# Computer Security for Small Modular Reactors and Microreactors

**Rodney Busquim e Silva**
**International Atomic Energy Agency**
r.busquim@iaea.org

**Robert Anderson**
**Idaho National Laboratories**
robert.anderson@inl.gov

**Paul Smith**
**AIT – Austrian Institute of Technology**
paul.smith@ait.ac.at

**Mike St. John-Green**
**Cyber Specialist**
mike@stjohn-green.co.uk

## Abstract

This paper 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. In the last two decades, the interest in development and deployment of small modular reactors and microreactors has increased due to many driving forces, but of primary interest for computer security are those associated with the innovative attributes taking advantage of advances in digital technologies. Such attributes include, digital instrumentation and control, increased digital automation, and remote monitoring and supervisory control that may lead to improvements in the overall plant capacity factor; the capability of increasing installed capacity within a relative short time; and the lower capital cost compared to traditional nuclear power plants among others. Such features reinforce the need for instrumentation and control solutions and computer security measures being considered and maintained during the entire small modular reactors and microreactors lifecycle, from design to operation to decommissioning. Innovative small modular reactors and microreactors attributes may introduce unintended vulnerabilities to cyber-attack, for example, the need for secure communications between the local control room and remote operation and maintenance centers; the use of mutualized plant systems with digital technologies new to the nuclear industry, e.g. smart sensors and inferred process measurements; and strategies for modular construction with a more complex digital supply chain. The IAEA has been discussing with the international nuclear community these key computer security aspects and challenges related to the application of digital instrumentation and control and emerging digital technologies in the design and deployment of small modular reactors and microreactors. As participants in these discussions, in this paper, we highlight some of the key themes that have emerged from these discussions.

Key words: small modular reactors, microreactors, cybersecurity, computer security, instrumentation and control.

## 1. Introduction

In the last decade, the global interest in the development and deployment of small modular reactor (SMR) and microreactors (MR) has increased. SMRs are advanced reactors that may be deployed as a single or multi-module plant, and are designed to be built in factories and shipped to utilities for installation as demand arises. They have advanced engineered features, should generate up to 300 MWe of electric power, and they include not only water-cooled reactors, but also high temperature gas cooled reactors, liquid metal cooled reactors, molten salt reactors among others. MRs are also advanced factory-built reactors designed to provide up to 10 MWe and that can be easily transported to provide reliable heat and power in remote areas and small power grids.

SMR/MRs offers an opportunity to meet the world's needs for increased energy generation capacity, delivering electricity in remote locations and in developing countries, producing heat, hydrogen and desalinated water among others. One of the challenges for the near-term deployment of SMRs and MRs is how to accelerate their technology development and demonstrate the level of readiness for nuclear applications, while maintaining high compliance with standards for safety and security, integrating those requirements, together, into the design of the instrumentation and control systems from their inception.

The IAEA Advances in Small Modular Reactor Technology Developments [1] booklet lists more than 70 SMRs and MRs designs under development. The SMR/MRs driving forces include better economics, power generation closer to the consumers replacing fossil fuel plants, and the need to generate flexible power for remote areas or hybrid renewables/nuclear energy systems. The nuclear industry interest in the development and near-term deployment of SMR/MRs presents some challenges for instrumentation and control and computer security. This includes, for example, the challenges of innovations that rely on digital technologies necessary for reactor remote operation, of using smart sensors and wireless protocols for I&C communications, use of artificial intelligence-based tools and digital twins to maintain safety and security.

The IAEA has been organizing consultancy meetings, technical meetings and workshops, such as the *Technical Meeting on Instrumentation and Control and Computer Security for Small Modular Reactors and Microreactors* (Vienna, Austria, 2022) and the *International Workshop on Instrumentation and Control, and Computer Security for Small Modular Reactors* (Paris, France, 2023), to identify gaps, share information and discuss the role of digital I&C and innovations in digital technologies, and computer security aspects, for SMR/MRs. These events have been organized jointly by the IAEA Department of Nuclear Safety and Security and the IAEA Department of Nuclear Energy.

## 1.1. Key SMR/MRs Enablers Driving SMR/MRs Development

There are many aspects driving the increased interest in SMR/MRs. The new innovative SMR/MRs designs have been developed to be economically competitive with other power generation technologies while considering the global international market. Some of the key driving forces are:

a) Capacity to address climate change. Nuclear power is one of the best options to meet the need to limit the rise in global temperature by providing baseload and reliable production of electricity. SMR/MRs offer an option to replace fossil fuel-based thermal power plants (mainly coal, oil, and natural gas), including in a load-following demand scheme.
b) Lower costs when compared with nuclear power plants (NPPs). An improved economy of scale is expected based on the SMR/MRs modularity and scalability, smaller site footprints, and reduced need for on-site staffing due to higher automation. This will require new I&C designs, embracing non-nuclear digital technologies new to the nuclear industry while demonstrating their level of readiness for nuclear applications and the compliance with standards for safety and security.
c) Modular standard construction framework. A modular framework allows for improvements in the overall plant capacity factor as SMR/MRs are expected to be quicker and more flexible to deploy than traditional NPPs. A modular standard construction framework also presents opportunities for electricity generation in remote areas, and in locations that require reliable power for electricity production and applications such as desalination, hydrogen production, process heat among others. SMR/MRs will also be able to better integrate with intermittent sources of power (for example, wind and solar) through smart connections to the grid.
d) SMR/MRs international market. SMR/MRs have been designed for an international market to improve the economy of scale by increasing SMR/MR production and thereby reducing costs. An international market requires more engagement between developers and regulators to ensure

SMR/MRs can earn and maintain the confidence of the public, while keeping project risks for potential investors within viable limits

e) Advances in nuclear technology. While SMR/MRs designs are adopting passive safety features, they are also anticipating advances in digital I&C technology and architectures. Such SMR/MRs are likely to need enhanced safety, security and proliferation resistance in design, construction, transportation, assembly and operation because of the increased attack surface of SMR/MRs.

## 2. SMR/MRs Innovations Driving Computer-based Systems Solutions

There are a large number [1] of SMR/MRs concepts under development with different design maturity levels. The most mature SMR/MRs concepts are based on light water reactors (LWR) Generation III/III+ designs, such as evolutionary integrated SMRs, which benefit from more than five decades of operating experience of LWRs. Generation IV SMR designs use non water coolants such as liquid metal, gas or molten salt, adopt new system configurations and use advanced fuels. Generation IV concepts have been object of extensive research over the last decades although they lack operating experience and will prompt a review of current regulations.

To be economically viable, Generation III+ and Generation IV SMRs designs must have a higher degree of modularization, with more in factory manufacturing, and their safety and security systems must be simplified. In addition, the deployment of SMR/MRs may require mutualized control rooms, with on-site reduced staffing, and they may require remote support centers for monitoring and supervising normal plant operation. In addition, the small SMR/MRs core sizes, and their unique environmental conditions (e.g. high coolant temperature), present challenges in terms of sensors, actuators, data communications and reliability of analogue and digital systems that are usually located outside the reactor core of traditional NPPs.

SMR/MRs designs and construction rely on advanced manufacturing, modelling and simulation, that rely upon processes that are controlled by computer-based systems. Because the deployment of SMR/MRs will take advantage of modularity and increase the use of industrial fabrication capacity to reduce deployment times, the SMR/MRs supply chain will be tightly integrated with the plant deployment, and operators may have less visibility into vendor and developers' practices.

### 2.1. Control Room Architectures

SMR/MRs are driving advances in control room architectures that reflect remote operations and possibly even autonomous operations. SMR/MRs may be deployed as multiple units with a control room that share systems and functions between them. Yet those units may not be identical, with design and operational dissimilarities, deployed over time. Therefore, SMR/MR 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. There will be new human factors considerations about the basis on which operators trust the information presented to them.

SMR/MR control rooms are being designed to operate in integrated nuclear and renewable energy systems, and innovative control rooms designs will be essential to improve efficiency of power production, enhance load-follow capabilities, and for maintaining grid stability. These control room architectures may have new failure modes and provide new attack surfaces for malicious action.

### 2.2. Remote Operation

Remote operation is likely to be central to the financial viability of SMR/MRs. SMR/MRs that are designed to run in isolated locations, or where economic restrictions prevent significant numbers of on-premise staff, will still require constant and reliable monitoring (i.e. allowing an overview of parameters and significant variables for the operation without modifying or setting any value) and supervising (i.e. allowing access to the plant processes and interaction with controllers that alter them).

Remote actions may be performed with different degrees of control over the plant operation, with different operational and organizational boundaries. Not all control functions are susceptible to remote control: the communication delay, network latency and need of cryptography may be unacceptable in some cases.

Remote control of a SMR/MRs implies a trust relationship between the plant site and the remote connection. The nature of the trust, how it is established and assured are essential for the safe and secure design and plant operation.

## 2.3. Autonomous Operations

Innovative SMR/MRs designs may have a degree of autonomous operation. Autonomous control systems are computer-based tools that use model-based engineering, AI/ML for example, that can be explained as intelligent systems with self-governance ability to perform and execute control functions, and their degree of autonomy depends upon the extent to which it can perform forecasting, fault diagnosis, decision-making and planning. Some MR developers are looking at techniques that can be adopted to make them locally fully autonomous with the ability to monitor and make operational interventions from a remote location.

The strategies and control architectures for autonomous operation will require considerable analysis to assure that they are safe and secure, based on a model of trust relationships.

## 2.4. Safety-related Systems Simplification

The safety-related I&C systems that perform protection functions should be kept as simple as possible. This simplification is made by incorporating passive safety systems, an improvement of Generation III reactors over Generation II, in the SMR/MRs designs, with long grace periods before physical interventions may be needed.

The non-safety-related I&C systems that perform control functions should in contrast be capable of gathering, storing, processing and sharing the large amount of information that designers expect will be needed for the new SMR/MRs designs to operate cost-effectively and energy-efficiently. Therefore, SMR/MRs will use multiple I&C systems that may be interconnected in various ways, for reactor safety, reactor control, plant control, plant health monitoring, and remote supervising among others.

## 2.5. Smart Sensors and Programmable Hardware

The SMR/MRs innovations being considered in both Generation III+ and IV designs may lead to the adoption of emerging industrial standards, such as secure protocols like OPC Unified Architecture (OPC-UA) and smart sensors, and digital innovations like digital twins (DT). The economic viability of SMR/MRs may also rely on the use of wireless communications and programmable hardware, such as Field Programmable Gate Arrays (FPGAs).

Today’s sensors and transmitters used in the nuclear industry, including smart sensors that are capable of self–diagnostics, are based on conventional sensing technologies. For SMR/MRs operation, these sensors must be adapted or developed to operate in significantly more cramped or inaccessible spaces that restrict maintenance access. Instrumentation must be rugged enough to handle not only the high temperatures and high pressures (in some advanced reactor designs) but also the long-term effects of the coolant on the sensor interface.

FPGA-based safety systems have been considered because these reduce or remove run-time programmability and software-based decision-making in I&C systems. Application Specific Integrated Circuits (ASICs) may offer more secure operation in some respects, but ASICs limit the flexibility for minor design changes and can be significantly more expensive.

### 2.6. Digital Twins and Test Beds

Autonomous operation may rely upon a DT of the SMR/MRs against which real-time sensor data is compared to devise the appropriate I&C control actions, in order to operate the SMR/MR optimally and within its design basis. A DT is the virtual representation of a system that matches its physical counterpart over its life-cycle, and allows process knowledge to be readily accessible. A DT may use real-time data from sensors, and information from other sources, like historians, to maintain its model and enable learning, driving reexamination of actions being performed, or to estimate a system´s future state [2]

Testbeds may help to identify problems that may not be evident during initial design. An SMR/MR testbed may include a computer simulation, which may be similar in nature to a DT. Testbeds are also useful for various testing, research, and training activities.

### 2.7. Artificial Intelligence and Machine Learning (AI/ML)

Artificial intelligence refers to a collection of technologies that produce systems capable of tracking complex problems in ways similar to human logic and reasoning, while machine learning technologies learn how to complete a particular task based on large amounts of data [3]. These two terms may be interpreted differently by different audiences, but AI/ML will be used to encompass all related techniques in which algorithms make decisions that are influenced by data, which means that the behavior of the algorithm changes over time (it learns), which in turn can lead to a lack of determinism.

Because of AI/ML's perceived lack of determinism, there will be some uses that are not currently acceptable, such as protection systems and some reactor control functions. AI/ML could be used to support facility decision-making activities or for the detection of malicious activity but is unlikely to be applicable to all such problems. Therefore, the acceptable use of AI/ML must be clearly defined and bounded with acceptable levels of risk.

## 3. SMR/MRs Computer Security Challenges

The increased digital automation, unique environmental conditions, remote supervisory control and remote maintenance, with reduced on-site staffing, reinforces the need for digital instrumentation and control (I&C) solutions and computer security measures being considered and maintained during the entire SMR/MRs lifecycle, from design to operation to decommissioning.

### 3.1. Remote Operations

Two-way communications will be required between security zones of the physical SMR/MR facility and a potential support center for remote operations. This need of exchange of information may introduce pathways that can be exploited by adversaries, therefore requiring robust security considerations applied to the communication infrastructure. Current systems that are responsible for remote monitoring and supervising are limited by communication technologies, and this will place stringent requirements on both I&C and computer security, which must be integrated into the SMR/MRs I&C design.

If operational data needs to be supplied continuously to off-site control rooms and organizations that will be monitoring and supervising reactor operations, the confidentiality, availability and integrity of that information must be protected.

## 3.2. New Digital Technologies

There are many computer security challenges related to new digital technology. For example, the small size of sensors and actuators (analog and digital) in an integrated core environment of an SMR, the two-way communications segregation, and the possible adoption of an OPC-UA-based protocol (new to nuclear industry) will demand computer security assessment for SMR/MR environments and the development of computer security measures while maintaining safety standards.

In addition, the data transfer rates will need to accommodate new I&C technologies, with limited processing capacity, which may create inconsistences in data synchronization. The synchronization may be an issue for the application of computer security requirements.

The limitation in physical space (reduced cabling space) may increase the demand for secure wireless technology that may help monitoring the dynamic behavior of the plant. The use of wireless technology for safety-related applications must be well understood, and adequate computer security measures must be in place.

FPGAs are being considered as an option for safety systems as they reduce or remove run-time programmability, but FPGAs still exhibit vulnerabilities, including in the way that they are manufactured and programmed, and these vulnerabilities need to be fully understood and mitigated.

## 3.3. Artificial Intelligence and Machine Learning

The use of AI/ML based systems may increase the potential for cyber-attacks in different ways.  One way is by compromising the software-based algorithms or the data needed for AI/ML training that may rely on databases or simulation tools that may be compromised.  These systems may be subject to code injection during the development process, during delivery and software installation, for example, by feeding them intentionally corrupted data. The challenge overall is how to produce sufficient transparency over behaviors of the AI/ML algorithms and provide ongoing assurance on the correctness of their behavior.

The use of advanced real-time diagnostics and prognostics tools have the potential to reduce some risks due to greater understanding of plant systems conditions, which could indicate a facility process failure or a system being compromised. However, these tools will rely on computer-based systems that may themselves be target of a cyber-attack.

Any autonomous plant operation based on integrated decision making, control and diagnostics, which will depend on highly-integrated digital technology with software-based systems that access sensitive plant process networks. These will need computer security protection and the challenges are substantial.

## 3.4. Supply Chain Security

Another key aspect is the security of computer-based systems supply chain. Because SMR/MRs are being designed for remote deployment, it is expected that the construction of critical/core components will occur at various locations transported to the site for assembly. Cyber-attackers may be shifting their focus to the balance of the plant and to the (in)security of supply chain.  This will create new transportation and computer security supply chain risks.

SMR/MRs rely on advanced manufacturing, modelling and simulation, and advanced materials that rely upon processes that are controlled by computer-based systems. Supply chain attacks could target one or more of these critical components of SMR/MR fabrication to impact nuclear safety, security and reliability.

As the deployment of SMR/MRs will likely take advantage of modularity and increase the use of industrial fabrication capacity, there may be a pressure to use commercial off-the shelf (COTS) computer-based technology to reduce construction times. All these computer security related challenges have to be addressed. The security of the supply chain of these COTS products may be hard to assure.

The acquisition methods with greater off-site modular construction and assembly, relying on technologies and techniques new to traditional NPPs, will present new challenges over the maintenance of all the computer-based systems and it will require clarification over who owns the risks.

### 3.5. Integration of Safety and Security

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/MRs. Such a systems approach is described in detail elsewhere [4] [5].

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. Especially challenging are potential security events that may require the security system 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 defense in depth for computer security. Multi-unit supervisory control systems deployed in fleets consisting of different generations 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.

## 4. Conclusion

The use of new digital technologies can enhance the efficiency of operations and maintenance of SMR/MRs. For example, plant status can be available to the operator, plant performance can be provided to the corporate operations, and component or systems health status can be available to maintenance staff. It also can provide real time monitoring and prognostics that may indicate a component or system failure. By reducing cable installation costs, or allowing remote or autonomous operation, or by increasing plant availability and reducing staff requirements, it may also reduce operating costs.

However, there are many challenges that must be addressed in Generation III+ and Generation IV SMR/MRs. For example, remote operation requires communication links that may be not under the direct control of the facility operator. They will result in communications channels that are more susceptible to security threats, including physical and cyber-attacks. An operator would need to consider how such communication links could be protected and the potential consequence that could result were these communication links compromised

In addition, the deployment of mutualized control rooms to operate many SMR/MRs units will increase complexity of the integrated network and of human factors; it will need the implementation of an adequate defensive computer security architecture [6]. This will probably require a greater operator dependency on supporting tools, which may rely on AI/ML or even DT. This dependence implies more computer security concerns related to the safety systems. The use of DT for improving safety and security may require the development of computer security strategies to assure protection against compromise during the supply chain. New supply chain security controls may be also needed to manage new digital acquisition methods with greater off-site modular construction and assembly.

## References

[1] INTERNATIONAL ATOMIC ENERGY AGENCY. Advances in Small Modular Reactors Technology Developments, IAEA Advanced Reactors Information System (ARIS), IAEA (2020).

[2] R. Busquim e Silva et al. Integration of the Asherah NPP Simulator into a Closed-Loop Digital Twin Environment for Cybersecurity Assessment. 12th NPIC&HMIT (2021).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Artificial Intelligence for Accelerating Nuclear Applications, Science and Technology, Non-serial Publications, IAEA, Vienna (2022).

[4] National Cyber-Informed Engineering Strategy. https://www.energy.gov/sites/default/files/2022-6/FINAL20 DOE %20 National%20CIE%20Strategy%20-%20June%202022_0.pdf. Accessed on 09 May 2023.

[5] System-Theoretic Process Analysis (STPA) Handbook. https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf. Accessed on 09 May 2023.

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security Techniques for Nuclear Facilities, IAEA Nuclear Security Series No. 17-T (Rev. 1), IAEA, Vienna (2021).