EASI SMR

D 5.7 Literature review on cybersecurity regulations, guidelines and standards for different modes of operations

Oleksandr Kukhotskyi
Oleksandr Klevtsov
Naim Qachri
Sylvain Boulley
Olivier Fichot

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Atomic Energy Community ('EC-Euratom'). Neither the European Union nor the granting authority can be held responsible for them.

1. Document information

Grant Agreement Number	n°101164810
Project Title	Ensuring Assessment of Safety Innovations for SMR
Project Acronym	EASI-SMR
Project Coordinator	Nicolas Sobecki, EDF
Project Duration	1 September 2024 – 31 August 2028 (48 months)
Related Work Package	WP5
Lead Organisation	ASNR
Contributing Partner(s)	IFE, SSTC NRS, DEND, Bel-V
Submission Date	30/09/2025
Dissemination Level	Public

2. History

Date	Submitted by	Reviewed by	Version (Notes)
29/07/2025	Olivier Fichot	Céline Poret	V0
August 27, 2025		Nicolas Sobecki	V1
September 8, 2025	Olivier Fichot	Nicolas Sobecki	VF

3. Table of Contents

List of Figures

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

List of Tables

4. Summary

Small modular reactors (SMRs) have a great potential to play a key role in driving energy transition and industry decarbonisation in Europe.
With innovative business cases, SMRs bring new challenges for different stakeholders, especially in our digital world. Cyber security and its consequences in the control room are key parameters for the global safety of these reactors.
This literature review highlights several aspects of SMR's Instrumentation and Control (I&C) that could bring new vulnerabilities: multi-unit control room and remote operation.

Existing literature already identifies that these specificities will increase cybersecurity risks for SMRs: extended use of automated, integrated I&C systems, based on new technologies including AI and more complex operating procedures will increase the attack surface and the reduced or even absence of local staff for operation will increase the difficulty to act without remote link. SMR reactors will particularly be sensitive to insider threat and supply chain attacks.

Regulation, standards and guidance have been analysed to identify protective measures and good practices to cope with such risks. Among these, a particular focus is made on the *Defensive Computer Security Architecture (DCSA)* concept which gives guidance for building a computer network architecture both enabling remote operation and strongly reducing risks of cyber-attacks linked with such a remote operation. At least two different architecture designs have been presented so far, by CNL and IRSN, for implementing the DCSA approach in a remote operation context.

In parallel, some countries (Canada, USA) have started adapting their regulations to consider cyber threats in a remote operation context.

Literature also points out the need for a thorough testing of future SMR computer systems and presents some tools already available to perform such tests.

Based on these findings, the present document provides examples of attack scenarios in which an attacker would take advantage of the weaknesses induced by multi-unit operation and remote operation of SMR reactors.

5. Keywords

Cyber security, Multi Unit, remote operation, I&C

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

6.Abbreviations and acronyms

Acronym	Description
BOP	Balance Of Plant
C&D	Communication & Dissemination
DCSA	Defensive Computer Security Architecture
DiD	Defence in Depth
I&C	Instrumentation and Control
LW	Light Water
MCR	Main Control Room
NPP	Nuclear Power Plant
SL	Security Layer
SMR	Small Modular Reactor
VPN	Virtual Private Network
WCR	Water Cooled Reactor
WP	Work Package

7. INTRODUCTION

This literature review aims at providing an overview of the current state of regulations, guidelines, and standards relating to SMR cybersecurity. It is part of WP5/T5.3, which aims at reinforcing the safety of Light Water Small Modular Reactors (LW-SMRs) by addressing human factors and cybersecurity.

LW-SMRs are a type of SMR based on well-known and proven technology, widely used in the nuclear industry and already deployed in conventional reactors of varying power levels, mainly for electricity generation or naval propulsion. They are slow neutron reactors that use light water as a moderator and coolant.
A large documentary corpus describing relevant cybersecurity measures for I&C of light water reactors in general already exists and is also applicable for SMR.
To be more relevant when it comes to SMR cybersecurity, the present literature review aims at presenting cyber regulations, guidelines, and standards which focus on features and risks specific to SMRs.

Therefore, an initial analysis attempted to identify the cyber-specific features of SMR I&C, compared to LWRs already in operation, answering the question:

“What are the specific characteristics of the digital I&C of LW-SMRs that increase the cyber attack surface of reactors or potentially introduce new vulnerabilities compared to the systems used in already operating LWRs?”

IAEA SRS No. 123 [9] considers some specific features of SMRs. In conventional plants with multi-unit control rooms, typically, a single crew is dedicated to a single reactor, with the possibility that they or someone else is responsible for the balance of plant systems. An SMR may use a smaller staffing model commensurate with a potentially simpler safety case than for a

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

current WCR. In an SMR, the novel proposal may be that multiple modules (reactors) at a single site may be operated by a single team from a single main control room (MCR). This team may be responsible for multiple reactor modules, associated module secondary systems and possibly shared systems. The design of a multi-module SMR plant often has some plant systems shared by all or some modules. A single cyber attack on the shared system could possibly impact several reactors or the shared system could be used by the attacker to spread to several units. This naturally impacts on I&C architectures, control rooms, control room systems and electrical power systems. SMRs may use remote monitoring and support centres more extensively than current water cooled reactors (WCR). The same SMR design may be used at different sites, so some projects may consider remote centres for monitoring and support in normal operating conditions and under accident conditions. Remote link implied that communication can use system out of the control of the operator, for example internet. Maintenance represents an important part of operation and personnel costs, and SMR designs often look for ways to optimize it (e.g. by using on-line monitoring to promote condition based maintenance or off-site monitoring to assist local operators in prognostics and diagnostics). Longer operation cycles and reduced inventory of active components (e.g. valves, pumps) may also need to be considered when addressing on-line and off-site monitoring. There may be a distinction between the overall I&C architecture of a plant and the overall I&C architecture of individual modules at the plant.
Some possible areas of novelty related to computer security in SMRs are:

- computer security during transportation to a site of modules that are fully assembled, configured and tested in a factory;
- staged construction;
- remote monitoring and support centres;
- the existence of multiple, quasi identical units in many different geographical sites; and
- separation (from a computer security standpoint) between the modules of a multi-module plant.

In addition, the review benefited from the contribution of two projects, NUWARD SMR by Nuward and LDR-50 by Steady Energy, which served as a basis for defining the areas of literature to be explored from a cyber perspective.

LDR-50 is implementing multi-unit operation, with a single control room controlling several reactors. This is a key point that seems to be shared by many other SMR projects, regardless of their technology.

Secondly, the project of Steady Energy plans to set up a remote access to the reactor to collect operational data and, in the longer term, to possibly enable remote operation. Looking more broadly at the scope of SMRs, some projects use remote access in various forms, including remote control, remote maintenance, remote administration, etc. Remote access allows operations on multiple reactors from a single point of operation or maintenance. Calogena project is an LW SMR example planning to implement both multi-unit operation and remote access.
It should be noted that a remote access is a possible path for an attacker to take control of the reactor, even if it's not designed to. To be clear, a remote access allowing only the ability to send a shutdown command could theoretically be exploited by an attacker to send other types of command to the I&C.

At this stage of the design, neither project envisages using artificial intelligence for reactor control. However, without necessarily referring to artificial intelligence, it should be noted that advanced automation is often linked to, or even necessary for, the operation of several units in order to lighten the load on the operating teams.

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

The following literature review therefore focuses on two topics: multi-unit operation and remote access, with the aim of answering the question, for each topic, "what regulations, guidelines, or standards apply and how do these two areas increase the cyber attack surface of reactors ?"

A final chapter aims at identifying possible attack scenarios involving these two areas specific to SMRs, which could be explored in connection with the simulator experiments that will be carried out as part of WP5/T5.1.

8.MULTI-UNIT OPERATION LITERATURE REVIEW

The consortium experts reviewed 19 publications (standards, reports, articles) containing information about the different aspects of multi-unit operation.
The analysis covered 6 articles, 10 IAEA documents (standards and reports), 3 other organizations' reports.
All 19 analyzed publications can be conventionally divided into 4 topical groups:

Group 1: General multi-unit and SMR publications [1-11];
Group 2: SMR I&C publications considering multi-unit aspects [12-16];
Group 3: SMR cybersecurity publications considering multi-unit aspects [17-19].

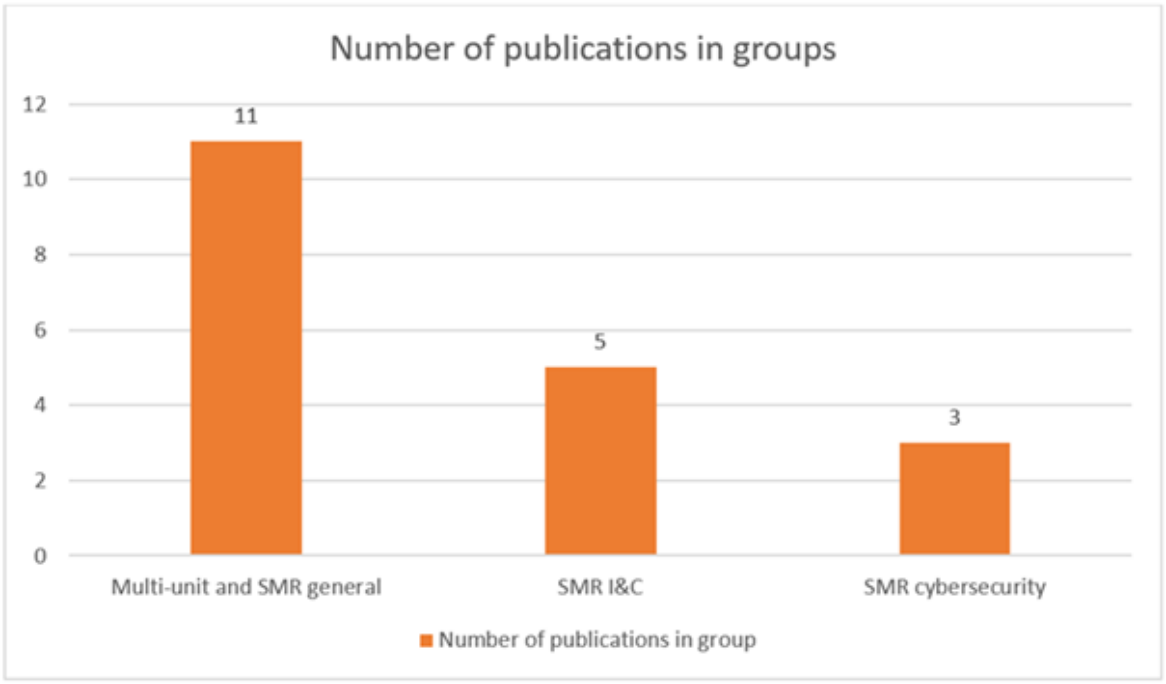

Fig 1. Groups of publications

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

8.1. GENERAL MULTI-UNIT AND SMR PUBLICATIONS (GROUP 1) REVIEW

The BNL-96816-2012-CP [1] examines lessons learned from non-nuclear industries to inform SMR operations. It highlights the challenges of managing multiple reactor units from a single control room and the role of automation and human factors engineering (HFE) in ensuring operational safety and efficiency.
Insights were drawn from three non-nuclear industries:

- Unmanned Aerial Systems: emphasized adaptive automation and workload management for multi-unit control. These systems rely on autonomous technologies that can dynamically adjust control levels based on operator workload, supporting efficient multitasking and reducing cognitive strain.
- Oil Refineries: demonstrated the importance of alarm system optimization and human-system interface (HSI) design. They use advanced alarm prioritization and filtering techniques to prevent alarm flooding and use intuitive HSI layouts that promote quick decision-making under stress.
- Tele-Intensive Care Units: showed how remote monitoring, communication strategies, and flexible staffing enhance multi-unit oversight. These systems leverage centralized monitoring platforms and role-based communication protocols to maintain situational awareness and allow specialists to oversee multiple patients (or units) simultaneously with minimal performance degradation.

The document concludes for SMRs based on an analysis of non-nuclear industries, highlighting key operational considerations. Namely, automation must balance efficiency and operator awareness to prevent cognitive overload. HSI design should incorporate clear alarms and comprehensive system overviews to enhance situational awareness. Additionally, flexible staffing models are essential for effective emergency response and workload distribution. While multi-unit SMR operations are feasible, their successful implementation requires advanced automation, optimized HSIs, and dynamic staffing strategies to ensure safety and efficiency.

IAEA No. SSR–2/1 (Rev. 1) [2] contains the requirements concerning multiple-unit sites.
Requirement 33 establishes the following requirements on safety systems, and safety features for design extension conditions, of units of a multiple unit nuclear power plant.
Each unit of a multiple unit nuclear power plant shall have its own safety systems and shall have its own safety features for design extension conditions.
Paragraph 5.63 requires that means allowing interconnections between units of a multiple unit nuclear power plant shall be considered in the design to further enhance safety.

IAEA publications [3] and [4] are devoted to description of design peculiarities for different types of SMRs developed by different countries. It is noted that most of the SMR designs adopt advanced or even inherent safety features and are deployable either as a single or multi-module plant.
Though significant advancements have been made in various SMR technologies in recent years, some technical issues still attract considerable attention in the industry. These include for example control room staffing and human factor engineering for multi-module SMR plants, defining the source term for multi-module SMR plants with regards to determining the emergency planning zone, developing new codes and standards, and load-following operability aspects. Some potential advantages of SMRs like the elimination of public evacuation during an accident or a single operator for multiple modules are under discussion with regulators.

The publications [3] and [4] reveals main technical characteristics among several SMR that use multi-module design, such as: IRIS (International Consortium), NuScale (USA), AP300 (USA), HTR-PM (China), HTMR100 (South Africa), 4S (Japan), Mk1 PB-FHR) (USA) and others.

It should be noted that some publications differently define terms “multi-unit” and “multi-module”. For instance, according to the IAEA No. NR-T-1.18 [7] multi module reactor plants describe reactor plant designs that have more than one reactor module located within the same plant, with the understanding that there could be several multi module plants built at a particular site. It is important to differentiate this from the more traditional multi-unit site approach employing large nuclear reactors, where a nuclear site can have more than one unit, with each unit having one large reactor housed inside.

IAEA No. NR-T-1.18 [5] highlights several advantages of multi-module design:

- - Lower initial capital investment;
- - Ability to add additional modules as the demand for power grows;
- - Higher plant availability since not all modules will need to be off line for refuelling at the same time saving ability to have several modules continuing operation during outage periods.

SMR designs as multi module plants may allow (depending on regulatory acceptance) several modules to be installed and operated, with others being installed at a later date. The early start of several modules will allow the ability to create a cash flow from operations and start repaying debt will significantly reduce the overall financing costs. Significantly reduced financing costs can make a high capital cost nuclear project economically viable.
To accommodate seasonal variations, reductions in baseload power can be achieved more effectively, and perhaps economically, in multi module designs by simply taking one or more modules off line. Maintenance and refuelling efforts can be planned and conducted during these seasonal variations.
Procurement processes for the acquisition of key equipment during different phases of an SMR deployment project life cycle may be slightly different from that of a large nuclear power plant project owing to the specific fabrication and transportation techniques of various SMR modules. For multi-unit (or multi module) nuclear power plants with SMRs, procurement may become complex. Sustainability of the supply chain is a prerequisite and this depends on the continuous order or demand. During the pre-project phase, procurement may be less, due to modularization adopted in SMRs.
As it is part of an engineering, procurement and construction package, procurement is an important factor in maintaining the economic competitiveness of SMRs. Fewer subcontractors and vendors may be required in the case of multi module SMR plants than in multi-unit large reactor plants.
In addition to these important regulatory issues, SMR developers need to carefully work through the technical details associated with developing the safety basis for the operation of multi module units while assessing both common cause and multi module failure scenarios.

IAEA No. NR-T-1.19 [6] contains the terms for describing advanced NPPs (including SMRs) need to conform to the broad, general, common understanding by the public as well as by the technical community.
In particular, IAEA No. NR-T-1.19 [6] defines the term «unit» (single-, dual-, multi-unit): each unit represents a separate reactor (nuclear island and BOP) capable of being operated. In the case of dual- or multi-unit plants, a unit can operate independently of state of completion or operating condition of any other units co-located on the same site but in different containment/confinement buildings, even though the units may have some shared or common systems.

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

According to the IAEA No. NR-T-1.19 [6] a small modular reactor is defined as an advanced reactor that produces electricity of up to 300 MWe per module and is designed either as a single or multi-module NPP, which systems and components can be fabricated as modules in their factory setting then transported to site to shorten construction duration.

According to IAEA SRS No. 123 [7] with respect to human factors engineering, the following aspects need to be considered:

1. Multi-module plants may have modules (production units) in different stages of the nuclear facility lifetime (i.e. construction, commissioning, operation or decommissioning), and multiple operational modules can be in different operational states (e.g. refuelling, outage, anticipated operational occurrences, design basis accidents). Hence, the human–system interface (HSI) may be different from that of a current WCR in that it includes operational strategies that can be applied when modules are in different operational states or different lifetime stages.

2. When a control room that is shared between modules and other shared operational support facilities, simultaneous monitoring and control of multiple modules is different to the monitoring and control of a single unit, which is current practice for WCRs.

3. For HSIs for shared systems, some considerations include:
   - the interdependence, overlap or redundancy of these HSIs raises the possibility of common cause failures that can affect multiple modules;
   - modification of these HSIs may be a particular issue if there are modules in operation while new modules are being constructed;
   - HSIs may be provided to isolate modules from shared systems, as necessary, for maintenance and other activities.

4. Potential module to module differences may – intentionally or unintentionally – affect human performance, which, in turn, will influence situational assessment and response planning. Intentional differences can be HSI design aspects of module differences that are planned and standardized. Planned and standardized HSI design is likely to be key to supporting the ability of plant personnel to distinguish between modules, particularly as part of outage management, when correct module identification is essential to safety.

IAEA-TECDOC-1785 [8] considers some specific issues concerning multiple-unit sites.
Two or more reactor units can be built in one site. The benefit of placing several units in the same site is not only economical, but also provides the possibility to have electrical system cross connections among the units which are very useful in emergency. One unit's equipment and staff support could help others when abnormal conditions such as failure of emergency diesel generators occur. However, a site with several units also faces potential major problems. The Fukushima Daiichi accident indicated that multiple reactor units in one site face the followings:

- Unexpected problems (especially spreading the problems from one unit to other units)
- Hydrogen gas produced in Unit 3 due to the interaction of melting core and steam leaked to Unit 4 through shared venting system between the two units. The hydrogen then detonated in Unit 4, damaged the reactor building and distracted the emergency team in dealing with the Unit 1. Such an explosion was never foreseen. The explosion in Unit 4 influenced the emergency team to concentrate more on Unit 4 spent fuel pool, wrongly perceiving that the source of hydrogen explosion was due to uncovered fuel in the spent fuel pool.
- Unexpected aftershock challenges

When multiple reactors are built at a site, unexpected challenges can happen as an accident in one unit may disrupt the operation and accident management of the neighbouring reactors. In

the Fukushima Daiichi accident when the emergency team was trying to cope with the situation in Units 1 and 2, the explosion in Unit 1 spread radioactive debris in the area around the complex. The explosion damaged the cables and mobile generators that had been installed to provide power to the standby liquid control pumps. The emergency teams had to work in challenging circumstances. They faced a mix of problems from stabilizing the reactor systems to protecting themselves from the radiation due to explosion in other units. The workers had to wear additional protective clothing and stay within time limitations thus limiting their mobility and availability.

- The need to respond to all units concurrently strained all resources on-site

In multiple-units sites, there is a possibility that several reactors undergo concurrent accidents due to a common cause. When these simultaneous accidents occur, the resources to handle all abnormal conditions at the same time become strained. For example, when operators of Unit 3 requested a fire engine to be dispatched to prepare water injection, all of the site fire engines were being used to mitigate the ongoing problem in Unit 1. Earlier, requests for off-site fire engines were unsuccessful because the roads were impassable.

As the above findings reveal, it is recognized that the issues concerning multiple reactor sites and multiple sites must be addressed. The current design of SMRs typically offers multiple reactor modules in one plant which ranges from two to twelve modules. So it is important to consider the issues of countermeasures shown in the Table 1.

Defense in Depth level	Critical issues addressed	Options for counter-measures	Considerations for water cooled SMRs	Relevant safety requirement
Prevention	Common cause failure	Ensure that the common cause failure and related accident management concerns are considered in the design.	• Multiple unit threat is particularly applicable to modular reactors. Some SMRs are proposed in multiple units. Regulatory body should require safety assessment for all units on the site as a whole. • Some safety related SSC could be interconnected between units in order to supply endangered units with vital assistance under external hazards. Two-unit plant, for example, would be more reliable than one unit. Safety assessment should take into account the suitability of sharing and cross connections, its vulnerability and benefits. • Provide cross connection between units with the reliable isolation capability. • Each module must be capable to cope with each type of accident.	IAEA No. SSR–2/1 (Rev. 1) [2], Safety of Nuclear Power Plants: Design Requirement 33 and relevant Paragraphs.

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

Control of accidents within DB	Safety systems	Ensure that countermeasures can be carried out for a unit where meltdown occurs and accident dose rate increases beyond analysis limits.	• Enhance the containment HYDROGEN control, using cooling, venting and filtering. • Provide shielding, convenient access and remote operations of countermeasures. • Assure crew can execute severe accident management guidelines without exceeding personnel dose.

Table 1 - Issues concerning multiple-unit sites

IAEA-TECDOC-1785 [8] analyses enhance human resource, skill and capabilities (in particular, taking into account possible multiple module reactor problems. It is noted that staffing for natural hazards is especially applicable to modular reactors where a response may be needed for multiple module reactors concurrently.

IAEA-TECDOC-2003 [9] presents the key SMR specific features and claims made by designers and vendors, particularly concerning the multi-module facilities:

- Control room staffing;
- Sharing of structures, systems, and components among modules;
- Modules' dependence/independence;
- Multi-module failure in hazards conditions.

IAEA-TECDOC-2003 [9] suggests that as the concept of SMR 'module' is not equivalent to the 'unit' or 'plant' concept for large reactors, the safety principles developed for the 'multi-units' issue cannot be transposed to 'multi-modules' in SMR facilities.
According to IAEA-TECDOC-2003 [9] the peculiarities concerning siting, design, construction, commissioning and operation should be taken into account during the licensing process (including the specific features of multi-unit or multi-module SMRs).
1. When licensing an SMR site or facility, regulatory bodies also need to consider, in particular, that many operating concepts can be different from traditional reactors (for example, multiple modules operated from a common control room by the same operating personnel).

IAEA-TECDOC-2003 [9] considers some safety analysis issues regarding multi-unit SMRs.
In particular, for the accident sequence modelling, regulatory bodies report that the following forward-looking considerations are needed:

- To delineate single and multi-unit accident sequences;
- To account for multi-unit common cause and causal dependencies, including functional, human, and spatial dependencies;
- To consider adverse impacts of a single reactor/facility accident on other units, thus creating additional multi-unit accident scenarios;
- To consider how operator actions may be adversely affected by multi-unit interactions;

It should be noted, that consideration of similar multi-unit factors is essential in the development of cybersecurity scenarios.

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

D5.7 Literature review on cybersecurity regulations, guidelines and standards for different modes of operations

IAEA-TECDOC-2003 [9] notes, that multi-unit/module SMRs may use shared systems to a greater extent that multi-unit NPPs because of their compact configuration and proximity, and this may impact among others, the selection of IEs, internal and external hazards, the approach to shared systems, DiD, human factors, engineering and risk assessment.
It should be noted, that cybersecurity scenarios must also take into account the impact of using shared systems.

Several teams, such as maintenance, emergency response, or training, are expected in some situations (design and country dependent) to be shared. It could be a maintenance team owned by a separate organization, or an emergency response team common to several owners on a same site. Each of these unique situations might raise a new challenge and has to be examined.

8.2. SMR I&C PUBLICATIONS (GROUP 2) REVIEW

Multi-unit operation of SMRs from a centralized control room induce specificities in the design of I&C systems for such SMRs.

IAEA No. NP-T-3.19 [10] describes the distinction between I&C systems for conventional, large reactors compared to those for advanced SMRs. Several advanced SMR concepts are planned to be deployed as multi-module plants (i.e. 2–12 modules per plant unit, with a power output of 10–300 MW(e) per module). The impact of shared resources and systems requires the implementation of more sophisticated controls to address, among others, the specific dynamic behaviour.
Integrated operation of multiple units SMRs can be implemented in a power park configuration of multiple units to satisfy evolving levels of power demand. As demand grows, additional capacity can be added through phased commissioning of more units. In addition to economical expandability a multi-unit plant has the advantage of only losing a small percentage of its power output should an individual unit be out of service due to a planned outage or unplanned trip. Unlike most existing multi-unit nuclear power plants, management of a multi-unit SMR plant is more likely to involve integrated operation of the units through shared systems and a common control room.
In fact, some SMR design concepts include configurations based on shared energy conversion systems (e.g. turbine generators) coupled to two or more reactors. The degree of operational integration within the plant can range from simple coordination of load allocation among separate units to co-located control room and workstations with some sharing of staff and equipment to single operator supervision of multiple units.

IAEA No. NP-T-3.19 [10] highlights the peculiarities of control room design for multi-unit SMRs. Some SMR designers propose operating models that either have multiple units or modules in a facility sharing a common control room or one operator (or operational team) supervising multiple modules simultaneously.

Human factors engineering (HFE) will most likely dominate the safety discussion of these proposals. As a result, human system interaction and human factors will be key considerations in I&C systems design of multi-unit SMR plants.

For multi-unit SMR plants, the control room and workstation are technically and financially important, and require extensive R&D. There is ongoing effort in design, analysis and simulation of control rooms and workstations for multi-unit SMR plants, with the goal of optimizing operational costs while meeting plant safety requirements.

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

Design considerations include the integration of automation addressing multiple units, new information systems, new operating procedures and any other aspect that changes the human–system interaction. Control room and workstation layouts and alarm management are two very important human factor features of an I&C system design for a multi-unit nuclear power plant. Alarm management in a multi-unit control room can be more complicated from a human factors perspective and can face significant challenges - not only alarms caused by each unit itself but also alarms caused by other units. An effective alarm management strategy will significantly enhance the operator's ability to reduce the consequence of an emerging abnormal occurrence.

Multi-unit control rooms for multiple reactor facilities already exist for large scale generating stations. For example, a four unit main control room (MCR) at a four unit CANDU facility. There is already a precedent for the safe operation of multiple units out of one control centre, and it should be noted that secondary control areas are not in shared facilities.

IAEA No. NP-T-3.19 [10] considers multi-unit control strategies. There are three architectural models representative of concepts under consideration for SMR facilities.

1. Traditional model. An MCR controls a single nuclear steam supply system (NSSS) to a single secondary side system (e.g. turbine and process steam plant). This model is used by most existing facilities.

2. Shared MCR model. A multi-unit MCR, with each unit controlled from a single independent I&C system. This model is used in Canadian multi-unit plants.

3. Shared MCR and BOP (balance of plant) model. A multi-unit MCR with each NSSS unit controlled from a single, independent I&C system but each interfaced with a common BOP I&C system. This model is currently not used; however, it is being proposed for some SMRs, such as the Chinese HTR–PM, which will connect two or more NSSS systems to a single turbine and steam plant.
Sharing BOP systems provides significant benefits, both in terms of capital cost and personnel utilization because these systems are not associated with a single reactor unit. With such a configuration, there is a strong coupling between the multiple SMR units and the BOP which, when presented with unbalanced load operation, can affect safe, smooth and steady operation of the reactors.

- In order to reduce the strong coupling between the multiple SMR units by the multi-use and unbalanced load operation, an advanced coordinated control strategy is needed. Some possible new coordinated control strategies are being studied and include the use of decoupling control, optimum control, non-linear adaptive control and intelligent control methods. All approaches seek to obtain better control performance of multi-unit SMR plants.

When considering a multi-layered I&C system architecture of multi-unit SMR plants, there will be commonalities between BOP systems and reactor systems at some levels.
In particular, some additional control layers may need to be made more unidirectional in nature and additional configuration management measures may need to be instituted. A multi-layered I&C system architecture can offer the following advantages:

- Each functional layer provides complementary control and monitoring capabilities that assure independent backup of the multi-unit plant operation and protection functions.
- The layered architecture allocates complex data management and display processing to the plant management layer, while making the control and protection systems as simple as possible.

- The highly distributed nature of the system network is flexible enough to allow upgrades of system components as additional units are added to the facility.

There are certainly technical challenges to be addressed to ensure a safe and economical design. In particular, the design of the I&C systems of multi-unit SMR plants will need to leverage rigorous engineering methodologies and proven automation technologies to address plant monitoring, control and protection systematically.
Shared MCR facilities, whether individual SMR units controlled by multiple operators or a single operator across multiple units, will require extensive HFE. Significant experience exists in other industries. There is also extensive operational experience for multi-unit control rooms in nuclear power plants, and designers need to build on this experience. It is important to note that the activity of plant operation is the focus of licensing by regulatory authorities. Where an MCR or secondary control room is planned to be located remotely from a facility in concert with local autonomous operation, the I&C systems will be considered by regulatory authorities to be an engineered extension of the facility's site I&C architecture. Thus, communication means has to be carefully considered as part of the design approach.
For multi-unit SMR plants the control room design has important technical and financial implications, and it requires extensive study and development. There is an ongoing effort in design, analysis and simulation of control rooms and workstations for SMR plants to optimize operator staffing and operational costs while meeting plant safety requirements.

Article [11] is devoted to human factors considerations for remote operation of SMRs. Advances in automation and the design of SMRs are key enablers for the remote operation concept, as well as for the multi-unit operational concept. It is claimed that the simpler design of SMRs, together with higher levels of automation than typically seen in conventional NPPs, and the increased use of passive safety systems, will result in less reliance on manual action. Thus, it might be possible for operators to oversee several reactor units operating in parallel. Another effect of these advances is that the number of staff required on site (including in the control room) can be substantially reduced.

While the argument for advanced design enabling remote operations appears reasonable, it brings uncertainties related to the potential new role of the human operator in a highly automated, multi-unit system.
When considering the multi-unit operational concept, the human factors aspects become more complex. Multi-unit operation raises questions about how operators can maintain situation awareness across multiple units, bearing in mind that these units may not be homogenous and may be in different operating states. When automation is introduced, this can further affect the operators' ability to be "in-the-loop" regarding process states and activities. There are concerns about both cognitive overload and cognitive underload associated with multi-unit operation, each of which can be detrimental to maintaining a good mental model and awareness of what is happening across the different units. There is recognition that new skills and competencies may be needed by operators in order to perform their tasks safely and efficiently in this new operating paradigm.

Report [12] proposes a developed supervisory control approach to enable automated control of SMRs. Authors of report [12] have created a fault-tolerant multi-unit SMR supervisory controller that collects and transfers information from local loops, supervise their actions, and adaptively optimize the controller parameters.
The vision for SMRs goes beyond large single-unit power generation to multiple smaller units at one site supplying steam to a turbine and the possibility of steam co-generation for industrial needs. The challenge for multi-unit operation is twofold. First, staffing needs must be addressed since this is seen a necessary for the economic viability of the concept. While many plant operations must be overseen by human operators, there will likely need to be an increased level

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

of automation in SMR operations. This will be particularly so for control functions, which must maintain suitable margins from safety limits during plant transients, versus safety functions, which must maintain a certain level of operator interaction in order to meet regulatory safety requirements.
Second, while each unit is independent from other units with respect to steam generation, the combination of multiple units feeding a single turbine or co-generation processes functionally ties these units together. Considerations for each unit's operation must be accounted for with respect to processes in the balance of plant and overall plant economics. SMRs likely will not be asked to provide base load but instead must provide load following. The economic considerations for load following can result in complicated economic dispatch models that also must account for operational considerations. While well-known algorithms for economic dispatching can be used to manage a multi-unit SMR site, start-up and shutdown increase operator workload, and some tasks (e.g., bringing a reactor critical) should demand operator action, even if only to provide permission.

The challenge is to find the correct balance between computer control and operator control. The objective is to have the computer maintain control over those tasks and processes that are tedious or trivial (e.g., rod control) and have the operator maintain control over plant objectives. The use of automatic control to control temperature and level setpoints has been well established in the nuclear industry. Three things are needed to meet these challenges. First, a system control architecture that allows controller parameters to be adjusted as necessary to meet changing operating conditions for multiple SMR units in a timely fashion. Second, a supervisory control strategy that allows units to be maneuvered independently to meet changing grid conditions, load following, and plant transients. Third, the system of SMR modules, balance of plant, and supervisory controller must be fault-tolerant to minimize the effects of failures on plant operation and safety.
According to the report [12] a primary objective of supervisory control of SMRs is the ability to manage multiple SMR units from one control room. In the research, authors aimed to provide both increased supervision, monitoring, and coordination between plants. It must be realized that this objective must be balanced with operator oversight. The proper balance between operation and automation must be determined.
One of the key differences between conventional NPPs and SMRs is the common design intention to operate multiple SMR units as a single plant, from a single, centralized control room. For example, a NuScale staffing plan report submitted to the US NRC for review and approval proposes a plant design of up to 12 modules, controlled from a single main control room. This concept of operation is vastly different from today's conventional NPPs which typically feature one or two reactor units are controlled from a single main control room. Canadian NPPs have up to four reactor units controlled from a single main control room, and so provide some valuable experience about the multi-unit operation and human performance aspects.
To achieve the multi-unit goal of SMR designs, consideration must be given to human factors engineering aspects such as the distribution of functions and tasks for multiple module operation, the design of control room layouts and human-system interfaces (HSI) to support operators in multi-unit operation, and the staffing policy to ensure there are enough operators available to monitor and control the plant in all operational states, as well as during potential disturbances.

According to the article [13] since 2018 the Halden Project has been worked a research activity on the topic of "Human Performance in Operation of SMRs". The main objective of the research activity is to identify the possible impacts of SMR control room concepts on human performance, and how these can be captured in human factors validation studies.

Two important documents were issued at the beginning of the research activity which helped to inform and shape the work going forwards. The first was a white paper issued in 2018 titled

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

"Small-scale simulator studies on multi-unit operation" which outlined some of the human factors challenges and research questions for multi-unit operation as understood at that time, including topics such as:

- operator vigilance in highly automated plants;
- the effects of distractions and interruptions in a multi-unit control room environment;
- the cognitive effects of multi-tasking when monitoring and controlling multiple units;
- the workload dichotomy of underload as a result of long periods of monitoring where operators are more prone to boredom and errors, to overload as a result of responding to simultaneous failures on multiple units;
- the effects on human performance of task switching between units and between passive monitoring to active control;

The second document that greatly informed the research activity was a Halden Work Report issued in 2019 titled "Operation of multiple reactors from a single control room: Experiences from nuclear and other industries" which contained a review of a range of control room designs and crew compositions for multi-unit operation in the nuclear and other industries. The report investigated CANDU nuclear reactors, hydropower plants, air traffic control and petroleum installations, with the goal of identifying human performance challenges and possible mitigation strategies that could be of interest for the SMR research activity.

The report identified that the multi-unit control room concept is also gaining popularity across these other industries and that many of these forecast that operations will become highly automated, with less human intervention. While these concepts can reduce (conventional) operator workload and the resources needed to monitor and control the plants, they may also introduce new operator demands for supervising and understanding the automated systems, to identify whether human intervention is needed. The report also identified a trend towards remote operation concepts amongst these other industries, which would introduce another set of challenges for operators, such as how to maintain knowledge of each plant and collect information about the current state of the plant.
The report also considered the ways in which multi-unit control room concepts differ from single-unit designs, the potential risk implications for one operator monitoring two or more units in parallel and for a team of operators monitoring multiple units in parallel, and which design principles exploit the operator resources for monitoring multiple units. The lessons learned from existing multi-unit concepts, and the available information about future concepts indicated that these issues will depend on the complexity of each unit, any differences and dependencies between units, and the expected need for human supervision and interventions at different operational states.

According to the article [13] in 2019, the Halden Project obtained a basic principle iPWR simulator from the IAEA, which was developed by Tecnatom. The IAEA simulator design is largely based on the Idaho National Engineering and Environmental Laboratory's Multi-Application Small Light Water Reactor (MASLWR), which is the basis for NuScale. Certain parameters have been modified to make the design more representative of several design variants being pursued around the world.
The first study on operating SMRs was conducted in the Halden Future Lab in 2019 to investigate monitoring strategies and prioritization of taskwork when one operator attends more than one reactor at a time. The main purpose of the study was to clarify and possibly develop new research questions beyond topics identified in previous reports.

The study identified several aspects worth further investigation, such as monitoring strategies when overlooking several reactors at a time; means to support monitoring of reactors in

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

different operating modes; detection of multi-unit failures; and team organization to support planned, parallel operations and safe prioritizations of tasks.

The main research questions for the next research activity on SMRs in the Halden Project are currently defined as:

- What are the impacts of expected staffing strategies (e.g., a 3-person crew for a 12-unit plant) on operating monitoring strategies across multiple units?
- What are reliable monitoring strategies for operators overlooking several reactors at the same time, that can minimize the risk of unit confusion?
- What are effective means for detecting single-unit and multi-unit failures?
- How can adaptive human problem-solving capabilities be utilized while ensuring safe prioritizations of tasks in multi-unit environments?
- To what extent will proposed control room layouts, user interfaces and staffing plans support operators' ability to maintain attention/stay alert, and/or how could these have a detrimental impact on human performance?

Further elaboration and prioritization of these research questions will be conducted in parallel with the development of appropriate scenarios for experimental testing in the new Halden SMR simulator.

IEC TR 63335 [14] identifies a number of issues of particular importance to light water SMRs. This report presents the main features of SMRs that not typically found in large reactors or that are of particular importance for SMRs, and that could require specific or additional requirements and recommendations. In particular, the following promising topics are considered:

- I&C architectures in a multi-unit and mutualized operation framework;
- extensive use of multiplexed digital communication or remote I/O for NC or Class 3 instrumentation;
- hazards and risk analysis in a multi-unit framework;
- impacts of staged construction in multi-unit plants;
- control of mutualized equipment in a multi-unit plant;
- staged construction of multi-unit plants;
- mutualized operation of multiple units;
- impacts of multi-unit plants and large fleets of identical units on security programmes;
- independence of electrical power supply systems in multi-unit, mutualized plant systems and mutualized operation frameworks, to avoid electrical issues in one unit causing issues in other units.

8.3. SMR CYBERSECURITY PUBLICATIONS (GROUP 3) REVIEW

Article [15] presents the framework and status of the development of a basic principle integrated pressurized water reactor SMR simulator designed to be an open-source tool to support computer security academic studies, capacity building activities, innovative SMR concept of operations, and digital instrumentation and control. This simulator aims to provide a test environment for integration and evaluation of novel and emerging digital technologies in the nuclear sector such as artificial intelligence, digital twins and smart sensors. Reference plant processes will be simulated to investigate the safety-security interface, show the application of the IAEA computer security guidance, demonstrate the effects of cyber-physical (blended attacks) and cyber-attacks, and reproduce the relevant digital communication channels and network protocols. The simulator has been developed using a modular framework to allow further integration of passive and inherent safety features or the replacement of the iPWR core by an advanced reactor core. Software containers are used to simplify replication and

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

deployment of the simulator. Ease of replication and deployment provides for quick instantiation of single or multi-unit reactor sites in different physical locations for analysing the impact of a centralized fleet management, and its nuclear security implications.

According to the article [15] the deployment and operation of SMRs will rely on advanced digital systems for innovative modes of operation, remote and autonomous operation, multi-unit or multi-module plants, and common control rooms and systems. These peculiarities should be taken into account during the simulation.

Article [16] presents a novel wavy-attention network for sensor attack detection in nuclear plants. The wavy-attention network comprises stacks of batch-normalized, dilated, one-dimensional convolution neural networks, and sequential selfattention modules, superior to conventional single-layer networks on sequence classification tasks. To evaluate the proposed wavy-attention network architecture, the International Atomic Energy Agency's Asherah Nuclear Simulator was utilized.
Although the ANS is developed for PWR, it can be repurposed as a Hardware-in-the-loop cybersecurity testbed for advanced reactors and SMRs. The ANS has been repurposed to develop an Advanced Reactor Cyber Analysis and Development Environment (ARCADE) that was integrated with a Small Modular Advanced HighTemperature Reactor (SmAHTR) model for cybersecurity applications. These ANS adaptations and applications underscore its role in preemptive security strategy development for SMRs and advanced reactors. The modular aspect of SMRs often involves the replication of standard units, and ANS can simulate the interconnected nature of these units under cyber-attack scenarios, providing insights into cascading effects within a multi-unit SMR site.

Article [17] explores key aspects and computer security challenges to digital instrumentation and control systems, resulting from new and innovative designs of small modular reactors and microreactors, and which have an impact on their deployment and operation. It is noted that SMRs are advanced reactors that may be deployed as a single or multi-module plant. Thus, SMR may be deployed as multiple units with a control room that share systems and functions between them. Therefore, SMR control rooms will be significantly different from those of today's NPPs and this may lead to the use of digital twins and artificial intelligence / machine learning (AI/ML) to support the operator. These control room architectures may have new failure modes and provide new attack surfaces for malicious action.

Article [17] provides insights about potential ways to prevent or mitigate cyber malicious actions:

- FPGA-based systems and ASICs being more specialized than general purpose CPUs may offer more secure operation;
- Requirements for safety and security will need to be integrated into the design of the I&C systems as part of a more harmonized approach, as part of the systems engineering approach for the SMR.
- The expected reduction of on-site staff, which will increase the use of autonomous systems, may demand a higher level of integration between safety and security systems.
- To decrease the surface attack against the plant and consequences of an attack against I&C, security system may be enabled to command the safety system to change operational/plant state to place the reactor in a more defensible state.
- Diversity for safety and security provides benefits to resilience, but increases the costs to the operator and regulator.

Diversity of design increases complexity and supports defence in depth for computer security. Multi-unit supervisory control systems deployed in fleets consisting of different generations

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

may use distinct hardware and software technologies, which may make difficult the integration of safety and security into the systems. This may be a challenge for the application of common computer security measures as data integration will be needed, especially if remote monitoring and supervising is in place.

8.4. CONCLUSION

Analysis of publications shows the following important multi-unit aspects that should be taken into account in frame of EASI-SMR project:
1) One general main control room is used for monitoring and controlling of technological processes and equipment of all SMR units/modules.
2) Interconnections between I&C systems of different SMR units/modules are possible.
3) The number of staff for operation multi-units (multi-modules) SMR is significantly less than number of staff at traditional NPPs.
4) Different SMR units/modules may be in a different modes or stages at the same time.

All these challenges will introduce new cyber risks, induced by new technologies, increased interdependency of systems which were previously independent, and more complex operating procedures.

In order to prevent or mitigate such risks, literature documents start to advocate some technical measures to take into account security in the design of future SMR reactors, such as replacing general purpose CPUs by specialized circuits (FPGA, ASICS), increase the ability of security systems to autonomously change a plant state, increase defence-in-depth by layer segmentation and diversity of security systems.

Literature also points out the need for a thorough testing of future SMR computer systems and presents some tools already available to perform such tests.

The identified features have been used as a basis for developing cybersecurity scenarios in Subsection 10.1.

9.REMOTE OPERATION LITERATURE REVIEW

9.1. IDENTIFICATION OF CYBERSECURITY RISKS LINKED WITH REMOTE OPERATION

The risk of cyberattacks against civil nuclear installations has been identified for a long time. A comprehensive report [118] was written on the subject a decade ago.

More recently, publications have underlined the increased risk of cyber attack against SMR reactors due to their specific features, including remote operation. Article [1919] highlighted the following specific weaknesses of SMR reactors against cyber-attacks:

- Remotely operating SMRs will cause functions previously performed by people physically present on-site or functions performed by analogue systems to be increasingly performed by remotely operated digital systems. It will induce an increase in the attack surface against SMRs compared to reactors already in operation;
- In addition, SMR operators will likely introduce digital systems performing new functions which are inexistant on traditional reactors, for example providing aid for remote operation. Such new systems may introduce new cybersecurity weaknesses;
- Remotely operating SMRs will increase the insider threat risk. Indeed, operating a SMR will involve fewer people but they will have extended powers compared to personnel currently working at a nuclear reactor. SMR operators will therefore have the ability to exert more influence on the reactor behaviour and security. Therefore, employees screening will be more critical to SMR operators;
- SMR reactors will not only be remotely operated but also remotely built, most parts being built at a factory. The licensee will therefore have less control over the quality assurance of the reactor components. An increased number of individuals and organizations will have access to the components before their installation on-site, compared to the traditional way of building a reactor which involves building most parts directly on-site. This will leave more room for supply-chain attacks;
- SMR reactors may become less resilient to cyber attacks than existing reactors, because of their increase reliance on digital systems for performing mitigation actions in case of incident, and because of their lack of on-site personnel.

9.2. PROTECTIVE MEASURES AGAINST CYBERSECURITY RISKS LINKED WITH REMOTE OPERATION

Article [1919] provided advice about how to avoid the cyber risks related to SMR remote operation. It highlighted:

- strengthening employees screening and supply chain integrity control;
- thoroughly testing new technologies used for remote operation;
- increasing air-gap protection of SMR computer systems (including protection against portable electronics such as USB devices);
- avoiding relying only on digital systems for critical functions.

From a computer system design point of view, a reference approach to be applied for securing critical computer systems against cyber-attacks is the *Defensive Computer Security Architecture*

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

(DCSA). Such an approach is key to the mitigation of a cyber-attack on the computer systems of any nuclear reactor, and particularly of SMR reactors.

The applicability of this approach to securing industrial I&C is described in detail in IEC norm 62443 [2121]. This norm is not specific to the nuclear sector, but another one is focused on the application of this approach to the I&C systems of a nuclear power plant: IEC 62645 [2222].

IAEA issued several guidance documents helping nuclear reactor designers to implement this DCSA approach in their design and which are relevant to the design of SMR reactors : the Nuclear Security Series guides 17-T [2323] and 33-T [2424].

As shown on the figure below from [2323], the DCSA approach aims at segmenting the assets of a computer system in different groups depending on their criticality to the system behaviour. It applies a graduated approach limiting cybersecurity risks by applying increasing security measures to increasingly critical assets.

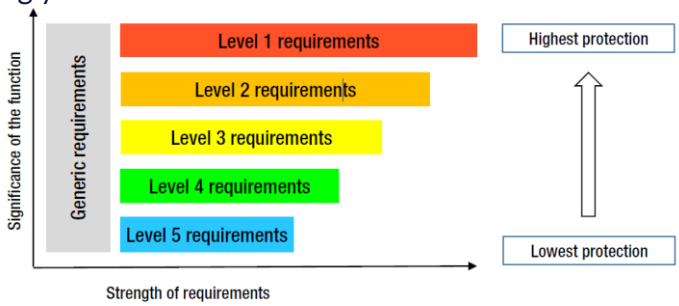

Fig 4. DCSA concept

DCSA Approach defines:

- Security Layers (SL) which are levels of a hierarchic classification, usually comprising 5 levels, defining increasing security measures to be applied to the devices belonging to each level. The lower the Security Layer, the more stringent the security measures applied to the devices in that layer. As shown on the figure below, from [2323], the most critical devices should be placed in SL1 and benefit from the strongest protection; while low criticality devices, of which there should be a highest number, can be placed in SL5 where they will be exposed to a greater risk;
- Zones which are subdivisions of the SL. Zones enable to form different groups of devices in a same SL and to apply additional security measures such as filtering of communications between pieces of equipment belonging to different zones of the same SL.

The DCSA approach also defines security rules and good practices such as:

- Filtering communications between pieces of equipment belonging to different SL;
- Filtering communications between pieces of equipment belonging to different Zones of a SL;
- Direct communication between a device belonging to a SLi and another device belonging to a SL which is not SLi-1 or SLi+1 is forbidden;
- Devices belonging to a given SL are not allowed to initiate a connection to devices belonging to a more critical SL, for example from SL2 to SL1 or SL3 to SL2.

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

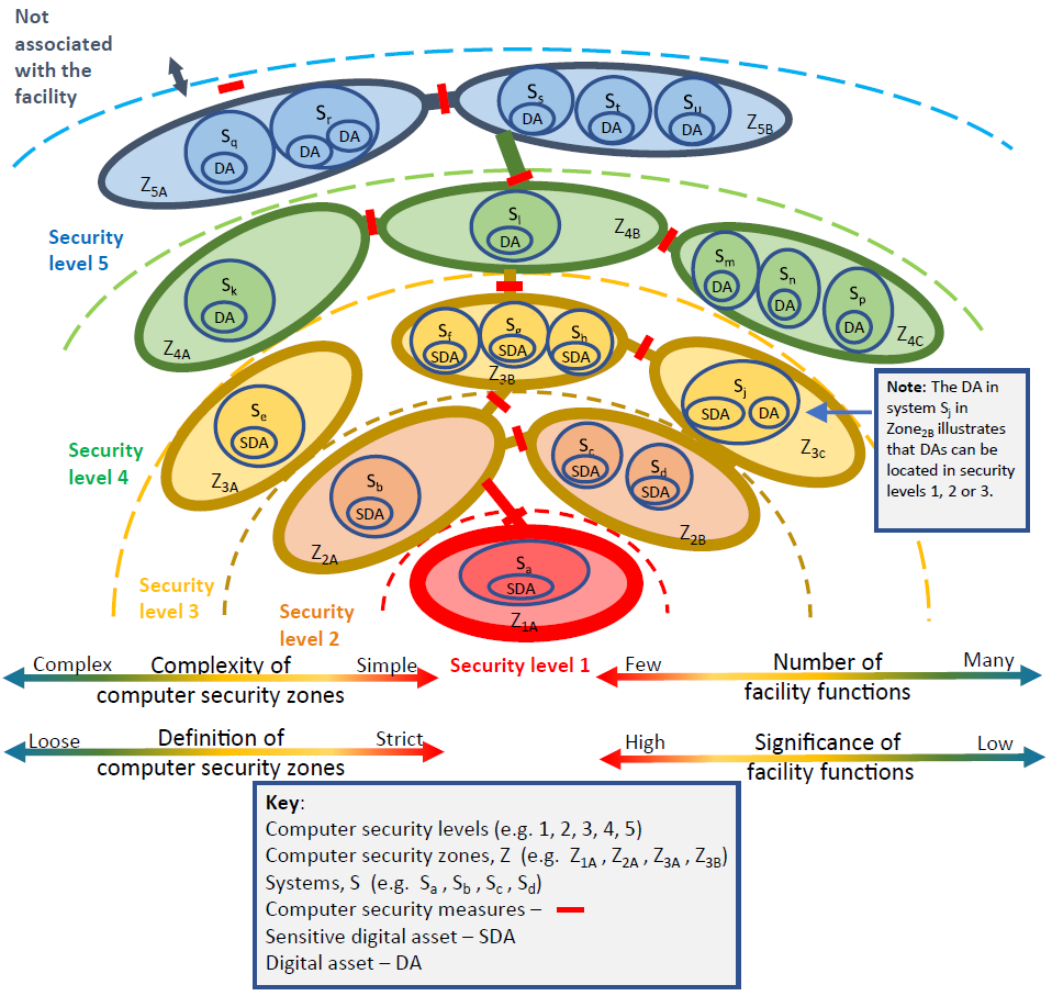

Fig 5. Security Layers and zones

The DCSA Approach has already been applied to SMR reactors. As an example, it was applied to General Electric PRISM SMR reactor in reference [2525] but this application did not specifically consider remote operation.

More recently, Canadian National Laboratory has defined, in [2626], an architecture for the I&C computer system of a SMR reactor, applying the DCSA approach and taking into account cyber risks specifically induced by remote operation. To enable on-site equipment to communicate with equipment located in a remote control-room, while enforcing the DCSA rules described above, this architecture applies the following principles:

- The on-site computer network and the control-room-side computer network are considered as a single computer network to which the DCSA approach is applied;
- An on-site device and the device located on the control room side it is communicating with shall be in the same Security Layer
- The on-site devices belonging to a given Security Layer and the control-room-side devices belonging to the same Security Layer shall communicate through a communication link dedicated to that Security Layer.
- The communication link of each Security Layer is protected from the devices in other Security Layers and from the outer world by setting up a VPN tunnel for that Security Layer between the reactor site and the control room.

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

The architecture resulting from applying these principles is shown on the figure below, from [2626].

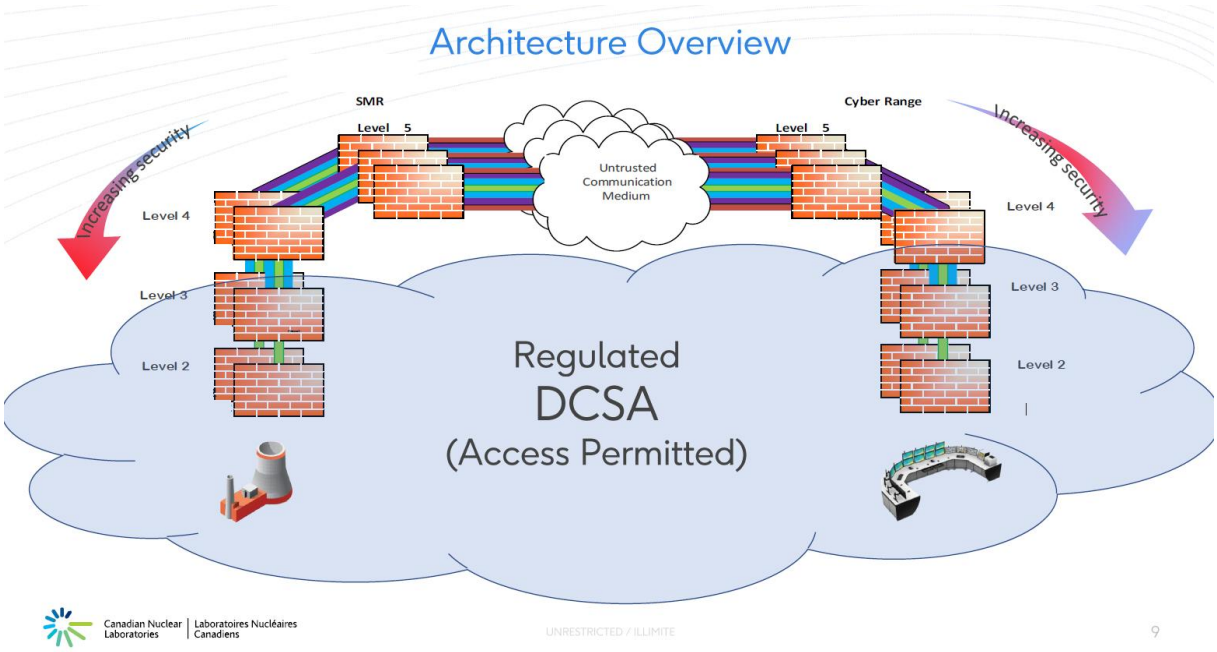

Fig 6. remote operation architecture proposal

Based on this architecture IRSN presented in [3030] an alternative architecture shown in the following figure. It uses a different implementation of the VPN tunnels between the reactor and the control-room, achieving a similar level of protection at a lower computational cost.

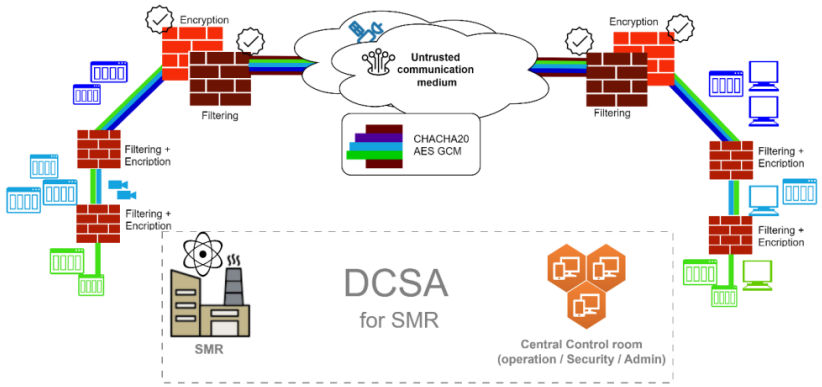

Fig 7. Alternative architecture proposal for remote operation

9.3. SMR CYBERSECURITY REGULATIONS

Regulators have been pushing SMR designers to consider security, including cybersecurity, into the design of SMR rectors. Article [2020] presents the benefits of integrating the approach of "Security by Design" into a regulatory framework. It cites remote operation of SMRs as a source of weakness against cyber-attacks making Security by Design even more critical to SMRs than to other reactors. The article lists the following principles to be applied in this approach:

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

- Integrated approach: working with engineering and safety specialists to achieve integrated security systems; for example, integrating physical and cyber security specialists in the design process;
- Inherently secure: design plants, facilities, buildings, and systems with security in mind at the beginning of the process;
- Passive security: reduce reliance on active security and human measures to counter a security event (e.g. segmentation, limiting access paths, stronger access control…) ;
- Evolving response: the ability to provide a flexible response to changing threat levels, and security systems to meet the unknown future threats.
-

Canada has updated its regulations in 2022 [2727] to specifically address the risks of SMR remote operation.
US NRC is also in the process of updating its regulations for the same purpose [2828], [2929].

9.4. CONCLUSION REGARDING REMOTE OPERATION

Existing literature identifies that SMR remote operation will bear new cybersecurity risks or increase existing ones. The increasing use of digital technology, including new technologies, for operating SMR reactors, while employing less on-site personnel, will both increase the attack surface and reduce the resilience of the system against a cyber-attack. SMR reactors will particularly be sensitive to insider threat and supply chain attacks.

To mitigate this risk, both technical (testing new technologies versus cyber risks, ensure air gap…) and organizational measures (employee screening) shall be strengthened. A particular focus is made on the Defensive Computer Security Architecture (DCSA) concept which gives guidance for building a computer network architecture both enabling remote operation and strongly reducing risks of cyber attacks linked with such a remote operation. At least two different architecture designs have been presented so far, by CNL and IRSN, for implementing the DCSA approach in a remote operation context.

Several countries have adapted their regulations, or are in the process of doing so, to add requirements so that SMR designers take protective measures against cyber threats in the frame of a Secure by Design approach.

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

10. POTENTIAL SMR SPECIFIC CYBER SCENARIOS LINKED TO THE LITERATURE REVIEW

10.1. CYBERSECURITY SCENARIOS RELEVANT TO MULTI-UNIT OPERATION

Based on the results of literature review and taking into account the specific features, described identified at §8.4, the following attack scenarios connected with multi-unit specificities can be defined:

- Simultaneous cyber-attack against a few or all SMR units/modules. I&C systems and software are identical for all SMR units/modules. This creates aggregated risks, increasing the vulnerability of all these I&C systems to the same cyber-attack. Thus, attackers can use I&C systems vulnerabilities for successful cyber-attack affected a few SMR units/modules due to a common point of failure.
- Cyber-attack can spread from one SMR units/modules to others through the shared communication lines.
- Cyber-attack against one or a few SMR units/modules and necessity of keeping of normal operation of other SMR units/modules. Such situation leads to increasing of workload of limited operational staff.
- Workload of operational staff sufficiently increases in case of cybersecurity attack against one or a few SMR units/modules and simultaneous incident or accident at another SMR unit/module. Such situation may require additional human resources for adequate response. Possible influence of different types of cyber-attacks when SMR units/modules are in different modes or conditions. For instance, first unit/module is in normal operation mode, second unit/module is in maintenance mode and third unit/module is under construction/installation. Different modes can make units/modules more vulnerable to different types of cyber-attacks.

10.2. CYBERSECURITY SCENARIOS RELEVANT TO REMOTE OPERATION

Based on the main risks linked with remote operation identified at §9.1, the following attack scenarios taking advantage of remote operation specificities can be defined:

- Taking advantage of remote connections between the SMR reactor and the remote control room, an attacker may connect to the SMR I&C system and send malicious commands to the reactor. Such commands may range from a simple shutdown to more aggressive commands activating/deactivating various systems and potentially inducing an incident or accident scenario at the plant. The consequences of such a scenario may be worsened by the fact that more mitigation means will be digitally controlled and by the ability of the attacker to interact with them.
- An attacker placing himself in a Man-in-the-middle position between the SMR reactor and the remote control room may block the control room from sending commands to the reactor, or may change them, and may alter the information sent back from the reactor to the control room, misleading the operators and preventing them from applying the required procedures depending on the state of the reactor.
- Taking advantage of remote connections between the SMR reactor and the remote control room, an attacker may connect to the physical security systems of the plant, including cameras, access control etc… In the framework of a hybrid scenario, the

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

attacker could use his connection to such systems to blind the control room and to open the way to on-site attackers aiming at stealing nuclear fuel or at sabotaging the plant.
- In the frame of an insider threat scenario, an attacker acting in the control room may send malicious commands to a reactor (or several reactors when combining since scenario with a multi-unit scenario defined in §10.1) with various consequences described in the previous scenarios. The chances of such malicious actions not being detected may be increased by the reduced size of the operating team and the fact that it will have to manage several reactors at a time.
- In a hybrid scenario, an attacker with physical access to the I&C of one of the local unit may try to compromise the multi units control room to pivot and spread to the other modules
- In the frame of a supply-chain attack, an attacker may plant malicious code in a computer system of the reactor, for example in I&C system, triggering malicious behaviour later, during plant operation. The consequences of such action may be worsened by the absence of on-site personnel.

11. Conclusion

The present literature review has been performed to provide an overview of the current state of regulations, guidelines, and standards relating to SMR cybersecurity. It has been limited by a few key factors:

- From an I&C architecture perspective, the designs are still at a preliminary stage, with the only specific features identified as having an impact on the cyber attack surface being multi units control rooms and remote operation.
- There is no feedback from experience in the nuclear field and, ultimately, very little in related fields.

However, existing literature already identifies that multi-unit operation will increase cybersecurity risks for SMRs: extended use of automated I&C systems, based on new technologies including AI, tighter integration of I&C systems over multiple units, increased variety of technologies among the systems operated from a single control room and increased complexity of operation will provide new attack paths to attackers.
Similarly, existing literature already identifies that remote operation will increase cybersecurity risks for SMRs: the new operating procedures introduced by the SMRs will increase the attack surface and the reduced or even absence of local staff for operation will increase the difficulty to act without remote link. SMR reactors will particularly be sensitive to insider threat and supply chain attacks.
Existing literature also provides first pieces of advice to mitigate these risks, by taking into account cyber security in the design of both the reactor computer systems and the way it will be operated. A particular attention should be paid to architecture in order to preserve the principles of defence in depth, for example based on the Defensive Computer Security Architecture (DCSA) concept. First architecture designs compliant with this concept have been presented by Canada and France to tackle the cyber risks induced by remote operation.
In parallel, some countries (Canada, USA) have started adapting their regulations to consider cyber threats in a remote operation context.

Literature also points out the need for a thorough testing of future SMR computer systems and presents some tools already available to perform such tests.

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

Based on these findings, the present document provides examples of attack scenarios in which an attacker would take advantage of the weaknesses induced by multi-unit operation and remote operation of SMR reactors. Such scenarios could be explored in connection with the simulator experiments that will be carried out as part of WP5/T5.1.

12. Bibliography

1. *Brookhaven National Laboratory BNL-96816-2012-CP «Multi-unit Operations in Non-nuclear Systems: Lessons Learned for Small Modular Reactors». USA, 2012. 11 pages.*
2. *Safety of nuclear power plants: design. IAEA safety standards series No. SSR-2/1 (Rev. 1). International Atomic Energy Agency. Description: Vienna, 2016. 75 pages.*
3. *Advances in small modular reactor technology developments. A Supplement to: IAEA Advanced Reactors Information System (ARIS), 2018 Edition. 250 pages.*
4. *Advances in small modular reactor technology developments. A Supplement to: IAEA Advanced Reactors Information System (ARIS), 2020 Edition. 343 pages.*
5. *Technology roadmap for small modular reactor deployment. IAEA Nuclear Energy Series No. NR-T-1.18. International Atomic Energy Agency, Vienna, 2021. 109 pages.*
6. *Terms for describing advanced nuclear power plants. IAEA Nuclear Energy Series No. NR-T-1.19. International Atomic Energy Agency, Vienna, 2023. 19 pages.*
7. *Applicability of IAEA safety standards to non-water cooled reactors and small modular reactors. IAEA Safety Reports Series No. 123. International Atomic Energy Agency, Vienna, 2023. 277 pages.*
8. *Design safety considerations for water cooled small modular reactors incorporating lessons learned from the Fukushima Daiichi accident. IAEA-TECDOC-SERIES-1785. International Atomic Energy Agency, Vienna, 2016. 140 pages.*
9. *Lessons learned in regulating small modular reactors. Challenges, resolutions and insights. IAEA-TECDOC-SERIES-2003. International Atomic Energy Agency, Vienna, 2022. 506 pages.*
10. *Instrumentation and control systems for advanced small modular reactors. IAEA Nuclear Energy Series No. NP-T-3.19. International Atomic Energy Agency, Vienna, 2017. 95 pages.*
11. *Human Factors Considerations for Remote Operation of Small Modular Reactors// Claire Blackett1 et al. 13th Nuclear Plant Instrumentation, Control & Human-Machine Interface Technologies. (NPIC&HMIT), San Diego, CA, July 15-23, 2023. 10 pages.*
12. *Advanced I&C for Fault-Tolerant Supervisory Control of Small Modular Reactors. Final progress report DE-NE0000739. Dr. Daniel G. Cole. University of Pittsburgh, 2018. 24 pages.*
13. *Human Performance in Operation of Small Modular Reactors// Claire Blacketta, et al. Probabilistic Safety Assessment and Management (PSAM 16), Honolulu, Hawaii, June 26-July 1, 2022. 10 pages.*
14. *Small and modular reactors. Instrumentation and control systems and control rooms. Specific Features. IEC TR 63335. International Electrotechnical Commission (IEC), 2019. 21 pages.*
15. *Simulator of small modular reactor for cyber security assessment// Busquim E Silva et al. International Conference on Nuclear Security: Shaping the Future - Vienna International Centre (VIC), Vienna, Austria, May 20-24, 2024. 6 pages.*
16. *Wavy-attention network for real-time cyber-attack detection in a small modular pressurized water reactor digital control system// Ayodeji et al. Nuclear Engineering and Design 424, 2024. 16 pages.*
17. *Computer Security for Small Modular Reactors and Microreactors // R. Busquim e Silva et al. 2023 INMM & ESARDA Joint Annual Meeting. May 22, 2023. 8 pages.*
18. *Cyber Security at Civil Nuclear Facilities: Understanding the Risks, D. Livingstone, C. Baylon, R. Brunt, Chatham House R. Inst. Int. Aff., 2015*

Co-funded by the European Union
UK Research and Innovation
The Research Council of Norway
Project funded by

19. *Net-Zero Through Small Modular Reactors - Cybersecurity Considerations, Brian Aamoth et al., IECON 2022*
20. *SMR and Advanced Reactor Security: Regulatory Perspectives on Integrating Physical and Cyber Security by Design to Protect Against Malicious Acts and Evolving Threats, Raphael Duguay, Canadian Nuclear Safety Commission, International Journal of Nuclear Security, 17 Décembre 2020*
21. *Sécurité des systèmes d'automatisation et de commande industriels - Partie 3-2 : évaluation des risques de sécurité pour la conception des systèmes, IEC 62443-3-2, 2020*
22. *Centrales nucléaires de puissance - systèmes d'instrumentation et de contrôle-commande – Exigences relatives aux programmes de sécurité applicables aux systèmes programmés. Ed.1.0, IEC62645, 2014*
23. *Computer Security Techniques for Nuclear Facilities, Nuclear Security Series No 17-T (Rev.1), AIEA, 2021*
24. *Computer Security of Instrumentation and Control Systems at Nuclear Facilities, Nuclear Security Series No 33T, AIEA, 2018*
25. *Definition of Architectural Structure for Supervisory Control System of Advanced Small Modular Reactors, ORNL/TM-2013/320, SMR/ICHMI/ORNL/TR-2013/04, ORNL, Août 2013*
26. *Remote Monitoring and Control of a SRM, Proof of Concept, Dave Trask, Canadian Nuclear Laboratories, IAEA Technical Meeting on Instrumentation and Control and Computer Security for SMR and Micro-reactors, 24 Février 2024.*
27. *Cybersécurité pour les centrales nucléaires, N290.7-F21, CSA, 2022*
28. *NRC regulatory efforts for cybersecurity of advanced reactors, T. RIVERA and I. GARCIA, ICONS2024*
29. *Micro-Reactor Licensing and Deployment Considerations: Fuel Loading and Operational Testing at a Factory, Enclosure 1, SECY-24-0008, NRC, 8 Février 2024*
30. *Cybersecurity matter for remote access of SMR, O. D'Hénin, O. Fichot, A. Benoit-rosario, IAEA International Conference on Small Modular Reactors and their Applications, Octobre 2024*