INSIDER THREAT SECURITY CONSIDERATIONS FOR ADVANCED AND SMALL MODULAR REACTORS

Z. S. HOMAN
King's College London
London, United Kingdom of Great Britain and Northern Ireland

R. PEEL
King's College London
London, United Kingdom of Great Britain and Northern Ireland
Email: ross.peel@kcl.ac.uk

Abstract

The wide range of nuclear power plant technologies currently in design globally have an assortment of unique characteristics that create novel security considerations compared to large conventional nuclear power plants. Some of these characteristics create "insider threat" considerations for nuclear security, where insiders are defined as individuals with legitimate access to nuclear facilities and materials who use this access to carry out sabotage or theft of nuclear material. These include a lack of mature security culture in developer organisations, serial plant manufacturing in a production line environment, plant siting in remote and isolated areas, minimised staff numbers, teleoperation of plants by offsite staff, the increased reliance on digital instrumentation and control systems, and the potential for greater involvement of foreign experts and third-party suppliers, especially on short-term bases for, e.g, refuelling and maintenance. The paper takes a technology agnostic approach to examine what these factors may mean for insider threat risks and suggests that plant designers should be identifying and minimising the opportunities of insiders to act throughout the engineering design process. Doing so is anticipated to strengthen effective insider threat mitigation in deployed small and advanced reactors.

1. INTRODUCTION

Modular Reactors (MR) are being considered today by a range of states to help meet their energy needs due to the range of potential benefits they offer, including low carbon heat and power generation, enhanced energy security compared to variable renewable sources, claimed lower energy costs compared to large nuclear, and more [1]. MRs are a class of small nuclear fission reactors, designed to be built in a factory, shipped to operational sites for installation and then used to power buildings or other commercial operations. Many developers have suggested that they will have first-of-a-kind operational MRs by 2030, and it is predicted that by 2050 there could be 375 GWe of operating SMR capacity [2]. A commonly adopted definition for small modular reactors (SMR) is that they produce 300 MWe or less, and some MR designs do exceed this, the majority have power ratings within this limit [3], meaning that there would be ~1000 new MRs operating in 2050. Many of these may be in countries which currently have little to no experience operating nuclear energy facilities or handling nuclear materials, lacking well-developed cultures, processes and frameworks for nuclear security.

Nuclear security seeks to protect nuclear facilities from sabotage and nuclear materials from unauthorised removal. It addresses three broad categories of threat: physical threats such as terrorist groups entering the site by force and/or stealth, cyberattacks on computer systems, and unauthorized actions taken by 'insiders'—staff members, contractors, and others with authorized access to sensitive areas, materials, and/or information. Insiders may have access to multiple security layers, understand system vulnerabilities, can gather intelligence and plan over extended periods, and are trusted within the organization. This allows them to act without detection potentially indefinitely. Nearly all historic cases of nuclear theft and sabotage have involved insiders or their assistance [4].

Complex threats may combine more than one category, for instance, by using a compromised insider to enable a cyber and/or physical attack. This paper focusses on the insider threat to MRs, how the risks from insider threats are different for MRs as compared to large conventional nuclear power plants, and how these threats can be mitigated.

MRs will have numerous features that create novel security considerations to be managed, stemming from their smaller size and modular manufacture, their designers' focus on economics, the greater use of automation and/or remote operation, the wide range of advanced technologies, fuels, and materials planned, the greater array

of siting and deployment options, and the increased diversity of technology developer organisations [5]. Some of these differences have the potential to enhance insider threats if not properly managed. However, as many of these MRs are currently in their design stages, developers are ideally placed to take account of insider threat mitigation during design. This security-by-design approach has to potential to radically reduce or eliminate security risks if properly considered [6].

The remainder of paper is structured as follows. First, current approaches in insider threat mitigation will be described, as applied to currently operating nuclear facilities. Then, a series of interconnected novel features of MR that create security considerations relevant to insider threat will be examined. Following this, modifications to insider threat mitigation approaches will be suggested to address the novel insider threat risks, before the paper is concluded with a recommendation that MR developers seek to design out insider threat risk, and particularly ensure that it is not merely transferred as a computer security risk.

2. CURRENT APPROACHES IN INSIDER THREAT MITIGATION

2.1. Security culture

Traditional approaches to nuclear facility security have depended heavily on human performance to prevent both deliberate and accidental incidents. Accordingly, experts have increasingly underlined the critical role of people and organisational culture in delivering effective security [7]. The IAEA defines nuclear security culture as the "assembly of characteristics, attitudes and behaviour of individuals, organizations and institutions which serves as a means to support and enhance nuclear security." [8] An awareness of the so-called 'insider threat' is crucial in developing and maintaining a strong security culture. Insiders may be motivated to conduct unlawful activities for a number of reasons, ranging from a malicious intent to cause harm to the public, to coercion by threat of violence against the insider, to an offer from a third party to help the insider escape outstanding financial debts, to disgruntlement with management, and more. Insiders may even be non-malicious and unwitting in their role [4]. An effective security culture should seek to address the full range of insider motivations.

2.2. Vetting

One of the main activities any nuclear organisation will undertake to prevent insider threat is vetting, i.e., thoroughly assessing the background, qualifications, and various risk factors associated with an individual to determine whether the risks associated with granting them access to sensitive areas, materials and/or information are sufficiently low. This applies especially to new personnel but can also be repeated periodically for existing personnel to detect any changes in their risk factors.

Vetting can be done with various levels of detail and intrusiveness, and many nuclear facilities implement a tiered security clearance system to ensure that only the most trusted individuals with the lowest overall risk are given access to the most sensitive information and areas. With that said, any level of vetting will almost always include conducting comprehensive background checks to uncover risk factors, such as past criminal activities, financial issues, and histories of coercion, blackmail, or susceptibility to external pressures, including past relationships. Reviewing an individual's employment history can expose patterns of concerning behaviour, gaps in employment, or reasons for leaving past jobs that might indicate potential issues. Rigorous identity verification processes, including evaluation of educational qualifications, certifications, and professional licenses, will help to confirm that applicants are who they claim to be. Finally, psychological evaluations and behavioural screenings are used to attempt to identify personality traits or mental health concerns that may worsen insider threat risks, gauge resilience to stress and susceptibility to manipulation, and uncover extremist beliefs or associations with radical groups. Consequently, vetting procedures play a critical role in mitigating risks to nuclear facilities, materials and associated sensitive information [9].

2.3. Access control

The next step to mitigate insider threat risk is to manage the access rights of individuals to sensitive facilities, equipment, materials, information, and so on. While it is common to primarily associate access control measures with physical protection rather than insider threat mitigation, compared to attacks by unauthorized individuals, insiders will often only need to defeat the comparatively small number of security measures that their

existing access does not allow them to bypass. Well known factors that enable insiders to gain this access include organisational biases that underestimate insider risks, such as the "halo effect" where well-liked individuals are assumed to be trustworthy, and a lack of positive incentives or perceived negative consequences for reporting suspicious behaviour, often resulting in complacency and reluctance to act on red flags. Many organisations also struggle with fragmented responsibility across different managerial roles – with past cases illustrating instances where extreme warning signs were overlooked or disregarded due to organisational inertia [4].

Particular strategies to prevent malicious insider access already exist [10]. For instance, the use of physical barriers such as locked doors, fences, and biometric access controls can restrict entry to high-security zones to only those individuals who require such access to carry out their duties [11]. Besides this, nuclear facilities benefit from implementing role-based access control ensures that personnel have access only to the areas necessary for their specific job functions. Similarly, computer security measures are commonly used that limit each user to the activities and information necessary for their role, and do not give complete or broad access for all users [12]. Going a bit further, it may be appropriate to implement continuous monitoring of personnel behaviour and activities within the facility using CCTV cameras and access logs. Significantly, a dual-control principle for handling nuclear material ensures that no single individual has sole control over sensitive materials or processes. Regular and rigorous inventory checks and audits of nuclear materials help detect discrepancies or unauthorised removals promptly. Integrated tracking systems and real-time monitoring can enhance accountability and prevent insider theft or diversion attempts.

2.4. Human reliability programmes

Lastly, but perhaps most importantly, MR designers must consider the role of Human Reliability Programmes (HRPs). HRPs are systematic processes designed to ensure that personnel working at nuclear facilities and/or with access to nuclear materials are trustworthy, reliable, and fit for duty [13]. Like vetting, components can include:

- Background checks (criminal, financial and employment history);
- Psychological evaluation (to determine mental and emotional stability);
- Drug and alcohol testing (to assess whether employees are affected by substances that can impair performance or may be coerced by exploitation of addiction);
- Fitness for duty assessments (of physical and mental health, but also, e.g., following events such as accidents or personal crises);
- Behavioural observation (monitoring staff behaviour, ensuring there are clear procedures to address threats, identify patterns, and identify concerns).

Most often however, these programmes will focus on training and education on safety and security protocols, the importance of vigilance, preventing complacency, and the recognition and mitigation of human errors. HRPs strengthen nuclear security culture by promoting accountability (fostering an environment in which people are both aware of and feel responsible for their actions), enhancing trust amongst staff (underlining integrity and communal expectations) and improving communication (e.g. facilitating the reporting of suspicious or concerning behaviour without fear of reprisal).

3. NOVEL FEATURES OF MODULAR REACTORS THAT AFFECT INSIDER THREAT RISK

3.1. Factory production of modular reactors

As compared to large conventional nuclear power plants which are largely constructed at their deployment site, MR developers aim to manufacture complete or largely complete nuclear power plants in factory environments, and transport these as modules to deployment sites by rail, road and/or water [1]. In such factories, workers will have access to the nuclear equipment as it is assembled, potentially throughout the entire process, allowing them to access nuclear equipment in a highly vulnerable state. Insiders could sabotage nuclear equipment in a very wide range of ways during this time, and potentially also access nuclear materials if the MR is fuelled before being relocated to its deployment site. This risk also exists for large conventional nuclear power plants,

where more complex components are often manufactured off-site and then shipped for assembly at the deployment site. However, for MRs, a much greater proportion of the assembly takes place in a factory environment, with the plant being brought to a much more complete state before relocation, centralizing the opportunities for sabotage within a single, or relatively few, location(s).

Whilst inspection and testing of finalized plants prior to commissioning and operation will help to mitigate the risk of insider sabotage during construction, such measures alone may not be sufficient to mitigate insider threat risks, and even if successful, the damage to the equipment will already have occurred. Additional suitable measures should be implemented to prevent insider sabotage, of the types discussed here, at a level appropriate to mitigate insider threat risk, although designers of both MRs and their manufacturing facilities should aim to minimize both the vulnerabilities and consequences of sabotage during the MR design process.

3.2. Progressive deployment of multiple MR units

An advantage of MR is that as each unit is relatively low in power compared to a large conventional nuclear, allowing the use of single or multiple units to deliver power at an appropriate level for a given demand, and for additional units to be added over time if demand increases. For sites with multiple units, it is possible that some security features might be shared to deliver security more economically. For example, several MRs might be located within a single building, or within a shared outer boundary fence, with common access control measures. As the number of shared measures increases, with common access between different areas, insiders are likely to have increased access to both nuclear facilities and to greater quantities of nuclear material, resulting in increased potential consequences from a nuclear security incident. Unless action is taken to separate each area, this situation will worsen if additional MR units are added to the site, due to both the transient increase in personnel with access, and the permanent increased in nuclear materials inventories. If security features are used in common, suitable measures must be put in place to mitigate enhanced security risks, including insider threat risks.

3.3. Isolated sites

One potential application for MR, largely due to their reduced size, is to provide power in isolated areas, such as in deserts, on islands, or in remote communities. Isolation presents a range of security considerations, primarily stemming from the challenge of providing on-site security staffing economically from low-power plants [14]. Isolated sites are commonly expected to be staffed by a minimal number of individuals, potentially compensated by an expanded use of automated systems, and possibly with staff located remotely from the site – these two points are discussed further below.

Being isolated may present challenges for both staff recruitment and staff mental states. Being isolated from loved ones, in an area without access to developed infrastructure, may be seen as a negative by many potential staff, leading to a reduced pool of candidates from which staff may be drawn and thus putting employers in a position where they may feel a need to compromise on some desired traits in staff and accepting higher risk individuals. Furthermore, those working at the site may find its isolation presents a lack of opportunity to relieve stress, resulting in an increased potential for insider threat activity. Taken together, isolation creates a risk of enhanced insider threat risk, which must be managed appropriately.

3.4. Remote operation

Teleoperation of MRs by staff in a centralised offsite location has been suggested to offer benefits in terms of allowing staff from numerous units to share expertise and experience, and to offer resilience in staffing across fleets of identical MRs [15]. Naturally, any control of a nuclear facility from offsite will require assured security in digital communication between the facility and offsite operators. Much of this is beyond the scope of this paper, however, human personnel will remain key in nuclear operations. Transferring personnel to an offsite location will reduce their physical access to the facility, reducing their ability to carry out many insider threat activities, but it risks in turn simply transferring these risks into the digital space. If offsite computer systems are to be used to control MR, these computers must be adequately protected both from external attacks, as well as the actions of witting and unwitting insider threats that might enable sabotage or the authorized removal of nuclear material. Centralising many staff in a location offers the potential for eased application of insider threat mitigation measures, such as behavioural observation programmes.

The question of teleoperation also raises the possibility of staff being outside of centralized locations, even working from their own homes, whilst travelling, and so on. Whilst the benefits of working remotely are enjoyed by many people today, it is questionable whether these could be available to people working within the nuclear industry with security-relevant roles. If such a scenario could be considered plausible from a computer security standpoint, there would remain an increased insider threat risk, as individuals working remotely without colleagues around them, and in the privacy of the own homes, are much more challenging to subject to monitoring.

3.5. Increased digitalisation

As suggested above, for many MR developers there in an intention to move towards having relatively few staff, a potential move to staff centralisation, remote operation, and a greater reliance on automation. These factors and more necessarily indicate that MRs will make greater use of digital information and operations technology compared to many large conventional nuclear power plants, and the plants' systems will likely need a greater degree of interconnection in order to allow for a reduction in human staffing. Interconnectivity between systems will likely streamline many processes, e.g., by bringing together data from numerous sensors to support automated analysis and decision making, but with this increasing interconnection between systems comes a greater risk of several issues. Specifically, within the insider risk context, it may enable an insider to use their access to deliver significant damage to nuclear facilities, or enable the theft of nuclear material. As with other points here, this is in large part an issue of computer security, but reducing and mitigating insider threats will reduce the ability of attackers to gain access to critical systems in the first place, hide their presence and actions, and more.

3.6. Reduced overall staff numbers

As indicated above, MR designers are often seeking to reduce staff numbers. This has the potential to bring both insider threat reductions and increases. Firstly, because with fewer individuals with access, there are fewer people who may carry out activities of security concern. Secondly, with fewer people comes the ability to focus human reliability measures on a relatively small number of individuals.

However, increased digitalization will primarily transfer human personnel away from basic monitoring functions which are more readily automated, whilst leaving higher supervisory and decision-making functions more often in the hands of human personnel. The result of this is that those personnel who remain will likely have a higher degree of trust and access, including potentially across numerous systems rather than being focused on single systems. As such, whilst the number of insiders is lower, the amount of harm each insider can do will be, on average, greater. Careful application of insider threat mitigation measures will be able to allow a balancing of the risks.

4. INSIDER THREAT MITIGATION APPROACHES FOR MODULAR REACTORS

In this section will be discussed how known insider threat mitigation approaches might be modified in light of the unique security considerations presented by MR.

4.1. Security culture for modular reactors

Over 80 MR designs have been proposed and most are currently spread across a range of stages within the design process [3]. The fraction of these being developed by experienced nuclear industry organisations is relatively low, with many instead being designed by newcomer organistions without established cultures of nuclear security. Whilst many personnel within these organisations might be nuclear engineering and other staff who understand and adopt good security practices, this is not sufficient, and these organization should take urgent steps to develop and maintain a positive security culture that pervades their work and approach. The earlier this is done, the greater the benefits will be to the organization.

In the absence of a positive security culture, the risk of insider threat action is greater, and even during the design stage of an MR's lifecycle, insiders can inflict harm. Intentionally or unintentionally, those with access to design information can share this with other threat actors, or make changes that, if undetected, will put the MR at risk of an accident or enhance the potential for the theft of nuclear material. Whilst internal and regulatory design

reviews should identify such changes, the defence-in-depth principle suggests that action should also be taken to minimize the incidence of such actions in the first place.

4.2. Vetting for modular reactors

When considering vetting for MRs, vetting will have to go beyond the traditional background checks and evaluation of technical qualifications to also cover personnel adaptability to the new technologies, operational models, and regulatory environments specific to MR systems. MRs may require personnel to perform multiple roles due to reduced staffing, especially as each staff member might have access to a wider array of systems, materials, information and so on compared to staff at large, conventional nuclear power plants delivering a comparatively narrow set of responsibilities. As such, vetting processes will have to ensure that individuals are adaptable and capable of handling the pressure of diverse responsibilities without compromising safety or security. MRs may also foster closer collaboration between personnel due to smaller teams and shared responsibilities, so vetting should cover any issues with teamwork and communication skills. Furthermore, personnel may need cross-training across various modules or units – so ideally vetting should assess aptitude for (or resistance to) learning new technologies and operational procedures. Individuals lacking these qualities may be more likely to, e.g., become disgruntled or experience excessive stress, increasing their risk of carrying out insider threat actions.

With a probable increased reliance on digital technologies, vetting will also increasingly need to focus on assessment of cybersecurity awareness and experience, both to detect individuals with the skills and/or motivation to use cyber methods to commit activities of security concern, as well as those whose lack of digital skills may result in them inadvertently creating or strengthening security risks. The latter would not necessarily prevent the person being given access, but it might suggest the need for additional training and development prior to access being given.

Notably, it has been pointed out that extensive and intrusive vetting could have an adverse effect, and result in a low-trust environment. MR designers will need to conduct benchmark studies on insider threats that consider the impact of vetting on staff confidence, satisfaction, turnover, and performance in order to find the right balance between insider threat risk mitigation achieved through vetting, and other challenges created by such vetting [16].

4.3. Access control for modular reactors

Of course, MRs will present new and unique access control issues [17]. Specifically, because MRs may consist of multiple smaller reactors operating independently or in clusters, access control systems must manage access across different units efficiently while ensuring security measures are tailored to each unit's operational status and specific security needs. Furthermore, it is anticipated that deployment of MRs may occur in stages, which would require more dynamic access control measures than conventional plants, to adapt to changing configurations and phases of construction.

It is also often suggested that MRs are more likely to be deployed in remote areas, so access control has to account for communication infrastructure limitations and differing local security regulations. At the same time, MRs may utilise centralised controls for monitoring and management – so securely connecting these remote sites to while maintaining data integrity and security will be paramount. This also ties in with robust cybersecurity measures, to protect against data breaches, and any actions that could compromise reactor operations.

4.4. Human reliability programmes for modular reactors

At the time of writing, no HRP specifically tailored for MRs was known to the authors. However, developers of new nuclear technologies and facilities can look to existing HRPs as they seek to develop their own. As most MRs as still in their design phase, developers have the opportunity to design out insider threat risks from the outset, or at least to mitigate these. Human factors are often underemphasised in the design process of new facilities, with economic factors taking a front seat. This can reduce the effectiveness and efficiency of security measures. Integrating plans for HRPs from the beginning, as recommended by international standards, can significantly improve the security of new nuclear facilities [18]. Developers have a one-time opportunity to enhance human performance using new methods, techniques and approaches, potentially resulting in lower human error probabilities and fewer human failure events compared to conventional reactors [19]. This should not be missed.

A report published by the U.S. Nuclear Regulatory Commission (NRC) over a decade ago already highlighted that existing risk assessments are insufficient for the unique challenges of MRs (such as modelling multiple units with shared systems) and identifying risk-important human actions (for example, in the scenario where one operator manages multiple SMRs) [20]. Other unique factors for MR HRPs will include consideration of the modular design and flexibility, requiring scalable and standardised training for varying configurations. The likelihood of advanced automation and digital control systems necessitate robust human-automation interface training and cybersecurity measures. Reduced on-site staffing demands cross-training for multifunctional roles and strategies for managing operator fatigue. Additionally, the potential of remote monitoring and operation capabilities must be addressed, with HRPs incorporating training on effective communication protocols between remote and on-site personnel.

5. CONCLUSION

Perhaps the most effective approach to MR insider threat mitigation would be to eliminate human access. If no individual is permitted to enter a nuclear site or induce others to do so, nor to use computer equipment to influence operations remotely, then the risk of insider threat action is effectively negated. But is this achievable? How can all the roles and functions previously fulfilled by humans be delivered? Ideally, designers would take a security-by-design approach to eliminate the need for those roles and functions from the outset, greatly reducing insider threat risk for MRs, but for many designs as currently conceived this has not been done, nor is it clear if it even can be done. However, some MR designers are attempting to achieve this – the smallest category of MR are microreactors, those with a power rating of less than ten megawatts. Such MR are also known as “nuclear batteries”, and are designed to be installed and then operate for an extended period with little to no human intervention. Simply automating all the functions previously delivered by human workers is not a true security-by-design approach, as it simply transferring the way the risk is managed from insider threat mitigation to computer security. Instead, designers should look to exclude the possibility of insider action, ideally by eliminating the possibility of any such action being taken, and if taken of it having a negative effect on nuclear safety or security. Designers should consider insiders both acting alone and in support of other threats, e.g., facilitating the access or actions of cyber and/or physical threat actors.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Technology Roadmap for Small Modular Reactor Development, IAEA, Vienna, 2021.

[2] The NEA Small Modular Reactor Dashboard, OECD Nuclear Energy Agency, Paris, 2023.

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Advances in Small Modular Reactor Technology Developments, IAEA, Vienna, Austria, (2022).

[4] BUNN, M., Insider Threats to Nuclear Security, in *The Oxford Handbook of Nuclear Security*, C. Hobbs, S. Tzinieris, and S.K. Aghara, Editors. 2023, Oxford University Press. p. 102-120.

[5] PEEL, R., FOSTER, G., and AGHARA, S., Nuclear Security and Safeguards Considerations for Novel Advanced Reactors, King’s College London, London, (2022).

[6] WORLD INSTITUTE FOR NUCLEAR SECURITY, 4.1 Implementing Security by Design at Nuclear Facilities, World Institute for Nuclear Security, Vienna, 2019.

[7] HOBBS, C. and MORAN, M., Exploring the human dimension of nuclear security: the history, theory, and practice of security culture, The Nonproliferation Review, **28** 4-6 (2021) 275-295.

[8] IAEA, Nuclear Security Culture, Nuclear Security Series No. 7, International Atomic Energy Agency, Vienna, (2008).

[9] HOBBS, C. and MORAN, M., Case Study 3: Koeberg Nuclear Power Plant – Rodney Wilkinson, in *Insider Threats—An Educational Handbook of Nuclear & Non-Nuclear Case Studies*. 2015, King's College London: London, UK. p. 16-17.

[10] IAEA, Establishing a System for Control of Nuclear Material for Nuclear Security Purposes at a Facility During Use, Storage and Movement, IAEA Nuclear Security Series No. 32-T, INTERNATIONAL ATOMIC ENERGY AGENCY, Vienna, (2019).

[11] GRIGG, M. and STERBA, J.H., The Fundamentals of Physical Protection, in *The Oxford Handbook of Nuclear Security*, C. Hobbs, S. Tzinieris, and S.K. Aghara, Editors. 2023, Oxford University Press. p. 233-253.

[12] IAEA, Preventive and Protective Measures Against Insider Threats, Nuclear Security Series No. 8-G, INTERNATIONAL ATOMIC ENERGY AGENCY, Vienna, (2020).

[13] FELIX ORIKPETE, O. and RAPHAEL EJIKE EWIM, D., Interplay of human factors and safety culture in nuclear safety for enhanced organisational and individual Performance: A comprehensive review, Nuclear Engineering and Design, **416** (2024) 112797.

[14] AGHARA, S.K. and PEEL, R., Nuclear Security for Next-Generation Reactors, in *The Oxford Handbook of Nuclear Security*, C. Hobbs, S. Tzinieris, and S.K. Aghara, Editors. 2024, Oxford University Press. p. 341-357.

[15] BRYAN, H.C., et al., Remote nuclear microreactors: a preliminary economic evaluation of digital twins and centralized offsite control, Frontiers in Nuclear Engineering, **2** (2023).

[16] AYODEJI, A., et al., Cyber security in the nuclear industry: A closer look at digital control systems, networks and human factors, Progress in Nuclear Energy, **161** (2023) 104738.

[17] BLACKETT, C., et al., Human Factors Considerations for Remote Operation of Small Modular Reactors, in *13th Nuclear Plant Instrumentation, Control & Human-Machine Interface Technologies*. 2023, American Nuclear Society: Knoxville, Tennessee.

[18] NACHREINER, F., NICKEL, P., and MEYER, I., Human factors in process control systems: The design of human–machine interfaces, Safety Science, **44** 1 (2006) 5-26.

[19] BORING, R.L. and GERTMAN, D.I., Human Reliability Analysis for Small Modular Reactors, in *11th Probabilistic Safety Assessment & Management Conference*. 2012, Idaho National Laboratory: Helsinki, Finland.

[20] O'HARA, J., et al., Human Reliability Considerations for Small Modular Reactors, Brookhaven National Laboratory, United States, 2012.