paramount importance for all nuclear facilities, but even more so for SMRs. In fact, preliminary studies show that nuclear security could be one of the main operating costs of SMRs.

Security by design offers a unique opportunity to design reactors that are more cost-effective and competitive.

This paper will explain, based on the French experience, why nuclear security should be better taken into account from the beginning. While it is not possible to share confidential information in an international conference, the historical example of the Opéra Garnier, one of the most famous buildings in Paris, will be used to illustrate the concept of security by design.

Who remembers today that security was one of the concerns of this building? In fact, its construction was decided after a bomb attack against Napoleon by Italian terrorists in front of the Paris Opera.

The principles applied to the Opéra Garnier are still relevant for SMRs, including a global approach to the protection of the facility and the transportation of nuclear materials, protection against stand-off attacks, and optimization of access to reduce the insider threat.

## INTRODUCTION

Let's step back in time to January 14, 1858, when Napoleon III fell victim to a bomb attack orchestrated by Italian terrorists outside the Paris Opera House. This act was a retaliatory measure against French interventionism in their homeland. In response to this grave incident, Napoleon III embarked on the construction of a new opera house that would not only exude prestige but also prioritizes security. Thus, one of Paris's most iconic landmarks was born: the Opéra Garnier. Yet, in the annals of history, how many recall that security stood as a primary objective in its conception? It becomes evident that security considerations were woven into the fabric of the opera house's design from its very inception.

During the era of Paris's extensive urban transformation under Haussmann's influence, the city resembled a colossal construction site. Consequently, a strategic decision was made to establish a direct thoroughfare between the Emperor's residence and the Opéra Garnier, now recognized as the Avenue de l'Opéra. This thoroughfare served a dual purpose: to minimize travel time between the Louvre Palace and the opera house and to accommodate effective security measures during transit. This example underscores the importance of integrating security considerations into the planning and design phases. In the context of nuclear facilities, a similar approach would involve conducting a comprehensive evaluation of transportation logistics for nuclear materials and radioactive substances when siting and designing a new facility.

Considering the type of attack the Emperor faced, a decision was made to construct a secure and exclusive passage to the opera for his use. The "Rotonde de l'Empereur" was devised to shield against external attacks, providing a covered pathway for the Emperor's carriage. This strategic arrangement finds resonance in the selection of an underground design for certain Small Modular Reactors (SMRs), which inherently fortifies against off-site assaults.

Another compelling demonstration of "security by design" emerges from the opera's layout. During its design phase, a direct and unobstructed route between the "Rotonde de l'Empereur" and the Emperor's box was established. Unlike scenarios where the Emperor would enter through the main opera entrance, this arrangement minimizes interactions between the Emperor and unauthorized individuals, avoiding the need for additional security measures at the main entrance that could hinder opera admissions. A pertinent analogy in the nuclear domain could be observed in access restrictions to safeguarded areas housing critical targets, akin to vital areas, in order to limit insider threat.

An illustrative case in France involves relocating the consignment room outside the main control room building to extricate it from a vital area. Typically, workers accessing consignment rooms do not require entry into vital areas.

These examples underscore how intrinsic or purpose-built features, integrated at the earliest stages of design, fortify building security against specific threats, obviating the necessity for later additions of dedicated physical protection systems

## SECURITY BY DESIGN

In France, the current approach to security by design encompasses two main components:

 1. Intrinsically Secured Design: This involves integrating inherent features into the installation that serve to minimize the number of targets, enhance nuclear security, and better mitigate potential vulnerabilities. By embedding security measures directly into the design, the aim is to create a foundation that inherently bolsters protection.

 2. Early Identification of Physical Protection Requirements: This aspect involves proactively identifying and addressing vulnerabilities of the installation through physical protection measures from the outset. By recognizing potential weaknesses early on, steps can be taken to fortify the facility against threats.

Moreover, the concept of security by design facilitates the anticipation of future changes in the threat landscape over the lifespan of the installation. This approach aims to develop a design that accommodates future enhancements and adaptations in physical protection systems to address evolving threats effectively. Thus, security by design not only enhances immediate security measures but also ensures flexibility and adaptability to meet future challenges.

### Intrinsically Secured Design

As mentioned in Nuclear Security Fundamentals IAEA Nuclear Security Series No. 20 (NSS20), nuclear security issues are related “to the prevention and detection of, and response to theft, sabotage, unauthorized access and illegal transfer or other malicious acts involving nuclear material and other radioactive substances”. Third level paper heading.

Hence, security by design encompasses a broad spectrum of risks that must be addressed during the design phase. Typically, targets are identified based on their potential consequences or the nature of materials susceptible to theft. Therefore, an intrinsically secured design approach aims to minimize or ideally eliminate targets within a nuclear installation and complicate the modus operandi for potential adversaries.

The primary objective of the designer should be the reduction of targets or their vulnerability to attacks, and various strategies can be employed to achieve this goal. Here are several approaches:

1. Restricting the category of nuclear materials utilized in the installation, particularly those posing a high risk of theft.
2. Enhancing fuel assembly design and nuclear material management to diminish vulnerability to theft.
3. Selecting or optimizing technologies that are less susceptible to sabotage or entail lower consequences in case of an incident. This could involve using materials with greater resistance to specific risks such as fire or corrosion.
4. Decreasing the potential release of radioactive substances within the installation. For example, small modular reactors (SMRs) are comprised of modules with lower power outputs compared to traditional nuclear power plants, thereby reducing potential consequences in the event of an accident or malicious act.
5. Integrating assessments of radioactive substance transportation issues into the siting and design considerations of a nuclear facility. This may include adapting access points to facilitate rapid entry and safeguarding parking areas against potential attacks, akin to the concept of the "Rotonde de l'Empereur."

By incorporating these strategies into the design process, security measures can be effectively integrated, mitigating risks and enhancing the overall security posture of the facility.

Certainly, by design, certain arrangements can effectively reduce the number of targets within a facility, often in response to operational needs or safety requirements. Small Modular Reactors (SMRs) serve as a prime example of such intrinsic dispositions. For instance, some SMR designs mitigate the risk of a Loss of Coolant Accident (LOCA) by limiting or eliminating primary loops, or they reduce the risk of criticality by minimizing reliance on borated water. These innovations inherently diminish the number of potential targets, thereby enhancing security.

Moreover, intrinsic security can encompass considerations of attack complexity. Increased complexity significantly raises the difficulty of executing an attack, thereby deterring both outsiders and insiders from acting. This complexity can be achieved through appropriate organizational and physical provisions. While physical provisions here refer not to dedicated physical protection measures, but rather responses to operational or safety needs. Concepts such as defence in depth and redundancy can distribute targets across multiple locations that are not interconnected, thus complicating attack plans and prolonging the time needed to achieve objectives. Such a layout can also enhance safety measures, particularly concerning fire and flooding risk requirements.

Organizational aspects can also serve as a deterrent to adversaries. For instance, optimizing access to specific areas of the installation can be achieved through thoughtful facility operation and activity organization. Designers can minimize the need for access to vital areas by segregating vital targets from other equipment, especially those requiring intensive on-site operation or maintenance. This strategic approach not only enhances security but also streamlines facility operations.

### Early integration of nuclear security requirements

For the remaining targets within a nuclear facility, nuclear security systems become imperative. Early integration of such provisions is essential to avoid being confronted with an irreversible situation. If relevant and adapted security systems are not integrated during the design phase, the security features may not adequately address threats or additional features may disrupt plant operation and prove costly.

At times, security systems may derive from design orientations initially intended for other purposes. For instance, some SMR designs incorporate half-buried or underground structures to mitigate specific natural risks. However, such arrangements also offer effective protection against stand-off attacks and specific malicious acts. Early consideration of security needs may validate the utility of such synergistic solutions and aid in optimizing benefits for both purposes.

Regarding the insider threat, controlling access to certain zones of the installation is crucial. Access control features require sufficient space and must be factored into building design early on, especially for compact layouts. Optimization of layout can identify synergies between access control zones, accountability and control zones, radiation protection zones, etc. Aligning operating needs (such as the number of people accessing an area and frequency) with security requirements can help optimize all constraints.

National legislative and regulatory frameworks, typically based on IAEA nuclear security series documents, mandate various security areas and systems. However, security measures can be costly if not anticipated and well-designed. Therefore, designers must possess a thorough understanding of the framework in which the reactor may be constructed. This foresight is crucial for navigating the national authorization process, which invariably includes security expectations, while minimizing the need for additional physical protection features to comply with national requirements.

For reactors like SMRs, which aim to offer an affordable alternative for nuclear power generation compared to traditional plants, maintaining a reliable economic model is paramount, making appropriate design imperative.

Furthermore, insider threat is a genuine concern. Insiders, leveraging their access, authority, and knowledge of the facility, pose a significant risk. Integrating the internal threat from the design stage is all the more important given that the start-up culture is based on information sharing and cross-functional working with all core businesses. The various people involved in the project need to be made aware of the internal threat, to ensure that sensitive documents produced by the designer are compartmentalised and that access is restricted. This is not an obvious issue for designers, who are not familiar with nuclear security and who have to adapt their ways of working to combat the risk of an insider threat. Designers should therefore also address insider threat early in the process, such as by implementing vetting procedures.

Ultimately, a well-integrated security design reduces constraints on other activities and staff, making security more acceptable and understandable. This fosters a positive security culture wherein security measures are seamlessly integrated into daily operations, akin to how tourists experience the security measures at the Opéra Garnier.

Another critical aspect during design is safeguarding sensitive information. Nuclear facilities are complex entities, and malicious actors require detailed information about the facility's design to plan an attack. Protecting information is a potent barrier against such threats. However, achieving the right balance between transparency and confidentiality obligations is essential, as excessive disclosure can inadvertently aid adversaries. Therefore, designers must implement robust policies for protecting sensitive or confidential information early in the design phase.

### How to implement security by design efficiently?

Access to the Design Basis Threat (DBT), typically a national and confidential document, can pose a challenge for designers as it outlines the threat scenarios a facility must withstand. However, designers can leverage disclosed information, such as past terrorist attacks, to consider current threats. Certain design choices, like underground layouts, can effectively address a wide range of threats. Design should also allow for adaptation of security measures to the national context, accommodating potential enhancements to basic security measures.

In order to dispense with the need to communicate the DBT to designers, the Nuclear Security Department has developed a guide to nuclear security for SMRs, intended for project developers. This guide provides information on current French regulation and all the major components of nuclear security. In addition, to provide project developers with some kinds of threats they will have to cope with. Examples are cited in the guide based on existing terrorist attacks (not necessary in the nuclear field), with information available from open sources.

The following threats are given as examples in the guide: an airliner (see the attacks in the USA on September 11, 2001) or a drone, a truck heavily loaded with explosives (see Oklahoma City bombing in 1995), an attack by an armed commando (see Paris attacks in 2015), an insider threat scenario (action conducted or facilitated by personnel inside the facility or during transport), a cyber-attack.

As a result, these examples give designers a good idea of what they need to take into account to design the reactor. Details are provided in the guide to help designers move forward and optimise and strengthen their design by taking security into account at the early stage.

Furthermore, security of nuclear installations must be ensured throughout their entire lifecycle, requiring consideration of evolving legislative and regulatory frameworks and DBTs. Design should allow for future additional security systems to address such changes. SMRs present challenges due to their compact footprint, but the use of margins during design can account for factors like wear, aging, and evolving threat capabilities. The choice of security features should also consider the best available techniques and potential for upgrades over time.

Implementing efficient security by design may prompt revaluation of technology choices or installation layouts to achieve better security outcomes without compromising safety or operational capabilities. Design teams with cross-functional expertise covering safety, security, and operations can enhance security implementation through collective work and systems engineering best practices. Ensuring efficient safety-security interfaces is crucial, requiring safety experts to possess a security culture and vice versa.

Security by design also poses challenges for States. Legislative and regulatory frameworks should facilitate early involvement in new nuclear projects and allow regulators to assess new designs upfront. States should also evaluate their frameworks to ensure they are adaptable to new concepts introduced by SMRs. A performance-based approach may facilitate adaptation to various nuclear facilities, including new concepts, without overly specific requirements.

Ultimately, all nuclear facilities, including SMRs, should adhere to the same security goals, applying a graded approach to security. This ensures robust security measures are in place across the board, regardless of facility type or size.

## CONCLUSIONS AND PERSPECTIVES

Early integration of nuclear security considerations into the design of nuclear facilities can lead to significant benefits in terms of security and cost-effectiveness. Intrinsic solutions that create synergies with other concerns, particularly nuclear safety, can optimize security provisions and reduce overall costs. Therefore, security should be regarded as a fundamental aspect of any nuclear project, and nuclear designers should receive training in security considerations. Additionally, involving security experts in the early stages of design is essential.

For new concepts like SMRs, which must be cost-effective, these considerations are crucial to achieving comparable security goals to other reactor types while employing a graded approach. To adapt to varying design basis threats and evolving threats, SMRs should incorporate technologies less susceptible to malicious acts and designs that allow for easy upgrades.

Moreover, States should review their regulatory frameworks and regulations to ensure they can adapt to these new concepts. This proactive approach will facilitate the implementation of innovative security measures and ensure the continued safety and security of nuclear facilities.