CYBERSECURITY CONSIDERATIONS OF AUTONOMY IN NUCLEAR FACILITIES (CYBERSECURITY LICENSING ACTIVITIES)

Dr. Anya Kim
U.S. Nuclear Regulatory Commission
Rockville, MD, USA
Email: anya.kim@nrc.gov

Kim Lawson-Jenkins
U.S. Nuclear Regulatory Commission
Rockville, MD, USA

Dr. Doug Eskins
U.S. Nuclear Regulatory Commission
Rockville, MD, USA

Ismael Garcia
U.S. Nuclear Regulatory Commission
Rockville, MD, USA

Tammie Rivera
U.S. Nuclear Regulatory Commission
Rockville, MD, USA

Abstract

Operators of nuclear facilities and reactor designers are looking at autonomous controls to lower costs of operation and maintenance, particularly for advanced reactors, including Small Modular Reactors (SMR). Autonomous control implies the capability to make decisions and take independent action under uncertainty for extended periods of time with limited or nonexistent communication while being able to compensate for and learn from failures. The paper characterizes autonomous systems using a framework with two dimensions: the levels of autonomy and the objectives of tasks within an autonomous system. Because the technology supporting autonomy can differ for each level and task, the framework is useful for the consideration of cybersecurity concerns, or any issues, associated with autonomous systems. The framework can provide the regulatory body with a basis for requesting information about autonomous systems from licensees to better assess expected behaviors and cybersecurity concerns associated with the systems.

Autonomous systems will incorporate various enabling technologies to gather data, perform situation analysis, diagnose, plan, decide and act. The enabling technologies used by autonomous systems also have their own set of cybersecurity risks and must be understood within the scope of the autonomous system. The paper will discuss cyber-physical risks and supply chain risks associated with autonomous systems that should be considered during cybersecurity licensing activities that can be evaluated within the framework.

1. INTRODUCTION TO AUTONOMOUS SYSTEMS

Autonomous systems with varying levels of autonomy have been employed in robotics, transportation, spacecraft, and manufacturing applications [1], [2], [3].

In nuclear power plants, automated[1] (but not autonomous) controls have played an important role in safety and operations [4]: Automated controls can close a valve or trip the reactor when predetermined parameters are reached. Reasons for automated control may range from regulatory requirements for automatic actuation of safety functions, improvements in efficiency over human operators, reductions of human errors, and protections for human operators from harsh environmental conditions [4], [5].

At this point, it is worthwhile to clarify the difference between automated and autonomous systems, as considered in this paper, particularly in the context of nuclear reactors: *Automated* implies a self-acting response based on fixed setpoints, parameters, or predefined scripts, while *autonomous* implies the capability of a system to make decisions and take independent action based on consideration of multiple inputs, states, and trends [3]. More specifically, fully autonomous systems are able to perform tasks and functions *independent* of the human operator, perform well under significant *uncertainties* for extended periods of time with limited or non-existent communication, and can *compensate* for and *learn* from failures, all without external *intervention* [6]. This kind of performance requires the system to possess many intelligent capabilities – such as diagnosis, modelling, analysis, planning, reconfigurability, self-validation and protection, and decision-making – that need to be supported by enabling technologies.

[1] The nuclear industry uses the term "automatic" systems and controls, e.g., automatic depressurization system, automatic rod control, automatic operation, automatic actuation, etc.

In general, the degree of automation or autonomy is not binary: it is often described as a continuum of "levels of automation" or "levels of autonomy." Currently, some in the nuclear industry are considering higher levels of automation (implying highly or fully autonomous systems) to increase availability, reduce accident risk, and lower the costs of operation and maintenance, particularly for advanced reactors and SMRs. Adoption of these concepts could enable significant reductions in costs associated with plant operations, maintenance, and security staff [7], [8]. However, autonomous systems must be supported by several enabling technologies that may shift or expand the attack surface, thereby creating new cybersecurity challenges. Novel cybersecurity risks such as those associated with cyber-physical systems and the supply chain, and their associated regulatory aspects, must be better understood before autonomous systems are adopted in nuclear power plants. At the same time, novel characteristics of advanced reactors and SMRs, such as fewer and passive safety features[2], smaller quantities of radioactive materials, and potential remote and/or underground siting, may lower the risk of attacks and require fewer security staff, challenging traditional approaches to nuclear safety, security, and safeguards (3S) risk [9]. Therefore, the use of autonomous technologies should be considered within the scope of the changing characteristics of the nuclear power plant.

This paper examines potential regulatory issues of concern as the U.S. Nuclear Regulatory Commission (NRC) staff considers how to best provide cybersecurity regulation and guidance in the development, implementation, and potential use of these systems. While the paper focuses on cybersecurity, the use of autonomous systems is a topic that may affect multiple technical disciplines, including human factors engineering and digital instrumentations and controls.

2. FRAMEWORK FOR AUTONOMOUS SYSTEMS

Currently operating nuclear reactors have automated controls – for example, automatically shutting a valve or performing some other specified action when a setpoint is reached. This automatic control implies a self-acting system response that is based on fixed setpoints, parameters, or scripts. However, highly autonomous intelligent control involves more than simple automation of routine functions. It implies the autonomous support/capabilities for at least the following supervisory functions [10]:

- Detection of conditions and events.
- Determination of appropriate response based on situational awareness.
- Adaption to unanticipated events or degraded/failed components.
- Re-evaluation of operational goals.

While there is a lack of consensus on the definitions, for the scope of this paper the authors used the definitions of "automated and autonomous" as such, especially within a nuclear domain [3]. The key attributes of highly autonomous systems are: (1) effective performance under all process operating conditions and performance demands; and, (2) the ability to compensate for system failure without external intervention [11], [12]. Unlike an automated system, an autonomous system should be able to independently assess and adapt to unanticipated situations, as well as plan and consider actions for which it was not programmed or trained. This capability also implies the ability to self-govern [13].

The paper examines how to characterize autonomous systems using a framework with two dimensions: the level of autonomy and the tasks within an autonomous system. This framework is an appropriate way to think about autonomous systems because the supporting technology can be different for each level and each task and hence, the associated cybersecurity concerns, or any issues for that matter, can also differ. The framework can also provide the regulatory body with a basis for requesting information about autonomous systems from licensees to better assess the cybersecurity aspects of the systems.

2.1. Levels of autonomy

Levels of autonomy refer to the degree to which a task or set of tasks is automated, ranging from fully manual (i.e., no automation) to fully autonomous (i.e., no human intervention) [14]. Tasks are the steps involved

[2] Passive safety systems that can safely shutdown a reactor without human intervention would be considered automated, but not autonomous.

in the decision-making of autonomous systems; they will be discussed in section 2.2. The levels of autonomy can be defined in terms of the degree of human intervention and the level of decision-making performed by an autonomous agent. Levels of autonomy can affect human performance, situational awareness, and workloads.

The nuclear industry literature has adopted various descriptions of levels of autonomy [14], [15], [16]. Yet these descriptions have various drawbacks. Previous definitions and usage of the concept of autonomy in the literature have focused on automation, some going so far as to use the two interchangeably. While it may fall on the continuum of levels of autonomy, full automation is not equivalent to full autonomous or partial autonomous operations/controls and should not be confused as such. Therefore, a definition of autonomy should reflect the features of autonomous operations and controls and should be consistently accepted by stakeholders to ensure they are using the concept in a consistent and intended manner.

An example of levels of automation can be seen in Table 1.

TABLE 1. LEVELS OF AUTOMATION FOR NUCLEAR POWER PLANTS IN NUREG-0700 [14]

Level	Automation Tasks	Human Tasks
1. Manual Operation	No automation	Operators manually perform all tasks
2. Shared Operation	Automatic performance of some tasks	Operators perform some tasks manually
3. Operation by Consent	Automatic performance when directed by operators to do so, under close monitoring and supervision	Operators monitor, approve actions, and may intervene to provide supervisory commands that automation follows
4. Operation by Exception	Essentially autonomous operation unless specific situations or circumstances are encountered	Operators must approve of critical decisions and may intervene
5. Autonomous Operation	Fully autonomous operation. System cannot normally be disabled but may be started manually	Operators monitor performance and perform backup if necessary, feasible, and permitted

It has been pointed out that this level of automation definition implies support of, rather than replacement of, operator functions/duties [8]. In fact, this taxonomy also does not clearly distinguish automatic and autonomous operations, but rather uses them interchangeably. In addition, the taxonomy does not specify how existing automation or automatic functions – not human performance related – will vary among the levels. Licensees must clearly define how tasks will be shared between the autonomous component and the human operator, under what specific cases the operator will give consent to the autonomous component, and what specific situations or circumstances will require human intervention and/or oversight.

Levels of autonomy can affect human performance, situational awareness (SA), and workloads. Studies have shown that SA tends to decrease with increasing levels of automation [6], [7], [15], [17]. This poses an "automation conundrum" in which automation increases system reliability and robustness but decreases the SA of human operators and their probability of successfully taking manual control when needed [6]. Additionally, the scope and potential consequences of machine error can increase with increasing levels of autonomy, while the potential for human intervention to mitigate such errors may decrease. Therefore, the degree of autonomy is a design decision that must trade off staffing reduction, operational flexibility, system complexity, and potential safety and reliability implications. Consideration of cybersecurity issues should also be part of the design and operation, as higher levels of autonomy involve more complex technology, and may present different and/or expanded attack surfaces. More research and consideration should be given to this matter.

2.2. Tasks within an autonomous system

Autonomy is applicable to the full range of decision-making tasks, or "cognitive functions," as defined in the literature [7], [14]. Distinguishing autonomy into specific tasks makes it easier to relate the specific technologies and functions that support the task. For example, some form of decision logic, whether based on artificial intelligence (AI) or not, will be used to support decision making. But if the goal is to assist with planning, different types of planning algorithms may be applied. Furthermore, levels of autonomy need not be uniformly applied to the whole system. Different tasks may be implemented at different autonomy levels within the same system, so consideration of decision-making tasks separately can help characterize the autonomous system.

A commonly-known decision-making process is the OODA loop, a cycle of four tasks of observe–orient–decide–act, with feedback loops as shown in Fig. 1. This process, developed by military strategist Colonel John Boyd [19], includes the following discrete tasks:

- Observe: Gather data and create actionable information; monitoring.
- Orient: Detect, filter, analyze, and enrich the information; reflect on data gathered as well as additional information such as operator experience, belief about the trustworthiness of the data and the system, to achieve SA and understanding to decide or predict and evaluate current conditions to perform diagnoses.
- Decide: Consider various alternatives and suggest an action or response plan based on potential outcomes; i.e., selecting a course of action.
- Act: Carry out the decision or course of action and determine if it was the correct action to take.

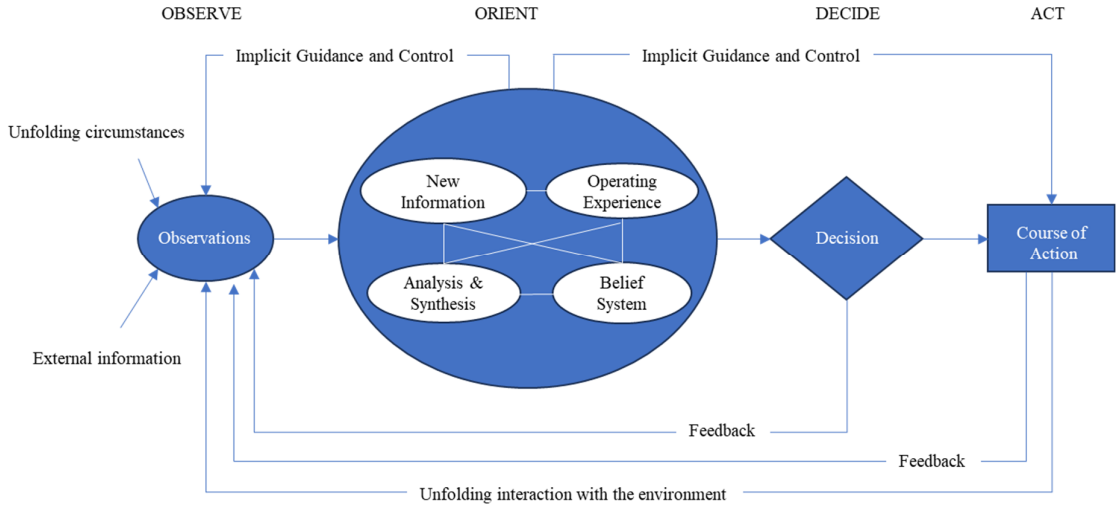

FIG. 1. OODA Loop based on John Boyd's drawing adapted from [19]

The following are examples of technologies that are or could be employed within the nuclear industry for implementing OODA tasks:

- Currently, operators are using unmanned aircraft system (UAS) technology for applications in commercial nuclear facilities for remote inspections of transmission lines, containment buildings, and high-dose areas of nuclear power plants [20]. Industry has shown interest in the potential use of UAS/drones for internal and external equipment surveillance (e.g., Dominion Energy, Xcel, Southern Company) [21]. These are a few examples of technology used for observation tasks. The information transmitted from a UAS can be transmitted to digital systems with the nuclear facility to perform orient and decide tasks.
- AI/machine learning (ML) and digital twin technology could be used for orient and decide tasks.
- For cybersecurity functions, security information and event management (SIEM) tools primarily perform observation and orient tasks through data collection and analysis for threat detection and incident handling.
- Camera systems perform a similar task for physical security. Some aspects of the orient task may be shared by the technology and the human, depending on the capabilities, training, and configuration of the devices implementing the technology.
- An example of a cybersecurity tool that may execute observation, orient, decide, and action tasks is an intrusion protection system (IPS). An IPS monitors network traffic for potential threats and has the capability to automatically take action by alerting the security personnel, terminating dangerous connections, removing malicious content, or triggering other responses to a cyber attack.

2.3. Proposed framework for autonomous systems

A framework can provide a basis for consistent assessment guidelines when examining different licensees' approaches to autonomous systems. The framework presented herein, or a similar framework, can provide a regulatory body with a basis for requesting information about autonomous systems under review from licensees. Furthermore, licensees could also benefit from such a framework for determining the required level of automation and associated system tasks during the design phase.

The proposed framework has two dimensions: (1) Levels of Autonomy; and (2) Tasks within the Autonomous System. For such a framework, the concept of autonomy must be clearly defined. This definition will provide the foundation for defining the levels of autonomy as well as the tasks involved. As an example, Table 2 shows how a framework can be depicted: for demonstration purposes, the framework uses the levels of autonomy that were presented in Table 1 and the OODA loop to describe the tasks.

TABLE 2. TEMPLATE OF A FRAMEWORK FOR AUTONOMOUS SYSTEMS

	Levels of Autonomy				
Tasks within an Autonomous System	Manual Operation	Shared Operation	Operation by Consent	Operation by Exception	Autonomous Operation
Observe					
Orient					
Decide					
Act					

Each cell in the table would define what the level of autonomy means for the given task. It can also show which enabling technologies would be applicable for each cell. For example, "Autonomous Operations" for the "Observe" task can describe how the autonomous system is wholly responsible for collecting data from sensors, images, and logs, and using the data to build an accurate picture. The underlying enabling technologies may include natural language processing and image recognition. Using a framework to characterize the autonomy of the system being evaluated may help focus on the capabilities of the technologies, and potential cybersecurity concerns. Whether adaptive automation is available or not can also be defined for each cell. An example of applying the framework is provided in section 2.4. Similar frameworks have been proposed by other researchers [15], [17], [22], [23].

Reaching higher levels of autonomy is not trivial – it is a shift from reactive response of an automated system to anticipatory and proactive response and decision-making of an autonomous system. This will require significant technology advancement, education and training, and validation and verification of the models, as well as regulatory guidance. A framework such as the one described above can be a starting point in providing such guidance. This framework is for illustration purposes – further research will be required to determine the best way to describe the framework.

2.4. Applying the framework

To better understand how to use this or a similar framework, this paper presents a scenario and describes how each task (observe-orient-decide-act) would work given the level of autonomy defined.

The hypothetical scenario used in the paper is as follows: while performing routine patrol duty, an unlocked cabinet door is observed. As a result of the observation, it must be determined whether the unlocked cabinet contains operational critical digital assets (CDA). Once the situation has been assessed, a decision must be made on what action to take regarding this situation and then perform the action. What entity – a robot or a human – performs these tasks is dependent on the specific level of autonomy where the task is executed.

In a fully manual scenario, a human guard performing a security patrol observes an unlocked door of a cabinet that contains operational CDAs; no robot is used for security patrols. In the scenarios employing autonomous monitoring and actions, the robot never takes physical action on a CDA or on connections to CDAs located within the unlocked cabinet; those actions must always be performed by human personnel. In this example, the only physical action that the robot can take is to lock the cabinet. The fully manual scenario for each task is not described in the example below, as the intent is to focus on those tasks that involve operations by the robot. The potential ways the scenario could be understood/implemented using the framework are shown in Table 3.

TABLE 3. EXAMPLE OF THE FRAMEWORK FOR A PHYSICAL SECURITY SCENARIO

	Levels of Autonomy			
Tasks within an Autonomous System	Shared Operation	Operation by Consent	Operation by Exception	Autonomous Operation
Observe	Observation tasks can be shared. Robot performs a routine security patrol within a specified area of the nuclear facility. The images captured by the robot are transmitted real-time, enabling plant personnel to observe the transmission from the robot.	Robot performs routine security patrol. Images captured by the robot are transmitted real-time. Plant personnel observe transmission, notice the unlocked cabinet, and interrupt robot's routine patrol. Personnel instruct the robot to capture additional information (e.g. video and sound) about the opened cabinet for orientation.	Robot autonomously performs its routine patrol. When it notices the unopened cabinet – an anomalous situation – it highlights the captured image of opened cabinet door and turns control over to plant personnel. Personnel may further instruct robot to capture additional information such as visible settings and connection of CDAs within cabinet and transmit these images for orientation.	Robot autonomously interrupts its routine patrol, highlights captured image of opened cabinet door, and autonomously captures additional images, such as visible settings and connection of CDAs within the cabinet for orientation. The robot *may* transmit these images to plant personnel.
Orient	Orientation tasks are divided between robot and plant personnel. For example, collection of additional information may be done by the robot, while actual situational awareness based on collected data may be done by plant personnel.	To determine whether the unlocked cabinet contains CDAs, plant personnel observe the real-time transmission from the robot. In addition to instructing the robot to capture more data, the plant personnel may request additional information from other sensors and data sources within the facility. Personnel may also ask the robot to communicate with other autonomous devices in the facility.	Robot autonomously collects additional information for situational awareness such as type of devices in the unlocked cabinet. If the robot discerns that the devices in the cabinet are CDAs, it may require plant personnel to take over. Plant personnel may verify or collect additional information to validate the findings.	Robot autonomously captures additional information of devices with the unlocked cabinet and communicates with other autonomous devices within the facility. The robot will determine whether the unlocked cabinet contains CDAs. Robot *may* transmit this situational awareness information to plant personnel.
Decide	According to predetermined agreement, robot may be allowed to make decision, or may require plant personnel to make decisions regarding the open cabinet containing CDAs.	Plant personnel may direct the robot to make a decision regarding the unlocked cabinet. When the robot is allowed to make the decision, it transmits the proposed course of action to plant personnel for supervision and final decision-making.	If an unlocked cabinet containing CDAs is defined as an exceptional situation, plant personnel may decide the course of action. If it is not viewed as exceptional, robot may be allowed to determine course of action. If robot makes the decision, it will transmit the proposed course of action to plant personnel for approval.	Robot autonomously determines course of action to address unlocked cabinet containing CDAs. The robot may transmit information to other autonomous devices that protect CDAs that could be affected (and these robots will then update their own situational awareness).
Act	Decision making task can be shared between robot and personnel: Assuming the decision is to verify the status of the CDAs in the cabinet and then lock the cabinet, the plant personnel can be dispatched to verify status of the CDAs in the cabinet, and robot secures the cabinet.	The plant personnel may allow the robot to perform all or part of the action. Or personnel may be dispatched to verify the status of the CDAs within the cabinet and to secure the cabinet while the robot resumes its security patrol.	By default, the robot performs the decided actions (e.g., verify the status of the CDAs and secure the cabinet) unless plant personnel intervene. The robot then resumes its security patrol.	The robot performs the decided action (e.g., verify the status of the CDAs and secure the cabinet). The robot then resumes its security patrol. Plant personnel may monitor the actions of the robot.

One thing to note is that an autonomous system will not necessarily perform at the same level of autonomy for each task. The system may have different levels of autonomy for each task. For example, the system may be *fully autonomous* for observing, *shared operation* for orientation, *operation by exception* for decision-making, and *operation by consent* for acting.

This example shows a method that can be applied when considering the use of automation for a set of actions – allowing it to be considered in a consistent manner and to assess the risk of such automation. It does not dictate the use of this specific framework, but rather highlights that whatever framework is used, it needs to be used and applied consistently. For example, if licensees use the levels of automation as described in the paper, what will *shared operation* look like for the given system? Clear and consistent definitions of how automated tasks will be divided between an autonomous device and the human operator need to be developed and applied consistently throughout the decision-making cycle. The framework will aid in assessing at what point human intervention and/or oversight may be needed to address a given risk. Application of this framework provides a more granular view of autonomous systems so that owners and operators can better assess the risk involved in using autonomous observations, orientations, decisions, and/or actions for a given system. One of the results of applying the framework may be that more human oversight needs to be added to reduce the assessed risk. This and other considerations need to be discussed and planned to design and assess autonomous systems.

For the foreseeable future, safety-related tasks categorized under “Decide” and “Act” of OODA should require human involvement (i.e., a physical action must be performed by a human) or oversight (i.e., shared operation, operation by consent, and operation by exception).

3. DISCUSSION OF RISKS ASSOCIATED WITH AUTONOMOUS SYSTEMS

Semi-autonomous or highly automated systems will likely be composed of digital components that use technologies – such as wireless, remote, or shared data processing and monitoring technologies, AI/ML, digital twins – as enabling technologies. This section discusses general risks associated with the introduction of these technologies.

3.1. Cybersecurity risks

The use of autonomous systems expands the attack surface and potential attack pathways of digital devices and communication systems through the addition of new components and new technologies. Complex digital devices increase the opportunity for adversaries to exploit vulnerabilities and misuse features or communication protocols to generate new tactics, techniques, and procedures for cyberattacks. In order to ensure that the use of autonomous technology does not adversely impact a nuclear facility’s cybersecurity posture, an assessment should be performed to identify, mitigate, and continuously monitor new cybersecurity risks introduced throughout the device’s life cycle. A nuclear facility can implement the following four-step process for performing a risk assessment to assess the security impact, which would include cybersecurity, physical security, information security, and operational security [24]:

Step 1. Evaluate new cybersecurity risks. The risks introduced by the autonomous technology should be evaluated by assessing the potential vulnerabilities. The processing requirements for functions such as data acquisition, data validation, and selection of training data that affect the safe and secure operation of the autonomous technology must be identified. Data confidentiality, access control, and data integrity of surveillance information and remotely accessed functions must be addressed. For example, information obtained by plant surveillance drones should be protected. New types of cybersecurity vulnerabilities associated with ML and other enabling technologies should also be explored. Just as decisions to rely on autonomous technologies to increase operational efficiencies are made early in the development of a facility or product lifecycle (i.e., the concept and/or requirements phase), mitigations to address cybersecurity risks for the complete life cycle – including installation, testing, and maintenance phases – should be identified in the concept and/or requirements phases. Understanding the capabilities and resources required to securely implement and maintain the devices employing autonomous technology is essential for knowing the true cost of deploying the technology.

Step 2. Update cybersecurity policies and processes. Plant operators should evaluate their cybersecurity policies and processes to identify ambiguity for use of the device. Because these devices using autonomous technology are most likely obtained from suppliers, nuclear facility owners and operators may need to enhance

their existing supply chain risk management programs to vet suppliers and devices before procuring and deploying the devices. The nuclear power plant's supply chain risk management program should implement best practices for the delivery of the device's technology (i.e., hardware, software, and firmware), such as vetting the supplier's cybersecurity practices and determining whether the device incorporates cybersecurity into its design (e.g., ability to manage device configurations and access, ability to scan for emerging vulnerabilities, malware protection and detection).

Step 3. Implement new mitigating controls. After identifying vulnerabilities of devices and processes, additional security measures can be implemented to mitigate risks and new threat vectors. Risk mitigation strategies include protection of data, software, firmware, and wired or wireless communication that are needed for the automated or autonomous device to function. If a mitigation cannot be addressed by implementing security controls directly on the device itself, operators may also decide to implement security features within the plant environment to mitigate the risk of deploying the emerging technology. Additional mitigations may include reducing the level of autonomous tasks and increasing human oversight.

Step 4. Monitor Security Controls. New security measures that have been implemented for the devices should be monitored for effectiveness to identify new risks. Examples of security controls for the secure operation and maintenance of the autonomous technology are equipment or applications to monitor specialized communications (e.g., wireless or industrial Internet of Things), to monitor data integrity for AI applications, or to scan devices to implement supply chain protections. Also, similar to requirements for functional applications to execute autonomously (i.e., with limited or no human intervention) on devices, autonomous self-protection and security reporting mechanisms should be required for deploying autonomous technology.

3.2. Cyber-Physical risks

The Physical Protection System (PPS) is the first line of defense of many nuclear power plants and has three main functions: detect, delay, and respond [25], [26], [27]. Yet, advanced reactors are likely to not have a large on-site security staff –due to remote and autonomous operations, for economic reasons, or both [11], [25], [28]. The lack of a large on-site protective force may increase the response time, putting additional burden on the effectiveness of the delay mechanisms and the detection time. Therefore, the cybersecurity of these highly digitalized PPS will have to be robust and resilient. If the PPS relies extensively on digital systems (e.g., digital cameras and sensors for detection) for its off-site security operations, the PPS could become an attractive target for the attacker. The ability to rely on a sufficient and effective on-site response to a security threat is a key factor that should be considered at the initial conceptual design phase to ensure sufficient intruder delays are included [25]. If on-site presence is not available, better detection mechanisms and extending of adversary delay times must be incorporated into the design.

Lack of a large on-site security staff may translate to lack of staff to perform the detect and delay functions as well; the physical access control and authentication procedures may not be equivalent to what traditional nuclear power plants have implemented. Some of the detection and delay mechanisms may take the form of cyber/digital systems. If the reactor is remotely sited, then the response time for off-site forces may take even longer, so the cybersecurity controls may need to be more robust and resilient to support the safety and security of the reactor. This is particularly true for reactors that may be in hard-to-reach areas, such as floating in the ocean. Research has been proposed to employ emerging technologies such as automated security systems, advanced robotics, UAS/drones and/or remotely operated systems to replace or augment security personnel [29]. Drones can be equipped with cameras and sensors, and perform tasks such as perimeter monitoring, radiation detection, intrusion detection, and emergency response. They may also be used to take down other drones that attempt to enter the restricted air space over the nuclear reactor. These technologies need to be tested and evaluated to demonstrate that they can be operated effectively, safely, and securely [26], [27].

3.3. Supply chain risks

Various types of advanced reactors will be highly modular. Because they are likely to be built in factories and assembled remotely by suppliers, with an increased number of individuals/organizations with access to the components, there will be more opportunities for cyber vulnerabilities to be introduced into the supply chain that may increase the risk of safety, security, and emergency preparedness equipment being compromised [29], [30]. Products should be procured from trusted sources and have traceability though use of a trusted distribution path.

Trustworthiness of devices needs to be ensured and verifiable. To counter this, SMR design and construction may benefit from being constructed in a restricted or protected area [29]. Additional regulation and/or guidance may be needed to provide assurance of the trustworthiness of the supply chain for autonomous systems for use in nuclear facilities.

4. CONCLUSION AND FUTURE WORK

Autonomous systems will likely become an integral part of nuclear power plants – especially for advanced reactors, including SMRs. However, the technology exposes the plant to new attack vectors that need to be explored and understood. Extensive research is needed to understand the risks of autonomous systems. The cyber risks of a plant employing autonomous systems depend in part on the type and characteristics of the reactor, siting, level of autonomy, enabling technologies used, and physical protection requirements, among other things. Understanding these risks will enable regulatory bodies, designers, and licensees to better understand how to mitigate and address these risks.

The paper presents a framework for autonomous systems based on level of autonomy and tasks for autonomous systems. It shows how the framework could be applied to describing autonomous systems. Achieving a high level of autonomy will require significant technological advancements, validation and verification of the technologies used and models employed, and regulatory guidance. The framework can be a starting point in achieving these objectives. Further research will be required to determine how to define autonomy and develop an ideal way to describe a framework for autonomous systems.

DISCLAIMER

This paper represents the personal opinions and viewpoints of the authors and is not intended to represent any official position of the U.S. Nuclear Regulatory Commission.

REFERENCES

[1] G. Brat, M. Davies, D. Giannakopoulou, and N. Neogi, “Workshop on Assurance for Autonomous Systems for Aviation,” 2016.

[2] S. Cho, E. Orye, G. Visky, and V. Prates, “Cybersecurity Considerations in Autonomous Ships,” NATO CCDCOE, 2022.

[3] G. W. Clark, M. V. Doran, and T. R. Andel, “Cybersecurity issues in robotics,” in *2017 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA)*, Mar. 2017, pp. 1–5. doi: 10.1109/COGSIMA.2017.7929597.

[4] D. Lee, J. Kim, J. Yang, S. Lee, and G. Kim, “Autonomous Control for Safety Systems of Nuclear Power Plant by Using the LSTM Neural Network,” *Transactions of the American Nuclear Society*, vol. 117, pp. 430–432, Oct. 2017.

[5] D. Lee, P. H. Seong, and J. Kim, “Autonomous operation algorithm for safety systems of nuclear power plants by using long-short term memory and function-based hierarchical framework,” *Annals of Nuclear Energy*, vol. 119, pp. 287–299, Sep. 2018, doi: 10.1016/j.anucene.2018.05.020.

[6] M. R. Endsley, “From here to autonomy: lessons learned from human–automation research,” *Human factors*, vol. 59, no. 1, pp. 5–27, 2017.

[7] J. Oxstrand, J. O’Hara, K. LeBlanc, A. Whaley, J. Joe, and H. Medema, “Development of an Initial Model of Human-Automation Collaboration--Results from a Needs Analysis,” *SMR/ICHMI/INL/TR-2013/01, INL/EXT-13-28682). Idaho Falls, ID: Idaho National Laboratory*, 2013.

[8] A. L. Alberti, V. Agarwal, I. Gutowska, C. J. Palmer, and C. R. E. de Oliveira, “Automation levels for nuclear reactor operations: A revised perspective,” *Progress in Nuclear Energy*, vol. 157, p. 104559, Mar. 2023, doi: 10.1016/j.pnucene.2022.104559.

[9] A. D. Williams, D. Osborn, and B. Cohn, “Security Safety and Safeguards (3S) Risk Analysis for Small Modular Reactors.,” Sandia National Lab. (SNL-NM), Albuquerque, NM (United States), 2019.

[10] M. D. Muhlheim *et al.*, “Risk-Informed Decision-Making and Reconfiguration using OPRA,” Oak Ridge National Laboratory, ORNL/SPR-2023/3078, Sep. 2023.

[11] R. Belles and M. D. Muhlheim, “Licensing Challenges Associated with Autonomous Control,” Oak Ridge National Lab. (ORNL), Oak Ridge, TN (United States), 2018.

[12] H. Basher and J. S. Neal, “Autonomous Control of Nuclear Power Plants,” United States, Technical Report ORNL/TM-2003/252, Oct. 2003. doi: 10.2172/885601.

[13] J. Kim, D. Lee, J. Yang, and S. Lee, "Conceptual design of autonomous emergency operation system for nuclear power plants and its prototype," *Nuclear Engineering and Technology*, vol. 52, no. 2, pp. 308–322, Feb. 2020, doi: 10.1016/j.net.2019.09.016.

[14] U.S. Nuclear Regulatory Commission, "Human-System Interface Design Review Guidelines," U.S. Nuclear Regulatory Commission, Washington, DC, Technical Report NUREG 0700, Rev. 3, Jul. 2020. [Online]. Available: ADAMS Accession No. ML20162A214

[15] M. R. Endsley and D. B. Kaber, "Level of automation effects on performance, situation awareness and workload in a dynamic control task," *Ergonomics*, vol. 42, no. 3, pp. 462–492, 1999.

[16] T. B. Sheridan, *Humans and automation: System design and research issues*. Santa Monica, CA: Human Factors and Ergonomics Society, 2002.

[17] J. Oxstrand and K. L. Blanc, "Effects of Levels of Automation for Advanced Small Modular Reactors: Impacts on Performance, Workload, and Situation Awareness," Jul. 2014, doi: 10.2172/1164865.

[18] U.S. Nuclear Regulatory Commission, "Cyber Security Programs for Nuclear Power Reactors Revision 1 Washington, DC, Regulatory Guide (RG) 5.71, Feb. 2023. [Online]. Available: ADAMS Accession No. ML22258A204

[19] "OODA loop," The OODA Loop Explained: The real story about the ultimate model for decision-making in competitive environments. Accessed: May 21, 2023. [Online]. Available: https://www.oodaloop.com/the-ooda-loop-explained-the-real-story-about-the-ultimate-model-for-decision-making-in-competitive-environments/

[20] "Drones Boost Efficiency & Improve Safety in Utility Inspections," Constellation Clearsight. Accessed: Feb. 01, 2023. [Online]. Available: https://constellationclearsight.com/blog/drones-can-boost-efficiency-improve-safety-in-utility-aerial-inspections/

[21] "The Future of Drones in the Electrical Power Industry," Dexotech Power. Accessed: Feb. 01, 2023. [Online]. Available: https://dexotechpower.com/engineering/the-future-of-drones-in-the-electrical-power-industry/

[22] J. M. O'Hara and J. C. Higgens, "Human-system Interfaces to Automatic Systems: Review Guidance and Technical Basis," Brookhaven National Laboratory, Technical Report BNL-91017-2010, Jan. 2010. [Online]. Available: ADAMS Accession No. ML102720251

[23] R. Parasuraman, T. B. Sheridan, and C. D. Wickens, "A model for types and levels of human interaction with automation," *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, vol. 30, no. 3, pp. 286–297, May 2000, doi: 10.1109/3468.844354.

[24] K. Lawson-Jenkins and F. Peralta, "Consideration Of Cybersecurity Risks With The Use Of Emerging Technologies," in *The INMM 61st Annual Meeting*, Virtual: Institute of Nuclear Materials Management, Jul. 2020.

[25] Nuclear Energy Institute (NEI), "Physical Security For Small Modular Reactors," Position Paper ML12221A197, Jul. 2012.

[26] Nuclear Energy Institute (NEI), "Proposed Physical Security Requirements for Advanced Reactor Technologies," Position Paper ML17026A474, Dec. 2016.

[27] A. Evans, C. Byrum, D. Stanford, E. Sandt, and T. Goolsby, "Physical Protection Recommendations for Small Modular Reactor Facilities," Nov. 2021, doi: 10.2172/1837151.

[28] R. Fasano, A. Hahn, J. James, C. Lamb, and A. Haddad, "Cyber-Physical Risks for Advanced Reactors," United States, Sep. 2021. doi: 10.2172/1854721.

[29] R. Duguay, "Small modular reactors and advanced reactor security: Regulatory perspectives on integrating physical and cyber security by design to protect against malicious acts and evolving threats," *International Journal of Nuclear Security*, vol. 7, no. 1, p. 2, 2020.

[30] B. Aamoth, W. E. Lee, and H. Ahmed, "Net-Zero Through Small Modular Reactors-Cybersecurity Considerations," presented at the IECON 2022–48th Annual Conference of the IEEE Industrial Electronics Society, IEEE, 2022, pp. 1–5.