UNITED STATES NUCLEAR REGULATORY COMMISSION ASSESSMENT OF EMERGING TECHNOLOGIES AND THREATS IN NUCLEAR SECURITY

Alex A.M. Brown
United States Nuclear Regulatory Commission
Rockville, Maryland, United States of America
Email: Alexander.Brown@nrc.gov

Dr. A. Kim
United States Nuclear Regulatory Commission
Rockville, Maryland, United States of America
Anya.Kim@nrc.gov

K. Lawson-Jenkins
United States Nuclear Regulatory Commission
Rockville, Maryland, United States of America
Kim.Lawson-Jenkins@nrc.gov

I. Garcia
United States Nuclear Regulatory Commission
Rockville, Maryland, United States of America
Ismael.Garcia@nrc.gov

S. Prasad
United States Nuclear Regulatory Commission
Rockville, Maryland, United States of America
Stacy.Prasad@nrc.gov

Abstract

The use of Uncrewed Aerial Systems (UAS), commonly referred to as "drones," like all technology, can be utilized as both a valuable tool and threat to security depending on the purpose of the operator. When used properly, UAS can provide value and contribute to the success of business operations and enhancements in safety. UAS are used to support first-responder operations, to monitor and assess critical infrastructure, to provide precision agriculture to the farming community, and for recreation. UAS technical capabilities continue to increase in many ways, from improved sensors and maneuverability to artificial intelligence (AI) and autonomous technology. While beneficial, these advancements also increase the threat to the safety and security of critical infrastructure facilities due to intentional or inadvertent actions. As a result, potential threats associated with UAS will continue to expand in the coming years. While significant work is underway within the United States (U.S.) Government regarding UAS, additional work is ongoing and necessary to expand existing US regulations regarding UAS detection and counter UAS mitigation strategies. The paper provides perspectives on emerging technologies, specifically UAS, and the threat they pose to nuclear security. Additionally, the paper will discuss coordination with federal partners to ensure the NRC provides prompt assessment of any security threats to NRC licensed facilities, materials, and activities resulting from such emerging technologies.

1. OVERVIEW OF UAS TECHNICAL CAPABILITIES

The popularity of UAS has grown – as a versatile business and national security tool, and a popular recreational hobby – as the cost has become more affordable. In addition to recreational use, UAS are used across the U.S. to support firefighting and search and rescue operations, to monitor and assess critical infrastructure, to provide disaster relief by transporting emergency medical supplies to remote locations, and to aid efforts to secure our U.S. borders. UAS have the capability to access and inspect places humans cannot easily access, including harsh environments. As their popularity increases, their technical capabilities continue to increase as well. They can attain higher speeds, longer flight times, and carry heavier payloads than ever before.

However, with these advances, potential threats associated with UAS will also continue to expand in nature and increase in volume in the coming years. Because of their physical characteristics and capabilities, UAS can create challenges for the critical infrastructure community. They can often evade detection, carry dangerous payloads, smuggle contraband, and conduct illicit surveillance. UAS can also be used for malicious schemes by terrorists, criminal organizations, and lone actors with specific objectives. UAS-related threats may include [1]:

— Weaponized or Smuggling Payloads – Depending on power and payload size, UAS may be capable of transporting contraband, chemicals, or other explosive/weaponized payloads;
— Prohibited Surveillance and Reconnaissance – UAS are capable of silently monitoring a large area from the sky for nefarious purposes;
— Intellectual Property Theft – UAS can be used to perform cyber-crimes involving theft of trade secrets, technologies, or sensitive information;
— Intentional Disruption or Harassment – UAS may be used to disrupt or invade the privacy of other individuals.

2. POTENTIAL BENEFICIAL USES FOR NUCLEAR SAFETY AND SECURITY

As an independent regulatory agency, the United States Nuclear Regulatory Commission's (NRC) mission includes safety and security aspects – specifically: "The NRC licenses and regulates the Nation's civilian use of radioactive materials, to provide reasonable assurance of adequate protection of public health and safety, to promote the common defense and security, and to protect the environment." The NRC has been assessing UAS and their use in commercial nuclear power plants. In this paper, the term "licensee-owned" UAS will be used to refer to UAS used for operations at U.S. nuclear power plants for approximately the last five years. From a safety standpoint, the NRC has researched the use of drones for commercial nuclear power plant applications such as radiation monitoring and surveys during decommissioning activities [2] [3]. The research revealed that UAS could be used beneficially for radiological surveys for detection at levels needed for decommissioning sites. Currently, operators are using UAS technology for applications in commercial nuclear facilities for remote inspections of transmission lines, containment buildings, and high-dose areas of nuclear power plants. [4] [5] [6] [7] [8] Industry (e.g., Dominion Energy, Xcel, Southern Company) has shown interest in the potential use of drones for internal and external equipment surveillance. For example, Dominion has an unmanned nuclear inspection team (UNIT) that uses UAS to perform inspections such as submersible drones performing inspections of piping and tanks. [9]

3. POTENTIAL PHYSICAL SECURITY RISKS

The increasing notoriety of UAS, technical advances in uncrewed technology, and the consistent availability of news and data on attacks involving UAS have likely driven threat actors to see UAS as a viable option to conduct attacks against critical infrastructure. Emerging UAS technologies offer improvements to support heavier payloads, precision guidance, evasion of counter-UAS technologies, and improved user control.

UAS can be used for malicious schemes by terrorists, criminal organizations, and lone actors with specific objectives in numerous ways. The NRC staff continues to evaluate the novel deployment of UAS technologies in conflict zones, most notably the Russia-Ukraine conflict, to assess the threat these technologies pose to our licensees. The pervasive use of UAS across the battlefield and against civilian targets has advanced the available data for potential threat actors to use to inform their attack tactics. This level of use has dramatically increased the production and distribution of UAS, including Ukraine setting a goal of producing one million drones per year. [10]

Both state actors and companies producing these drones have been forced to adapt battlefield tactics as advances in offensive and defensive technologies continue to leapfrog each other. Advances in navigation via first-person view technologies have been countered by radio-jamming electronic warfare equipment, which blocks the signal between pilot and UAS. These have in turn caused companies and states to explore the use of AI-enabled flight technologies that can guide UAS to targets in the event their link to a pilot has been lost.

These advancements present an easily adaptable set of instructions for threat actors to inform an attack against U.S. facilities. Non-state actors have successfully used UAS to conduct lethal attacks against hardened facilities outside of the United States, as demonstrated in the 7 October 2023 attacks by Hamas in Israel and by the 28 January 2024 attack against a U.S. military outpost in Jordan. In these attacks, non-state actors successfully adapted technologies and tactics that state actors had previously demonstrated as viable, showing that non-state actors have learned from previous conflicts and adapted their tactics to become a greater asymmetric threat.

The NRC staff continuously monitors the current threat environment for any changes that may impact NRC licensed facilities, materials, and/or other activities, and coordinates with its Federal partners to ensure that the NRC is providing prompt assessment of any security threats to those licensed facilities, materials, and activities. Should any change to the threat landscape occur, NRC will take prompt and appropriate action to address any security threats to its licensed facilities, materials, and activities. Furthermore, the NRC staff considers risk (a function of threat, vulnerability, consequence, and mitigation) to inform any recommendations to update the NRC's Design Basis Threats (DBT) of radiological sabotage and theft or diversion of special nuclear material. The NRC uses these DBTs to design safeguards systems to protect against adversarial acts. In the event of a change to the DBT in response to a changing or new threat, licensees would need to conduct site-specific assessments to determine if any additional protective measures were needed to address the new or changing threat.

Cognizant of the increase in frequency of UAS sightings at U.S. commercial nuclear power plants over the last decade, the NRC staff initiated a technical analysis in 2019 with Sandia National Laboratories to gauge the extent of the threat drones pose. That assessment is classified, but an unclassified executive summary [11] was released in October 2019. The technical analysis concluded that U.S. commercial nuclear power plants did not have any risk-significant vulnerabilities that could be exploited by adversaries using commercially available drones to result in radiological sabotage, or theft or diversion of special nuclear material. In addition, the study concluded that any information an adversary could glean from overhead surveillance using drones is already accounted for in the NRC's DBTs, which assume adversaries have insider information about the plant and its operations.

4. POTENTIAL CYBER SECURITY RISKS

Licensee-owned UAS operate with the use of software or firmware, and rely on computers or mobile devices (e.g., phones, tablets) to run the UAS applications. [12] Cybersecurity risks involve unauthorized access to the UAS' software and firmware vulnerabilities in order to gain access to the connected system and network, as well as any data stored or transmitted from the UAS. Malware could also be embedded in the UAS' software via the supply chain and eventually compromise the data on the UAS, the systems and software it interfaces with, or other connected devices. The use of UAS could also provide an additional conduit for malicious actors to gain proximity - or pivot - to networks and other wireless devices and equipment within the protected area of a nuclear facility that would not normally be accessible due to their physical limitations (i.e., range limitations). Communication between targeted licensee-owned drones and a ground station controller could be intercepted by a nearby attacker drone. In addition to the loss of confidentiality, the compromised UAS communication path could be used to attack wireless communication within the targeted facility. [13]

The communication methods used by these devices (e.g., WiFi, Bluetooth, low-power radio waves) can introduce new risks of the data and communications being intercepted and manipulated before being received by the correct device or operator. An additional risk with these communication methods is the possibility of having a file or malware inadvertently sent in the transmission without the operator's knowledge if the communication is not adequately secured and controlled.

New and expanded attack vectors[1] introduced by the use of licensee-owned UAS present a possible risk to be evaluated and mitigated. Data confidentiality, integrity, and availability of the information received, stored, and transmitted by the UAS must be addressed. Cyberattacks against UAS can cause disclosure or theft of confidential data, unauthorized alteration of data, as well as theft or disruption of operations of the UAS itself. A licensee needs an understanding of how these devices communicate with the operator and interfacing systems to monitor for and detect abnormal behavior.

Threats to confidentiality may occur through a supply chain vulnerability that can be addressed by use of trusted foundries for hardware and firmware, as well as extensive software testing. The cybersecurity breach of SolarWinds' —a Texas-based network management software company— software, which began in 2019, publicly demonstrated the vulnerabilities from malicious actors using supply chain attacks to breach critical technologies. The U.S. fiscal year 2024 National Defense Authorization Act limited procurement by U.S. Government sources of UAS produced by covered foreign entities. This prohibition aimed, in part, to protect the collection and transmission of sensitive information, consisting of communication links and the components that control the unmanned aircraft, that enable the operator to operate the aircraft in the U.S. National Airspace System. Lack of encryption or use of weak encryption between the UAS and the ground station controller can also lead to loss of confidentiality.

Security information and event management (SIEM) tools can be configured to deny all communication except for finely tuned expected behavior and use of communication protocols. The ability to scan for known and new vulnerabilities in the devices will also become an important feature for risk management. A licensee needs to understand the minimum functionality needed from the emerging technology to execute the required function at the plant in order to allow the licensee to minimize the attack surface[2] by implementing least functionality and system hardening security controls on the new devices with emerging technologies. Implementing least functionality on protected assets will assist the operator in fine-tuning SIEMs to monitor expected device behavior and to detect abnormal behavior or communications. Additionally, least functionality will also aid the operator in maintaining a device in a secure state by reducing the number of vulnerabilities – which include known vulnerabilities and future zero-day vulnerabilities - that could be exploited by an adversary in a cyber-attack.

5. CURRENT U.S. REGULATORY FRAMEWORK

Three separate U.S. statutes [16] (6 U.S. Code § 124n, 10 U.S. Code § 130i, and 50 U.S.C § 2661) grant four U.S. Government departments—the Departments of Justice (DOJ), Homeland Security (DHS), Defense (DoD), and Energy— the ability to take certain UAS detection and Counter-UAS (C-UAS) actions to protect covered facilities or assets. The term "covered facility or asset" is defined in each of the three statutes and requires the Attorney General or respective Department Secretary to identify and designate the specific facility or asset based on the criteria outlined in each statute. For example, "covered facility or asset" in 50 USC § 2661 includes a criterion that the facility be owned by the U.S. or contracted to the U.S., to store or use special nuclear material. These statutory provisions are needed because many technologies that could be used to intercept data or the content of electronic communications between a UAS and its operator (e.g., an operator's cell phone, UAS remote controller) may violate statutes, such as the Wiretap Act (18 U.S. Code § 2510), which criminalize the interception of electronic communications and associated data without judicial authorization or pursuant to an exception. In addition, there is an inherent risk of UAS detection and C-UAS mitigation systems introducing potentially adverse secondary effects on the national airspace system. For this reason, the DHS, Federal Aviation Administration (FAA), DOJ, and Federal Communications Commission issued an advisory guidance [17] document to assist non-Federal public and private entities interested in using tools, systems, and capabilities to detect and mitigate UAS.

---

[1] Means, method, mechanism, or technique (or combination thereof) used or might be used by an adversary to gain unauthorized access to, exploit a vulnerability in, produce a malicious outcome on, or otherwise cause adverse impact to a digital asset, network, or system. [14]

[2] The set of points on the boundary of a system, a system element, or an environment where an attacker can try to enter, cause an effect on, or extract data from, that system, system element, or environment. [15]

The advisory is intended to provide an overview of potentially applicable federal laws and regulations, and how those laws may apply to actions or systems.

Based on the current statutory provisions, NRC licensees and other entities within the U.S. critical infrastructure are limited in the actions associated with UAS detection and are not authorized to utilize countermeasures against UAS. For example, commercial nuclear power plant licensees' security forces do not have the authority to attempt to interdict or shoot down aircraft flying over their facilities, including UAS. Instead, the NRC asked commercial nuclear power plant licensees to voluntarily report any sightings of UAS over their protected areas. The NRC then relays this information to state and local authorities, the FAA, and the Federal Bureau of Investigation (FBI). To aid licensees in this reporting process, the NRC issued two security advisories specifically related to UAS overflight activity in recent years, one in 2021 [18] and another in 2022 [19]. These advisories highlight some of the challenges posed by UAS activity at/near sites, encourage robust reporting of suspicious UAS overflights, and provide guidance for the type of information that can be reported to the NRC to enhance its analysis work. In 2023, the NRC issued new requirements in § 73.1215, "Suspicious Activity Reports," which requires licensees to report activities occurring at or around their sites they deem to be suspicious, including UAS flyovers, within 4 hours of the time of discovery. Implementing guidance is available in Regulatory Guide 5.87, "Suspicious Activity Reports." Licensees are required to make the notifications to local law enforcement, the FBI, NRC, and the FAA.

6. INTERAGENCY ENGAGEMENT ON UAS

The nuclear industry has been engaging with the NRC, DOE and FAA to designate the airspace over commercial nuclear power plants as "restricted airspace" under "special security instructions" codified in 14 CFR 99.7, which prohibit UAS from overflying these facilities without lawful cause. On October 28, 2020, one commercial nuclear power plant, Diablo Canyon Power Plant, was the first to receive "National Security" designation for restricted airspace from unauthorized overflights by UAS. Other commercial nuclear power plant licensees are considering requesting restricted airspace designation for their facilities. There is no near-term pathway to enabling licensees to take active counter-UAS actions.

The NRC staff is engaging in other interagency actions related to UAS, including potential legislative actions to remove barriers for critical infrastructure protection from UAS. The US DHS's Cybersecurity and Infrastructure Security Agency (CISA) established a working group related to small UAS which includes public and private sector partners. This working group provides a forum for public and private sector partners to develop best practices and recommendations associated with the mitigation of risk to critical infrastructure posed by small UAS. The working group also informs and makes recommendations to the U.S. Government on actionable, reliable, and scalable risk mitigation solutions for small UAS threats. The working group makes recommendations to assess and manage risks associated with small UAS security to: (1) inform Federal efforts to detect and mitigate small UAS threats to critical infrastructure; (2) enhance critical infrastructure capacity to assess vulnerabilities and effectively manage small UAS physical and cyber risks; and (3) enable the effective and secure integration of small UAS into critical infrastructure operations.

7. FUTURE LEGISLATION

U.S. Government agencies continue to take action to assist non-federal public and private entities in generating strategies to detect and mitigate UAS. For example, the National Security Council, with support from federal agencies, developed an action plan [20] documenting eight key recommendations addressing critical gaps in our ability to address UAS risk. One of the recommendations includes working with Congress to enact a new legislative proposal that reauthorizes existing C-UAS authorities for DHS/DOJ and expands certain authorities to better protect critical infrastructure. The proposal seeks to expand UAS detection authorities for State, Local, Tribal, and Territorial (SLTT) law enforcement agencies and critical infrastructure owners and operators. The proposal would also create a Federally-sponsored pilot program for selected SLTT law enforcement agency participants to perform UAS mitigation activities and a process that permits selected critical infrastructure owners

and operators to purchase authorized UAS mitigation equipment to be used by appropriate Federal or SLTT law enforcement agencies to protect their facilities.

8. CONCLUSIONS

The NRC staff continues to evaluate the threat in coordination with its Federal Partners for any changes that may impact NRC licensed facilities, materials, and/or activities. The NRC staff plans to update the 2019 assessment on UAS to: (1) Address UAS advancements in capabilities since the previous assessment and as observed during the conflict in Ukraine, including attributes such as speed, flight range, payload capacity, and tactical use; (2) Update prior scenarios in the study for realism, reducing conservatisms where appropriate, and determine if they remain valid or whether any new scenarios and/or vulnerabilities exist; and (3) If specific vulnerabilities are identified in the study, identify licensee mitigation strategies that can be employed today to attenuate those vulnerabilities and highlight future legislative changes and how they may impact licensee mitigation.

REFERENCES

[1] DHS, "Unmanned Aircraft Systems Addressing Critical Infrastructure Security Challenges", https://www.cisa.gov/topics/physical-security/unmanned-aircraft-systems/resources, (2017).

[2] Federal Remediation Technologies Roundtable, "Potential Use of Drones and Robotics for Radiological Characterization, Survey, and Emergency Response", https://frtr.gov/pdf/meetings/jun2022/abu-boby-stephanie-amoret-presentation.pdf , (2022)

[3] Pacific Northwest National Laboratory, "Drones for Decommissioning – Proof of Concept: PNNL-32519", Rev. 1, July 2022, Agencywide Documents Access and Management System Accession No. ML22196A040, (2022).

[4] Utility Fleet Professional, "DOMINION VIRGINIA POWER'S DRONE PROGRAM TAKES FLIGHT", https://utilityfleetprofessional.com/blog/dominion-virginia-power-s-drone-program-takes-flight , (2017).

[5] Drone Life, "Xcel Receives FAA Blessing to Fly BVLOS Power-line Drone Inspection" https://dronelife.com/2018/04/19/xcel-receives-faa-blessing-to-fly-bvlos-power-line-drone4-inspection/ , (2018).

[6] Southern Company, "Southern Company to Expand the Use of Unmanned Aircraft" https://www.southerncompany.com/newsroom/innovation/2016-09-06-unmanned-aircraft.html , (2016).

[7] World Nuclear News, "New drone for mapping radiation in nuclear plants," https://www.world-nuclear-news.org/Articles/New-drone-for-mapping-radiation-in-nuclear-plants. (2021).

[8] U.S. NRC, "Executive summary for "technical analysis of unmanned aerial vehicles for nuclear power plants and category I fuel cycle facilities" secy paper," https://www.nrc.gov/docs/ML1930/ML19302E409.pdf. (2019).

[9] Dominion Energy, "Drones Are Making Our Nuclear Operations Safer and Smarter", https://www.dominionenergy.com/our-stories/drones-are-making-our-nuclear-operations-safer-and-smarter , (2023).

[10] Reuters, "Ukraine to produce one million drones next year, Zelenskiy says", https://www.reuters.com/world/europe/ukraine-produce-one-million-drones-next-year-zelenskiy-says-2023-12-19/ , (2023).

[11] U.S. NRC, "Executive summary for "technical analysis of unmanned aerial vehicles for nuclear power plants and category I fuel cycle facilities" secy paper," https://www.nrc.gov/docs/ML1930/ML19302E409.pdf. , (2019)

[12] Kim M. Lawson-Jenkins, Fleurdeliza De Peralta, "Consideration of Cybersecurity Risks with the Use of Emerging Technologies" 2020 INMM annual meeting proceedings, (2020).

[13] Matthew Leccadito, et al, "A Survey on Securing UAS Cyber Physical Systems", IEEE Aerospace and Electronic Systems Magazin, (2018)

[14] U.S. NRC "Cyber Security Programs for Nuclear Power Reactors," https://www.nrc.gov/docs/ML2225/ ML22258A204.pdf , RG 5.71, Revision 1, (2023).

[15] The U.S. NRC, Security Advisory SA-22-08, "Recent Unmanned Aerial System Activity Over An NRC-Licensed Facility," (2022).

[16] White House, "The Domestic Counter-Unmanned Aircraft Systems National Action Plan", https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/25/fact-sheet-the-domestic-counter-unmanned-aircraft-systems-national-action-plan/, (2022).

[17] DHS, "Advisory on the Application of Federal Laws to the Acquisition and Use of Technology to Detect and Mitigate Unmanned Aircraft Systems," https://www.dhs.gov/publication/interagency-legal-advisory-uas-detection-and-mitigation-technologies , (2020).

[18] U.S. NRC, Security Advisory SA-21-06, "Updated Voluntary Reporting Guidelines For Suspicious Flyover Activity—Unmanned Aircraft Systems," (2021).

[19] U.S. NRC, “Cyber Security Programs for Nuclear Power Reactors,” https://www.nrc.gov/docs/ML2225/ ML22258A204.pdf., RG 5.71, Revision 1, (2023).

[20] The White House, “The Domestic Counter-Unmanned Aircraft Systems National Action Plan”, https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/25/fact-sheet-the-domestic-counter-unmanned-aircraft-systems-national-action-plan/ , (2022).