# cybersecurity matter for remote

# access of SMR

Olivier D’HENIN

IRSN

Fontenay-aux-Roses, France

Email: olivier.dhenin@irsn.fr

Olivier FICHOT

IRSN

Fontenay-aux-Roses, France

Abel BENOIT ROSARIO

Ministry of Ecological Transition and Territorial Cohesion

French Nuclear Security Authority

Paris, France

**Abstract**

Remote operation is a crucial aspect of the business model for some Small Modular Reactor (SMR) operators, encompassing Physical Protection Systems (PPS) and Instrumentation and Control (I&C) systems. However, the reliance on digital technologies raises viability concerns related to the growing potential for cyber-attacks.

The paper presents a study on cyber security issues of remote communication and identifies technical vulnerabilities related to potential unmanned teleoperated SMR plants. It proposes a new implementation that complies with the Defense-in-depth principle highlighted in NSS 17 that relies on nested VPN tunnels for both PPS and I&C operation. This approach is compared with other possible implementations, addressing their advantages and drawbacks. The study also examines some of the implementable solutions in terms of encryption algorithms to consider the whole lifecycle of SMR operations. The document proposes generic recommendations for telecommunication hardware to take account of diversity and segmentation of usage principles.

This study also analyses the French regulatory framework in order to identify the potential adaptations required for the development of such systems.

## **INTRODUCTION**

### SMR designers emphasize technological breakthroughs. They highlight the use of factory-assembled modules, standard industrial components, innovative business models and lower costs. Among the technological disruptions, the concept of unmanned plants operated remotely from a central control room appears to be a major challenge.

While the performance of remote links has improved considerably in recent years, cybersecurity issues have become a major concern. This article attempts to review the fundamental concepts elaborated in standards and guides, and then to imagine the implementation of a technically and economically viable architecture. Finally, we will assess the acceptability of the solution from a computer security point of view.

In France, a dozen SMR concepts are at various stages of design. One of these considers the fully remote operation of an HTR-type reactor. This project is intended to produce heat for various industries. Some of the technical elements of this study are inspired by this use case, which is one of the most disruptive and therefore represents an appropriate case study.

### French regulation, are there any blocking points?

Before tackling the technical aspects, we examined possible regulatory hurdle to remote operation in French regulatory framework. Today, French nuclear operators have to comply with two sets of regulations: the first is aimed at nuclear facilities/NPP in terms of non-proliferation of nuclear materials and protection against sabotage, and the second concerns the cybersecurity of all national critical sectors, including the nuclear industry. Among all the requirements of these two sets, the following are related to remote operation.

The first deals with Physical Protection Systems (PPS), which generally include detection systems, video management systems, access control and central alarm systems. The regulatory framework mentions that the information system must be **isolated**. This restriction prevents any connection outside the site, but it is mentioned that a waiver can be considered if duly justified. We can assume that the future SMR operator will provide this type of justification.

The second concerns all critical systems that may be remotely connected. The French national cybersecurity agency (ANSSI) requires encryption and authentication mechanisms in accordance with their guide [4]. This regulation also requires double factor authentication. These technical obligations are fully applicable and will be discussed in chapter 2 of this paper.

Regarding the European NIS2 directive, which is currently being transposed in French national laws and regulations, the requirements have not yet been officially implemented. This is a point to keep an eye on when this work will be available.

### DCSA for I&C and PPS

Today, nuclear French operators implement the security level approach supported by IAEA and detailed in NSS-17T document [3]. It should be noted that some of them have extended this approach to the Physical Protection System. In the case of remotely operated SMRs, the sharing of communication resources and a common central control room hosting safety and security teams should reinforce the concept of Defensive Computer Security Architecture (DCSA). Whereas today I&C and PPS are isolated and operated by independent teams, we should see a technical and organizational convergence for remotely operated SMRs. It is highly probable that the I&C and PPS systems located both sides (reactors /control room), will be considered as a single architecture integrating different functions. This is the principle presented by the Canadian National laboratory (CNL) and illustrated in Figure 1.

### Type of link between CCR and nuclear plant

The communication means considered for SMR operation are highly dependent on the telecommunication infrastructures available in the country. As defined by ANSSI in its guide [2], an infrastructure leased from a telecom operator with dedicated resources (such as MPLS: Multi-Protocol Label Switching) is not considered a public network as long as the resources are logically partitioned from the rest of the traffic (e.g. with MPLS labels) and the operator offers service guarantees. It should be noted that this type of solution does not necessarily guarantee the confidentiality or integrity of flows, and in no way exempts the entity responsible from applying appropriate measures (such as a VPN) to ensure the authenticity, integrity or even confidentiality of flows.

In order to comply with this recommendation, the telecommunication links for remote operation of SMRs should be pseudo-private (or private) links. In this case, an attacker would need to have access to the operator's cloud (e.g. MPLS) in order to compromise the tele-operation link, which reduces the opportunity for an attack.

### Architecture proposed by CNL

The starting point for this study is mainly based on Canadian Nuclear Laboratories (CNL) work presented at AIEA Technical Meeting in 2022 [1] and we take the opportunity to thank them for their tremendous work.



FIG.1. *SMR Architecture overview proposed by CNL*

In the illustration above extracted from their presentation, CNL sums up several interesting concepts:

* Remote systems (SMR side) and central control room systems are considered as a unique system;
* Security Level approach (see IAEA-NSS17T [3]) is applied on both sides;
* Encapsulated VPNs concept in order to fulfil Defense-in-depth for remote communication;
* Security level 1 (most critical level) is not remotely accessible;
* Redundancy of the media.

The first phase of the study involved moving from concepts introduced by this presentation to effective concrete implementation of this architecture.

## **HOW to IMPLEMENT such ARCHITECTURE?**

For several years, IRSN has been developing a simulation platform for cybersecurity assessments. This platform called HYDRA is based on commercial cyber range provided by Airbus Cybersecurity, it is enhanced by Hardware in the Loop devices usually met in the nuclear industry. It’s the perfect candidate to implement SMR architecture and coming face-to-face with the reality of the field.

### Hardware selection

The selection of network assets must fulfil several criteria. First, even though most firewall suppliers offer products ensuring encryption and filtering functions, a good practice is to separate these two means by using dedicated devices. Secondly, it is recommended to diversify the suppliers, with the aim of limiting an attacker's leverage in the event of a vulnerability that could compromise a specific device. Finally, the qualification of products is one of the processes supported by ANSSI in accordance with French regulation. The aim is to provide vital operators and governmental entities with products and services that meet a strong need of security. Using qualified products for SMR infrastructure is then highly recommended.

Applying these criteria to the construction of the architecture, some necessary compromises emerged: as the number of qualified devices is limited, the choice was made to place them at the most exposed points of the architecture, between the SL5 and the outside (on both sides).

Concerning the diversity of the firewall providers, it makes no sense to go up to unreasonable number of providers. Indeed, multiplying the number of suppliers implies significant training resources for administration teams. Apart from the cost involved, this increases the risk of configuration errors, which is counterproductive. We have therefore limited ourselves to two manufacturers for our pilot architecture. Moreover, because splitting encryption and filtering functions implies a significant increase of Hardware, we applied this measure at SL5/Outside level only.

As regards equipment dedicated to I&C or Physical protection (PPS) hosted within different security levels, the segregation usage principle shall be applied too. To achieve this, zoning principle presented in AIEA NSS17T [3] document is fully applicable. Based on these elements, we implemented this part of the architecture on the HYDRA platform, and the result is presented below.

### Sizing limitation

Link performance in terms of bitrate, jitter and latency are obviously crucial for the exchange of operational dataflows. Video flows are the most affected by these characteristics. These constraints will be decisive in appropriate sizing of cameras in the installation. By way of example, a geostationary satellite (i.e. KA-SAT) link has an announced dataflow around 50Mb/s in reception (download) and 6Mb/s in transmission (upload). We can consider that each 1080p video stream (Full HD resolution), with H264 or H265 compression, requires between 4 and 12 Mb/s bitrates (per camera). If, on this basis, an optical link can easily support the flow of a dozen cameras, it will be necessary to degrade the quality and/or number of cameras to switch to a satellite data stream.

The bandwidth available on WAN links varies depending on the technology used (fiber optics, 4G/5G, xDSL, satellite). This must be taken into account when sizing the video protection system.

Video surveillance uses the largest amount of bandwidth of all the functions. It is therefore necessary to consider the number and type of links according to the video streams to be transmitted, the latter being proportional to the number of video streams proportional to the number of cameras used. The image quality and operability of the system will depend on factors such as the latency and jitter associated with each link. In the use case, it is envisaged that the number of cameras used to provide video protection for the site will be limited, making it compatible with some of the telecommunications link technologies.

Performance tests have been carried out on the pilot architecture to determine the maximum number of high-definition video streams that can be managed simultaneously on the platform. The actual platform, based on virtual appliances, can support up to 40 cameras. This limit is acceptable considering our use case.

## **IMPLEMENTATION**

As introduced in chapter 2, HYDRA allows to build realistic architectures with a “limited” investment. In the first instance, we used the virtual capabilities[[1]](#footnote-2) of HYDRA in order to limit the purchase of hardware. The first step was to perform a criticality analysis and then allocate I&C systems and PPS systems to the various security levels and different zones. For network simulation part, suppliers of firewalls and other network assets generally propose a virtual version of their products. Thanks to these virtual appliances, it is possible to create infrastructure and implement parameters and then check if the architecture can meet the requirements set out above. Reproducing the various remote links (satellite or LTE) and their intrinsic characteristics was the next challenge. This has been achieved in part by using the QoS[[2]](#footnote-3) parameters available in the equipment and then reproducing bitrate/latency limitations of wireless link types. Because HYDRA has a graphical user interface, the outcome of this work is presented below:

Une image contenant texte, diagramme, Plan, Parallèle

Description générée automatiquement

FIG.2. *HYDRA screenshot*

Finally, the devices related to control room are positioned at the top, while the lower part represents the systems installed on the reactor side. In the blue frame (on the right), different communication channels are modelized.

### Simplify tunnelling!

During the implementation phase, the following technical issue was pointed out: even if on a technical point of view, tunnelling encapsulation proposed by CNL is applicable, some experts in network domain have pointed out that maintaining operational readiness over a significant period of time could be tricky. Indeed, successive tunnels requires to establish connections between levels according to a precise time sequence. A variation in this sequence can lead to a global communication discontinuation. In the case of an unmanned site, on-site intervention can be both complicated and time-consuming. Here again a compromise emerged. While retaining the concept of Defense-in-depth, ANSSI considers **acceptable and more reliable** that an approach where all encrypted data flows (from SL2 to SL4) are encapsulated in the SL5 encrypted flow as illustrated in the following figure:

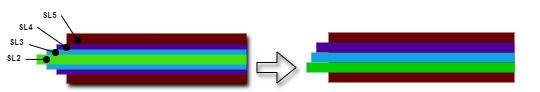


FIG.3. VPN Encapsulation

This approach effectively reduces the problem of the number of algorithms mentioned above. From the Defense-in-depth point of view, the concept is still implemented with a number of levels reduced to two.

### Cryptographic Algorithm selection

Information security is partly based on the encryption of data communications. Part of the problem is the choice of encryption algorithms to be used at each level of security in order to comply with the principle of Defense-in-depth.

It is vital to diversify the encryption algorithms used. There are two main reasons for this: reducing the risk of a single point of failure and reducing vulnerabilities.

Using a single encryption algorithm can create a single point of failure. If that algorithm is compromised, all data encrypted with it are vulnerable. By diversifying, or using multiple encryption algorithms, you reduce the risk. If one algorithm is broken, the others will still provide protection.

Different encryption algorithms have different strengths and weaknesses. For example, some algorithms may be susceptible to certain types of attacks or vulnerabilities that others are not. By using a variety of algorithms, you can protect against a wider range of potential threats.

It is therefore necessary to diversify the encryption algorithms for Security Level 5 and those for Security Levels 2, 3 and 4 by applying the principle of Defense-in-depth.

Great care must also be taken to select algorithms that comply with the recommendations to ensure that the algorithms used provide a security appropriate to the issues at stake.

In our pilot architecture, we use authenticated encryption to guarantee the confidentiality and integrity of data, as well as to authenticate its origin.

Of the few possible algorithms to choose from, we followed the ANSSI recommendations (see guide [4]) and opted for **ChaCha20-Poly1305 and AES-GCM** (Galois Counter Mode). For each of these algorithms, precautions must be taken, in particular regarding the non-reuse of initialization vectors (IV).

At each maintenance phase, the rekey can be performed in compliance with these precautions, and can be considered perfectly suitable.

### Next steps

It is envisaged that the administration of the SMR infrastructure (network equipment, security equipment and virtualisation infrastructure) have to be remotely performed from dedicated equipment fully segmented regarding functional means. The exact functions of each administration workstation have not yet been defined. As a next step, we will therefore have to work on a possible distribution of these functions, which will be very closely linked to the organisation of the operator.

It is possible that in this model the SL partitioning will no longer be respected: the nomadic SL3 administration workstations will connect to the equipment to be managed in SL5 (e.g. firewall). However, SL5 is not adjacent to SL3.

Remotely operated SMRs therefore appear to be borderline cases for the application of IAEA good security practices. Failure to apply an IAEA recommendation must therefore be justified by a risk-based approach.

In this particular case, the separation by SL is not strictly respected for administrative workstations connected to separate SL equipment within an SMR. However, the way in which nomadic administrative workstations are implemented ensures that they are not lacking any operational and security maintenance procedures and contribute to the high level of security of this architecture.

## **Conclusion**

The implementation of theoretical concepts often comes up against technical or economic issues that require compromises. This adage is appropriate when it comes to architecture that involves remote operation.

Regardless of the technology and resources used, the availability of a remote link can’t be fully guaranteed. This major concern is common to the safety domain. It has been correctly identified by SMR designers, who incorporate some risk mitigation measures in their design (redundancy and media diversity), but also plan to implement automatic shutdown and passive safety features.

The aim of the study was to focus on integrity (and confidentiality) means in an operational approach. Based on a CNL presentation as a starting point, an alternative implementation of a DCSA is proposed. Finally, the following figure illustrates a new version of the DCSA, including additional key points highlighted by this study.

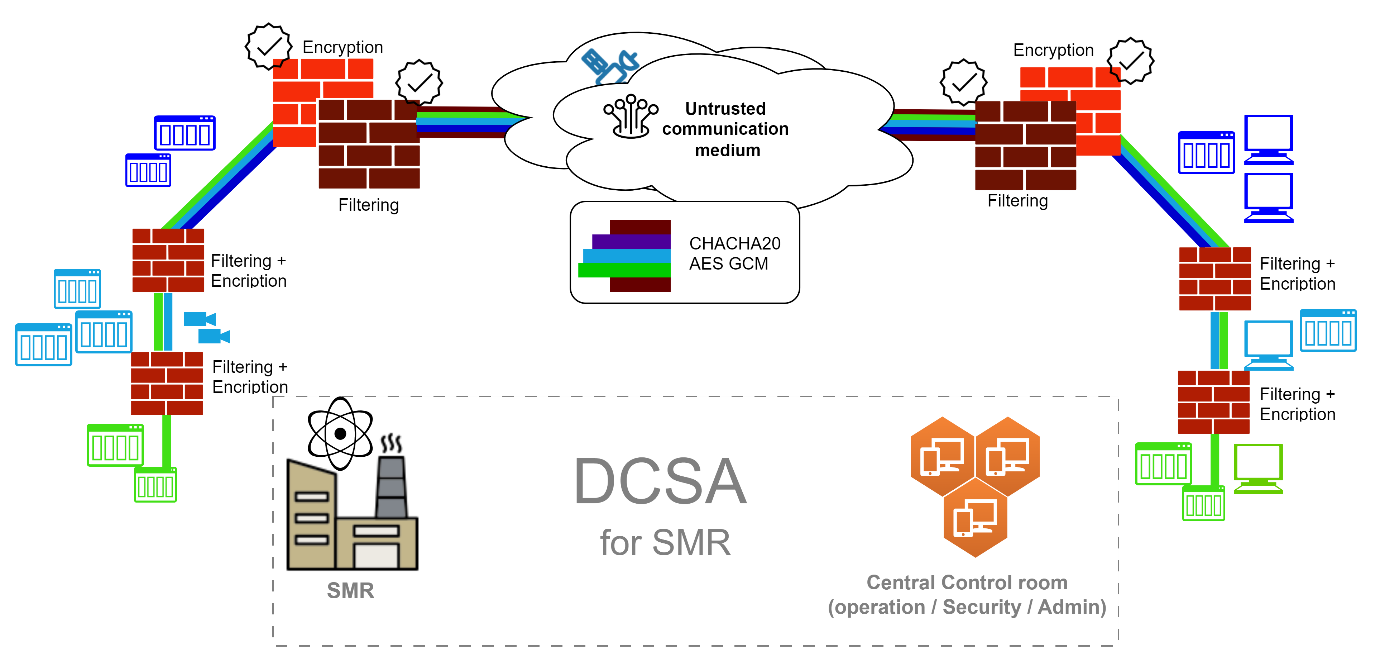


FIG.4. DCSA for SMR

|  |
| --- |
| **Lessons learned are:**   * **PPS can adopt security level approach (DCSA).** * **Filtering / Encryption functions are ensured by dedicated devices.** * **Front end devices have to be qualified by national cybersecurity agency.** * **Tunnelling principle can be simplified.** * **ChaCha20-Poly1305 and AES GCM algorithms are recommended.** |

References

1. Remote Monitoring and Control of a SMR, Proof of Concept, Canadian Nuclear Laboratories, Dave Trask 24Feb, 2022
2. Annexe B2 du Référentiel Général de Sécurité version 2.0, ANSSI, 08/06/2012
3. Computer Security Techniques for Nuclear Facilities, NSS17-T (Rev.1), AIEA, 2021
4. Guide de sélection d'algorithmes cryptographiques, ANSSI, 08/04/2021

1. Based on VMWare ESX product [↑](#footnote-ref-2)
2. Quality of Service [↑](#footnote-ref-3)