FRENCH APPROACH OF SECURITY BY DESIGN: FROM THE OPÉRA GARNIER TO SMR

Thomas LANGUIN
Ministry for the Ecological and Solidary Transition, Department of Nuclear Security
French Nuclear Security Authority
Paris, France
Email: thomas.languin@developpement-durable.gouv.fr

Erik DUCOUSSO
Ministry for the Ecological and Solidary Transition, Department of Nuclear Security
French Nuclear Security Authority
Paris, France

Abstract

History is full of illustrations of the benefits of security by design, in particular what is sometimes called "intrinsic security". However, if we look at the current installed civil nuclear facility fleet, security was not one of the main concerns when these facilities were designed. Still, it is important to emphasize that security level of nuclear facilities increased significantly in the last couple of years under the impetus of national legislative and regulatory framework and the strengthening of the international framework. This increase is not an easy task. Working on existing installations can lead to either security features that will not cope the threat in the best possible manner or additional physical protection features that may impact the installation operation. In addition, the threat changes over time. Having rooms for implementation of new features needed to cope with new threats is required. But it is a real challenge when dealing with existing installations that did not take into consideration this issue during the design phase. Currently, new nuclear installations, based on already designed and built concepts, are being built or are in project to be built. In parallel, new types of nuclear facilities are under design (such as Small Modular Reactors - SMR, deep storage facilities, etc.), with already advanced design for some of them. The purpose of the paper is to draw attention to the fact that to be efficient during the entire life cycle of a nuclear installation, security aspects should be considered as early as possible during the design phase of the installation.

1. INTRODUCTION

As an introduction, why not going back in time? On 14 January 1858, Napoleon III was victim of a bomb-attacked in front of the Paris opera house by Italian terrorists, as a response to French interventionism in their country. After this attack, Napoleon III decided the building of a new opera house that would be more prestigious but as well better secured: one of the most famous building in Paris was born: the Opéra Garnier. Who remembers today that security was one of the main objective of this building? It clearly appears that security was considered as early as the design phase of the opera. The following three examples will be used as illustrations of the benefits of security by design, in particular what can be called "intrinsic security". To go further, these security principles will be transposed to nuclear facilities to illustrate the relevance and importance to consider security as early as possible.

At that time, Paris became a gigantic worksite (Haussman period building). Therefore, it was decided to build a direct link between the house of the Emperor and the Opéra Garnier, known today as the avenue de l'Opéra. This avenue has been designed with two purposes: to reduce as short as possible the travel time between the Emperor Palace (Louvre) to the Opéra and to be large enough to allow effective security measures during travel time. A possible transposition of this illustration of security concern to nuclear facility would be to ensure an integrated assessment of nuclear material and/or radioactive substance transport issues when considering the siting and design of a new facility.

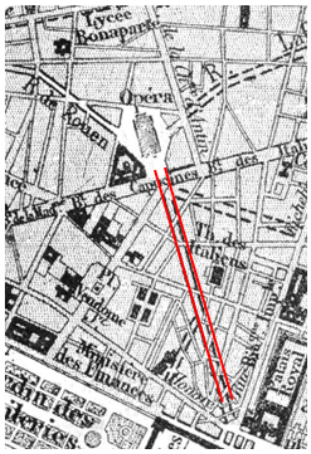

Fig. 1: Projected route of the Avenue de l'Opéra

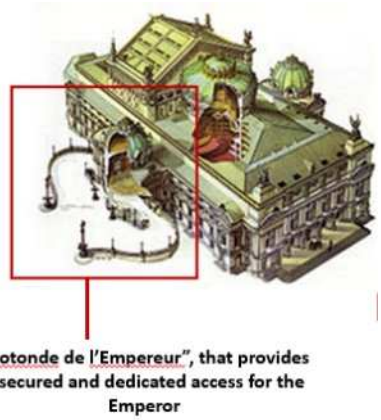

Fig. 2: Layout of the Rotonde de l'Empereur

Considering the nature of the attack whose the Emperor was victim, it was decided to build a secured and dedicated access to the opera for the Emperor. The "Rotonde de l'Empereur" prevents external bomb attack by providing a covered access for the coach. Such kind of disposition can be compared to the choice of an underground design for some SMR that provide protection against off-site attacks.

The last "security by design" illustration is related to the layout of the opera. A direct and straight access between the "Rotonde de l'Empereur" and the Emperor's loge has been decided during the design phase of the opera. Compare to the situation where the Emperor access would be through the main entrance of the opera, this disposition prevents interactions between the Emperor and people that have no reasons to enter into contact with the Emperor or additional access protection features at the main entrance that could impede the admission to the opera. A possible analogy with the nuclear field could be access restrictions to protected areas where targets can be found (such as vital areas). One concrete example implemented in France concerns the consignment room that has been moved away from the main control room building in order to be outside of a vital area. Indeed, most of the time the workers requiring information from the consignment rooms had no need to access to the vital area.

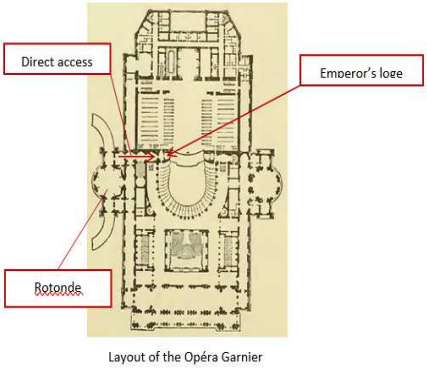

Fig. 3: Layout of the Opéra Garnier

These examples show how inherent or dedicated features integrated as early as possible during the design phase, contribute to enhance the security of the building regarding specific threats without the need to add dedicated physical protection systems afterward.

2. AN PPROACH OF SECURITY BY DESIGN

In France, the current approach of security by design can be resumed as a combination of:

— an intrinsically secured design, with inherent features of the installation that contribute to reduce the number of targets, to facilitate nuclear security and allow a better mitigation of the potential consequences of the remaining vulnerabilities and;

— an early identification of physical protection requirements, to cope with the vulnerabilities of the installation.

Security by design may also help to make easier the consideration of future changes in the threat during the lifetime of the installation. Therefore, it is expected to result in a design that provides rooms for future additional physical protection systems to cope with evolutions of the threat.

2.1. An intrinsically secured design

As mentioned in Nuclear Security Fundamentals IAEA Nuclear Security Series No. 20, 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*". Therefore, it covers a large range of risks to be addressed when considering security issues as part of the design. From these risks, targets are generally identified based on the potential consequences or on the nature of materials that can be stolen. Consequently, an intrinsically secured design approach aims at preventing or at least reducing as low as possible the number and sensibility of targets in a nuclear installation and also to make the *modus operandi* complex for the adversaries.

Reduction of targets or their sensibility to attacks should be the main goal of the designer and there are different approaches to achieve this goal. Here is a non-exhaustive list:

— By limiting the category of nuclear materials[1] used in the installation, in particular regarding the risk of theft;

— By optimizing fuel assembly design and the management of nuclear materials to reduce vulnerability to theft;

— By choosing or optimizing technologies that are less easy to sabotage, or with lower consequences. For example, using materials that are less vulnerable to specific risks (such as fire, corrosion, etc.)

— By reducing the potential source term of nuclear substances used or processed in the installation. For instance, small power reactors, such as research reactors, have a limited potential source term in case of an accident or a malicious act. By design SMR are composed of modules of around tens of megawatts. Therefore, potential consequences compared to traditional nuclear power plants should be lower depending on the number of modules constituting the SMR plant and the possibility to reach the integrity of all modules at the same time;

— By integrating assessment of transport of radioactive substances issues when considering the siting and the design of a nuclear facility. For example, access can be adapted to allow quick entry and protection of the parking area against attacks, similarly to the "rotonde de l'Empereur";

By design, in response to operating needs or safety requirements, some arrangements can lead to reduce the number of targets. SMR is a good example of such inherent dispositions: for instance, a few SMR designs reduce the risk of loss of coolant accident (LOCA) by limiting or removing primary loops, or regarding the risk

[1] The notion of nuclear material is defined as "*any material that is either special fissionable material or source material as defined in Article XX of the IAEA Statute*" in Nuclear Security Fundamentals IAEA Nuclear Security Series No. 20

of criticality some SMR are designed to rely less on borated water, etc.. Such kind of innovations contribute to reduce the number of targets.

Intrinsic security can also consider the complexity of an attack. Complexity can lower significantly the ease to achieve an attack, and deter outsiders or insiders to act. It can be achieved through adequate organizational and physical provisions. When referring to physical provisions, we don't mean here measures dedicated to physical protection but to answer operating or safety needs. Defence in depth and redundancy can lead to a high number of targets to be reached before an act of sabotage results in high or unacceptable consequences. If these targets are dispatched in several places that are not connected, then the attack plan may become complex to achieve and time needed may be significantly increased. Such layout can be beneficial also to safety, for example for fire and/or flooding risk requirements.

Organizational aspects could also be a mean to discourage adversaries. One example could be to optimize the number of people to access specific areas of the installation. To do that, designers should have a reflection on how to operate the facility and how to organize activities to ensure a relevant access policy to the different areas that composed the installation. For example, need to access to vital areas can be minimised by separating vital targets from other equipment, in particular those that need intensive on-site operation or maintenance.

2.2. Early identification of nuclear security requirements

For the remaining targets, nuclear security systems will be required. An early identification of such provisions is mandatory to prevent the risk of being faced with a fait accompli. Indeed, if the relevant and adapted security systems are not integrated as soon as the design phase of the installation, either the security features will not cope the threat in the best possible manner or additional features may impact plant operation and will be very costly.

Sometimes security systems result from design orientations that were initially considered for other purposes. For example, some SMR designs are half-buried or underground to cope with specific natural risks. But such arrangement provides a relevant and efficient protection against stand-off attacks and specific malicious acts. Early consideration of security may then confirm the interest of such synergetic solutions and help optimizing benefits for both purposes.

As far as the insider threat is concerned, there is a need to control the access of certain zones of the installation. Control of access features need sufficient space and, therefore must be considered early in the design of buildings, especially for compact layouts. The layout can be optimized to find synergies between access control zones, accountancy and control zones, radiation protection zones, etc. Considering as well operating needs (number of people accessing to the area, frequency, etc.) together with security needs may be helpful in order to optimizing all constraints.

The national legislative and regulatory framework (generally based on the IAEA nuclear security series documents) require different security areas along with security systems. However, security measures can be costly if they are not anticipated and well designed. Thus, it is important for designer to have a good knowledge and understanding of the framework where the reactor could be built. This anticipation is necessary in order to go through the national authorization process (which all include today security expectations) while limiting the need for additional physical protection features to comply with national requirements.

For reactors like SMR, which aim to provide an affordable alternative for nuclear power generation compared to traditional nuclear power plants, keeping a reliable economic model is of major importance, and thus appropriate design seems vital.

Another aspect to take into account during design is the protection of sensitive information.

As said before, nuclear facilities are complex objects and malicious actors will need a lot in information regarding the design of the facility to plan an attack. Protection of information may be therefore a very effective barrier.

Nevertheless, malicious actors can benefit, in particular on safety issues, from transparency and information required by legislative and regulatory obligations. Besides, designers, at the time of presenting their new projects may feel like communicating many details on the specificities of the design.

That is why designers should be aware that they product sensitive information. For example, explaining in details how major accidents could occur and how they prevented by safety measures could help a lot malicious actors to identify sabotage targets. Preventing the risk of leak of sensitive information relies on the implementation, as soon as possible as part of the design phase, of an appropriate and effective policy for the protection of sensitive or confidential information. This policy, in particular regarding information related to safety or operation, should be well defined and balanced with regard to transparency and information obligations, but still having in mind that threat to nuclear installations is credible.

On the other hand, gathering such information has no use without relevant technical skills to analyse them. The knowledge required from the adversaries could be seen as a limit for the capabilities to achieve a malicious act, but it should not because these skills are accessible to the adversaries (both outsiders and insiders). Insider threat is a real challenge. As mentioned in the IAEA Nuclear Security Series No. 8 "*insiders could take advantage of their access […], complemented by their authority […] and knowledge of the facility […]*" to bypass dispositions dedicated to protect the installation. Designers should take into consideration insider threat early in the process, for example by implementing vetting.

Lastly, benefits of a good, integrated design of security is that, by reducing security constraints on other activities and on the staff, security can be more easily accepted and understood, which may be very helpful for promoting security culture. Ideally, security measures will even be "transparent" for most people, as they are today for tourists visiting the Opéra Garnier.

2.3. How to implement security by design efficiently?

One possible limiting factor for the designers is to have access to the design basis threat (DBT), which is generally a national and confidential information, since it generally defines the load cases of the threat that the installation has to withstand. Nevertheless, designers can benefit from a lot of disclosed information (for example regarding past terrorist attacks) that can help them taking into consideration current threats.

Some design choices can be very beneficial to cope with a wide range of threats, such as underground designs. The design should take into consideration the possibility to adapt security measures to national context, by letting room to potential enhancement of the basic security measures.

Moreover, security of a nuclear installation should be guaranteed during the entire lifetime of the facility from the construction to its dismantling. But evolutions of the legislative and regulatory framework, as well as the DBT, should be envisaged, because the threat changes over time and new knowledge may lead to new requirements. That is the reason why, when designing a nuclear installation, it is expected also to let room for future additional security systems to cope with such evolutions. With regard to SMR, it could be challenging because of its compact footprint and the will of designers to optimize the installation. Moreover, as done in safety, it could be interesting to consider the use of margins during the design of security features, first to take into consideration normal wear, ageing, the limit of the knowledge at the time of design and potential evolution of the capabilities of the threat. As a complement, the choice of the security features should consider the best available techniques, emerging techniques and eventually the possibility to upgrade existing security features during the lifetime of the installation.

Implementation of an efficient security by design may also lead to evaluate and question the choices of technologies (not dedicated to security) or installation layouts to end up at a better solution regarding security purposes. For instance, some materials may show better characteristics with regard to operating purposes, but are more vulnerable to the threat than other technologies. On the other hand, without downgraded the safety level of the installation or the operation capabilities, some technologies offer better intrinsic security than others. Even

though these technologies are not, at the time of the design, identified as targets, but still are part of sensitive systems of the installation, choosing the more secured technologies will contribute to the robustness of the facility to withstand the threat.

All the above observations lead us to consider that designer should benefit a lot from using a design team which would be composed of a set of cross-functional skills (covering safety, security and operations). The use of such a combined effort and collective work should improve the implementation of an efficient security by design. In particular, such teams are ideal for incorporating systems engineering best practices and performing requirements analysis to best trade off the different functional requirements. Interfaces between safety and security is a key aspect to ensure an efficient security by design and SMR are a good opportunity to implement it. So, even if it is a collective work, it is important for safety experts, who are part of the team, to have a security culture in order to understand and propose relevant solutions and conversely for security experts.

Security by design is also a challenge for the States. Firstly, the current legislative and regulatory framework should allow taking into account security by design as part of the authorization process. That means, States should be able to get involved in new nuclear project to build in their country as early as the design phase. For instance, national framework could enable the regulators to assess the acceptability of new nuclear installation designs up front in advance of specific proposed developments or at their early stages.

Secondly, States should assess their national framework and regulations to ensure that they are adapted to these new concepts. SMR, even though their designs are based on well-known concepts (such as PWR or BWR), will introduce specificities on which the State might need to have a thought. For instance: would additional or specific regulations be necessary to consider SMR? How could national DBT apply to SMR? Should the regulatory process be adapted to adapt to smaller, more numerous facilities? Etc. The use of a performance-based approach may be very useful, because it may be easier to adapt to any nuclear facility, including new concepts, without need to adapt too specific requirements.

In any case, all nuclear facilities, including SMR, should be submitted to the same security goals, applying a graded approach.

3. CONCLUSIONS AND PERSPECTIVES

Early consideration of nuclear security concerns in the design of nuclear facilities can allow substantive gains regarding security and costs, thanks to intrinsic solutions creating synergies with other concerns (particularly with nuclear safety) and to optimized security provisions. As such, security should be treated as a basic part of any nuclear project and should be part of the training of nuclear designers. Security experts should also be involved in early steps.

For new concepts such as SMR, that will need to be cost-effective, these considerations are vital, in order to achieve comparable goals to other reactors, considering a graded approach. In order to adapt to different design basis threats depending on the country, as well of evolutions, these concepts will need to consider technologies that are less sensitive to malicious acts and designs that can be easily upgraded.

But States should also consider reviewing their regulatory framework and regulations to be able to adapt to these new concepts.