YEARBOOK OF UNWE (2025), ACADEMIC PUBLISHING HOUSE UNWE
ISSN (print): 1312-5486; ISSN (online): 2534-8949; http://unwe-yearbook.org/en/
DOI: https://doi.org/10.37075/YB.2025.1.03

ENHANCING NUCLEAR SECURITY TO COMBAT THE THREATS POSED BY SMALL UNMANNED AERIAL SYSTEMS

Sara Khalid Khider[1]
e-mail: sarakideir@gmail.com

Abstract

Drones, or small unmanned aerial systems, have introduced significant security challenges to critical infrastructure, particularly nuclear facilities. While these systems can serve a variety of purposes, they can also pose potential threats. This is due to their ability to carry malicious payloads, conduct surveillance, or cause physical damage. To enhance nuclear security protocols, it is necessary to integrate risk assessment strategies into a comprehensive approach that effectively mitigates these threats. This response examines how risk assessment strategies can be integrated with existing security frameworks to address evolving threats posed by small, unmanned aircraft systems. To neutralize potential threats, it is necessary to identify vulnerabilities, implement advanced detection systems, and establish response protocols. For security measures to be adapted to UAS technology capability, collaboration among stakeholders, including government agencies, industry experts, and technology developers, is essential. This paper examines the threats posed by UAS to nuclear security facilities, as well as protective measures taken to mitigate these risks.

Keywords: threat, drones, unmanned aircraft systems, nuclear security, risk assessment, security measures

JEL: Y80

Introduction

UAS are called by various names and acronyms by some regulators of the Federal Aviation Administration (FAA) such as pilotless aircraft, robot planes, remotely piloted vehicles, while the word "drone" is military in origin. According to the FAA Modernization and Reform Act of 2012, an unmanned aircraft is one that is operated without direct human intervention. In March 2003 Unmanned Aircraft Vehicles (UAV) Roadmap, the Office of the Secretary defense defines a powered aerial vehicle as one that does not need a human operator.

Defense defines a powered aerial vehicle as one that does not need a human operator, uses aerodynamic forces to provide vehicle lift, can be operated autonomously or remotely, can be expendable or recoverable, and can carry a lethal

[1] PhD Candidate, Department of National and Regional Security, University of National and World Economy, Bulgaria

or non-lethal payload. Among unmanned aerial vehicles are ballistic or semi-ballistic vehicles, cruise missiles, and artillery projectiles in recent guidance, the British define a UAV as "an aircraft without a pilot" (Mouroutsos, 2017). It is operated under remote control or in restricted autonomous modes of operation". According to the International Civil Aviation Organization (ICAO) and the European Commission, UAVs belong to a broader class of unmanned aircraft that can be programmed to operate autonomously.

Drones are usually embedded with a diverse range of cameras such as powerful and light video, infrared (or cryoscopy) cameras that send the most current information to ground-based equipment with or without payload. Most of them are equipped with IMU/GPS systems or access to Google Earth data, thermal/power/distance-photometric high-resolution sensors, and circuit boards with IP software for secure data storage. A wide range of tachymeters, altimeters, mobile hotspots, RFID tags, and other innovative technologies are used in the aerospace industry and in UAS. They can complete a wide variety of tasks but differ in shape, cost, and capability, depending on their purpose. Drones are small multicomputers of diverse sizes. They take off vertically either fixed-wing or rotary-wing and have multiple rotors to fly and balance while running on rechargeable batteries operated by a brushless electric motor.

The majority are remote-controlled, independent, or semi-autonomous while some can move, hover or perch with minimal human intervention. A human pilot can program the ground control using a tablet, onboard computer, and smartphone with a Wi-Fi connection, or a hobby airplane radio-controlled for low altitude and displayed with buttons, switches, and sounds. They can manage timed and autonomous missions. ("Classification of Drones – AJER") This considers measurements of the wing, lithium polymer battery level, national flight regulations, and site data. They also manage lateral obstacles based on artificial and intelligent models with little or no fossil fuel.

Drones gain in sophistication and accessibility; nuclear facilities face substantial security concerns. The use of drones, commonly referred to as UAS, for accessing restricted areas, sabotage facilities, or transporting hazardous materials could be exploited. Artificial intelligence could eagle drones to bypass traditional physical security barriers, resulting in nuclear material theft or disruption of critical operations, for example. This misuse of UAS technology could lead to catastrophic outcomes, including the construction of a "dirty bomb" or severe damage to power-generating infrastructure.

This paper analyzes the potential threats UAS pose to nuclear security. An evaluation of nuclear facilities' vulnerability to drone attacks is provided, along with strategies for mitigating those risks. By understanding UAS capabilities and their potential for misuse, stakeholders can better prepare for them. By examin-

ing UAS capabilities and analyzing incidents involving drone-related security breaches at nuclear facilities, stakeholders can gain critical insight into vulnerabilities that drones may exploit. This understanding enables them to better prepare for and implement targeted countermeasures to mitigate these emerging threats. This strengthens nuclear facility security against future incidents.

Methodology

This qualitative research employs a document-based analytical method to examine the security challenges posed by Unmanned Aerial Systems (UAS) to nuclear facilities. The study draws upon a wide range of secondary data sources, including peer-reviewed academic literature, policy papers, incident reports, and international guidelines from organizations such as the International Atomic Energy Agency (IAEA) and the International Civil Aviation Organization (ICAO). Through systematic document analysis, the research identifies trends in UAS-related incidents, evaluates vulnerabilities within nuclear security frameworks, and assesses the adequacy of current detection and response measures.

A comparative analytical approach is applied to explore variations in national and institutional counter-UAS strategies, emphasizing best practices and areas requiring improvement. The study integrates established theories of risk assessment and nuclear security management to contextualize findings within a structured conceptual framework. This methodological approach enables the synthesis of diverse information to provide a coherent understanding of how evolving drone technologies intersect with nuclear security, and how mitigation strategies can be effectively adapted to address emerging aerial threats

Assessing the Threat landscape

Recently, small, unmanned aircraft have been enhanced in autonomy, payload capacity, and endurance. These advancements have made them attractive tools for malicious actors, including terrorists and rogue states, who can exploit their capabilities for sabotage, espionage, or the delivery of harmful substances (Wilson et al., 2020; Kallenborn, 2022). These small aircraft can be used to attack critical infrastructure, military bases, and public events. They can also deliver chemical, biological, or nuclear materials to targeted locations. As a result, there is a growing need for effective countermeasures to detect and neutralize these threats. The proliferation of low-cost, commercially available UAS has further exacerbated the threat, as these systems can be easily modified for nefarious purposes (Pettit, 2020; Puranik, 2021). Recent incidents involving UAS breaches at nuclear facilities highlight the urgency of addressing this threat. For instance, several nuclear power plants in France have experienced unauthorized UAS intrusions, raising

concerns about the potential for similar incidents elsewhere (Solodov et al., 2018; Araujo, 2017). These events underscore the need for robust risk assessment strategies to identify vulnerabilities and implement effective countermeasures. For example, in 2015, a drone carrying radioactive material landed on the roof of the Japanese Prime Minister's office. This highlights the potential for UAS to be used in terrorism (BBC News, 2015).

Legal and Regulatory Frameworks

The strength and clarity of national regulatory frameworks are also crucial for addressing drone-related threats to nuclear security. In the USA there are two main agencies responsible for airspace control and enforcing "no-fly zones" around critical infrastructure in the United States: The Federal Aviation Administration (FAA) and the Nuclear Regulatory Commission (NRC), which establishes safety measures and incident response requirements for facilities (FAA, 2023; NRC, 2022). It is important to keep these two agencies separate to maintain specialized oversight, but it can cause a slowdown in cross-agency coordination when threats are rapidly changing.

Ukraine adopted a more centralized and adaptive approach during wartime, combining regulatory and operational control through emergency legislation in order to integrate the two in a more centralized manner (State Aviation Administration of Ukraine, 2023). As a result of this framework, counter-g UAS operations were authorized quickly, and a closer coordination between defense, intelligence, and energy agencies was established so as to protect nuclear sites from drone attacks.

In analyzing these frameworks, it is important to note that there is a tension between maintaining distributed regulatory authority for precision and accountability or consolidating it for speed and flexibility under conditions of high threat (OECD Nuclear Energy Agency, 2023).

Drone Threat to Non-Nuclear Security: A Growing Concern

As unmanned aerial vehicles (UAVs) develop rapidly and become more accessible, significant concerns have been raised about their misuse in non-nuclear security contexts. Several high-profile incidents have disrupted critical infrastructure, challenged law enforcement, and threatened public safety. It was revealed that government facilities are vulnerable, even when highly secure, when a civilian drone struck the White House in January 2015. The incident was later attributed to an off-duty, intoxicated intelligence employee using a commercial UAV (BBC News, 2015). As a result of suspected terrorist attacks on spectators and athletes during the Rio Olympic Games, UAVs threaten mass gatherings (Moore, 2016). Al Jazeera (2022) reports that drones were used to target fuel tanks in Abu Dhabi in

January 2022, resulting in fatalities and exposing critical energy infrastructure to aerial threats. Greenpeace's use of drones to crash a Superman-shaped drone into a French nuclear plant highlights the ease with which UAVs bypass security and capture public attention, emphasizing vulnerabilities in security systems across sectors (Pradier, 2018). The sighting of drones above the Savannah River Site has also prompted federal investigations into unknown UAV operators operating in secure zones (Gardiner, 2016). Drones, while commonly used recreationally, pose a significant threat to non-nuclear security, necessitating urgent policy and technological responses (Solodov et al., 2017; Dukasiewicz, 2020).

Threat to the Nuclear Facility

Unauthorized Access to Nuclear Facilities

In nuclear facilities, the use of small unmanned aerial systems (UAS) represents a significant and evolving security challenge. By circumventing perimeter barriers, surveillance networks, and access control mechanisms, these systems circumvent traditional physical security measures. The reason for this is their small size, maneuverability, and ability to operate in restricted airspace. Such intrusions pose considerable risks, including the delivery of explosive devices, the illicit transport of hazardous or radioactive materials, intelligence gathering, and the potential sabotage of critical infrastructure (Shin et al., 2023; Solodov et al., 2018; Meliana et al., n.d.). Furthermore, the widespread availability and low cost of commercial off-the-shelf (COTS) drones increase the likelihood of exploitation by non-state actors, terrorists, or other malicious entities. These developments underscore the necessity for nuclear facilities to implement comprehensive counter-UAS strategies, encompassing advanced detection technologies, real-time threat assessment protocols, and rapid response mechanisms to mitigate the associated risks effectively.

Threats Posted by Unauthorized Access

Unauthorized access by small unmanned aerial systems (UAS) poses a multifaceted threat to nuclear facilities, combining operational, cyber, and intelligence-gathering risks. Physically, small UAS can be outfitted with explosives or hazardous payloads capable of inflicting considerable damage, thereby endangering facility integrity and public safety (Shin et al., 2023; Solodov et al., 2018). From a cyber-physical perspective, drones may serve as delivery mechanisms for malware or perform reconnaissance to facilitate digital intrusions targeting critical infrastructure (Tavares et al., 2022; Popova & Chechulin, 2023). A key concern is the surveillance capability of these platforms: small UAS can covertly collect detailed intelligence on facility layouts, security protocols, and operational routines (Swinney & Woods, 2022; Afonin et al., 2024). Such data can be

exploited to plan coordinated attacks or identify systemic vulnerabilities. The increasing use of drones for unauthorized surveillance highlights the urgent need for robust, integrated countermeasures to safeguard nuclear assets from these emerging airborne threats**.**

Nuclear Security Measures Against Drones

Methods of Unauthorized Surveillance

Through various unauthorized surveillance methods, unmanned aerial systems (UAS) pose a significant threat to nuclear security. With high-resolution cameras, drones can provide aerial reconnaissance images of critical infrastructure, revealing sensitive areas like reactor cores, fuel storage, and perimeters (Swinney & Woods, 2022; Afonin et al., 2024). Furthermore, modern UAS possesses capabilities for real-time video transmission, allowing adversaries to monitor facility operations dynamically, tracking security patrols, observing routine activities, and identifying operational patterns (Solodov et al., 2018; Zhang & Chandramouli, 2019). In addition, aerial surveillance data can be exploited to support cyberattack planning, as drone reconnaissance can reveal the layout of digital communication assets and infrastructure vulnerabilities (Tavares et al., 2022; Popova & Chechulin, 2023). In response to these threats, nuclear facilities must adopt a layered defense strategy incorporating detection, delay, and response mechanisms. This is to prevent unauthorized drone access and mitigate surveillance risks effectively.

Detection, Delay, and Response Strategies

A variety of countermeasures have been developed and implemented to mitigate small UAS risks. These countermeasures can be divided into detection, delay, and response strategies. UAS Detection Strategies: Radar-Based Detection: Radar systems are widely used to detect UAS in nuclear facilities' vicinity and to track their movement, providing early warning of potential threats. (Liaquat et al., 2024; Famili et al., 2021). Acoustic Sensors: Acoustic sensors detect UAS noise patterns, allowing the identification and localization of these devices. This method is particularly effective in environments with minimal background noise (Famili et al., 2021; Zhang & Kusrini, 2021). RF-Based Detection: Radio frequency (RF) sensors can detect communication signals emitted by a UAS, enabling identification of both the drone and its controller. This method disrupts the command-and-control link between the UAS and its operator (Slimeni and Dalleji, 2022; Roy et al., 2019). Delayed Strategies: GPS Spoofing: GPS spoofing involves transmitting false GPS signals to the UAS, losing its navigational capabilities. This method can be implemented to redirect the UAS away from the facility or force it to land (Liaquat et al., 2024; Maksimovic, 2023). Jamming of RF signals can disrupt the communication link between a UAS and its controller.

Effectively neutralizing the threat this method is particularly useful in scenarios where the UAS is used for malicious purposes (Slimeni and Dalleji, 2022; Roy et al., 2019). After a UAS is detected and identified as a threat, a variety of neutralizing devices can be used. These include net guns, laser systems, and physical interceptors, which can disable or destroy the UAS (Shin et al., 2023; Maksimovic, 2023). Legal and Regulatory Measures: Strengthening legal frameworks and regulatory measures is crucial to preventing UAS misuse. This includes strict licensing requirements, mandatory UAS registration, and the establishment of no-fly zones around critical infrastructure (Barka et al., 2019).

Security Risks at Nuclear Facilities

According to nuclear security experts, increasing use of unmanned aerial vehicles (UAVs) poses several new threats to nuclear facilities. There are conventional as well as novel risks, such as unauthorized data collection, direct physical attacks, diversionary tactics, smuggling contraband near secure access points, and the purposeful creation of distractions called "wild UAV chases".

Despite significant security improvements implemented after 9/11, nuclear facilities remain vulnerable. An independent nuclear power expert at the Union of Concerned Scientists has claimed that upgrades made by the Nuclear Regulatory Commission (ory) have not eliminated suicide aircraft threat. Current security measures could be overwhelmed by an orchestrated attack involving multiple UAVs equipped with explosives. The threat posed by UAVs to nuclear facilities can be effectively analyzed through adversary objectives, which categorize the risks posed by these technologies. The objectives include reconnaissance and intelligence gathering with UAVs; smuggling is the transport of contraband into or out of restricted zones with UAVs; kinetic attacks are the direct delivery of explosives or weapons by UAVs; electronic attacks are directed at disrupting facility operations through cyber or electronic interference; distraction is the use of UAVs to divert security forces and facilitate other malicious activities. It is important to understand that these threats can manifest individually, simultaneously, or in conjunction with traditional methods such as ground-based attacks, posing complex and multifaceted challenges to nuclear security systems (Solodov et al., 2017).

Analysis of Accidents that Happened by Drones at Nuclear Facilities

A growing threat to nuclear infrastructure has been posed by unmanned aerial systems (UAS) in recent years. From surveillance and psychological operations to kinetic attacks and smuggling attempts, drones have exploited critical security gaps at facilities. This table (1) describes key incidents involving drones near or near nuclear facilities, highlighting nature, implications, and institutional responses.

Table 1: Overview of Drone Incidents Involving Nuclear Facilities

Date	Location	Facility Type	UAS Type	Description	Response	Reference
1	2	3	4	5	6	7
Fall 2014	France	Nuclear Power Plants	Civilian Drones	Multiple unidentified drones flew over 13 of 19 facilities, often simultaneously.	EDF filed complaints; French parliament tightened drone regulations.	Lochbaum (2015)
Jan 2015	USA (White House)	Government Facility	Civilian UAV	UAV crashed on White House grounds; operated by intoxicated government employee.	No injuries/ damage; raised UAV regulation concerns.	Lochbaum (2015)
Jan 2015	UAE	Civil Aviation (Dubai)	Recreational UAV	UAV halted all air traffic for 55 minutes at Dubai Airport.	Significant economic disruption.	The National (2015)
Jul 2016	USA (Savannah River Site)	Nuclear Facility	Unknown UAVs	Eight UAVs sighted in late June–July 2016; origins unknown.	Federal investigation launched.	Gardiner, 2016
2012	Sweden (Ringhals)	Nuclear Power Plant	Smuggling Attempt	Explosives found in a truck entering the facility; UAV-based smuggling theorized.	No charges filed; highlighted security vulnerability.	Łukasiewicz (2020)
2016	Brazil (Rio Olympics)	Public Event	Terror Plot via UAV	Al-Qaida operatives planned UAV attacks on athletes and spectators.	Brazilian police arrested ten suspects.	Moore (2016)

Continued

1	2	3	4	5	6	7
2018	France (Bugey)	Nuclear Power Plant	Activist Drone	Greenpeace crashed a Superman-shaped drone into a nuclear reactor building.	No damage; criticized for lack of preparedness.	Pradier (2018)
Sep 2019	USA (Palo Verde)	Nuclear Power Plant	Small Drones	Swarms flew over Units 1 and 3 on consecutive nights.	NRC recorded an incident; called for better UAV defense.	NRC Reports
2021–2023	UK	Various Nuclear Sites	Civilian Drones	~25 drone-related events logged by MOD Police; mostly false alarms or accidental.	Protocols reviewed; no major breaches.	MOD Police Reports
Jan 8, 2025	USA (Minnesota)	Prairie Island NPP	Hobbyist Drones	2–5 drones spotted; no threat confirmed.	Police investigated; no suspects found.	Local Police Reports
Feb 14, 2025	Ukraine (Chernobyl)	Decommi-ssioned Reactor	Russian Armed Drone	Drone damaged the New Safe Confinement roof (~500 sq ft) and caused a fire.	IAEA condemned; emergency response activated.	IAEA (2025)
Dec 10, 2024	Ukraine (near Zaporizhzhia)	Nuclear Power Plant	Attack Drone	The drone struck an IAEA-marked car near the plant; no injuries.	IAEA condemned the strike; called it deliberate.	IAEA (2024)
Feb 12, 2025	Ukraine (Enerhodar)	Nuclear Power Plant	Attack Drones	Multiple drones struck ~300m from a reactor.	IAEA confirmed normal radiation; warned all parties.	IAEA (2025)
Aug 2024	Ukraine (Zaporizhzhia)	Nuclear Power Plant	Ukrainian Drone	Drone dropped explosives ~100m from critical power line.	IAEA stated this showed “escalation;” assessed site.	IAEA (2024)

Continued

1	2	3	4	5	6	7
Apr 2025	Ukraine (Zaporizhzhia & SU)	Nuclear Power Plants	Unidentified Drones	Multiple drones spotted near plants; operators went indoors due to nearby threats.	Temporary operation pauses; IAEA called the risk "unsustainable."	IAEA (2025)
Aug 2024	Germany (Brokdorf)	Decommi-ssioned NPP	Suspected Military	Repeated drone overflights: one high-speed drone suspected to be Orlan-10.	Prosecutors launched a probe; security heightened.	German Prosecutors (2024)
Oct 25, 2023	Khmelnytskyi, Ukraine	Nuclear Power Plant	Military Drone	Drone explosions near administrative buildings shattered windows; no reactor damage.	IAEA expressed critical concern; highlighted risks to nuclear security in conflict zones.	Grossi, IAEA (2023)
Feb 14, 2025	Ukraine (Chernobyl)	Decommi-ssioned Reactor	Russian Armed Drone	Drone damaged the New Safe Confinement roof (~500 sq ft) and caused a fire.	IAEA condemned; emergency response activated.	IAEA (2025)
Dec 10, 2024	Ukraine (near Zaporizhzhia)	Nuclear Power Plant	Attack Drone	The drone struck an IAEA-marked car near the plant; no injuries.	IAEA condemned the strike; called it deliberate.	IAEA (2024)
Feb 12, 2025	Ukraine (Enerhodar)	Nuclear Power Plant	Attack Drones	Multiple drones struck ~300m from a reactor.	IAEA confirmed normal radiation; warned all parties.	IAEA (2025)

Note: Full reference for the source is available in the reference section

Source: Composed by the author

Analysis

Unmanned aerial systems (UAS) threaten nuclear facilities including four primary risk types: surveillance and reconnaissance, kinetic attacks, smuggling illicit materials, and psychological or operational disruption. Surveillance-oriented overflights such as coordinated drone incursions in France (2014) and recurring sightings in the UK (2021 – 2023) suggest efforts to gather intelligence or test response protocols. More alarming are kinetic attacks like those witnessed in Ukraine during 2024 – 2025, where drones damaged infrastructure near or at nuclear sites. This highlights the escalating use of UAS in active conflict zones. Smuggling attempts, as suspected in the 2012 Ringholes incident in Sweden, raise concerns about drones delivering hazardous payloads undetected.

Current nuclear security systems exhibit significant vulnerabilities despite the increasing frequency and diversity of these threats. Most facilities are unable to detect drones real-time through radar, acoustic, or radio frequency (RF) monitoring. Small, commercially available drones can easily bypass no-fly zones around nuclear sites, even though they are legally designated. In several areas, drones must be intercepted or neutralized before they can be used, especially in civilian airspace, which often results in inconsistent or delayed responses from law enforcement.

To resolve these deficiencies, several implications emerge for facility design and policies. In addition to radar, radio frequency, and acoustic sensors, counter-UAS measures such as jammers, drone catch nets, and autonomous interceptors must be deployed. In addition, drone incursions must be responded to rapidly and proportionately through international and national legal frameworks. As a third step, nuclear facility staff should undergo scenario-based training so they can integrate UAV threats into existing physical and cyber-security protocols. Finally, red-teaming exercises and adversarial simulations can be conducted to stress-test current systems and improve incident response time. From a research standpoint, the growing threat environment offers several urgent opportunities. These include the development of autonomous swarm detection algorithms, new containment structure designs resistant to drone-delivered explosives, and electromagnetic shielding technologies to protect sensitive equipment. Simulation studies analyzing blast and sabotage effects from UAS payloads could further guide resilient facility design and emergency planning. As UAS technologies evolve, so too must strategies to safeguard the nuclear sector from misuse.

Enhancing Nuclear Security Against UAS Threats

Technology Solutions

A variety of technologies are used to detect drone threats to nuclear facilities, each with unique strengths and limitations. Radar systems can operate in diverse weather conditions and cover large areas. Aerial objects are detected and tracked using radio waves. Their accuracy, however, may be compromised by their price and difficulty distinguishing between drones and other flying objects (Famili et al., 2021). Acoustic sensors, which detect drone motor and propeller sound, make a cost-effective solution for urban deployment. However, their performance is compromised by ambient noise and distance, limiting their range and reliability (Famili et al., 2021). Optical sensors, such as cameras and imaging systems, provide high-resolution visual identification of drones and can be integrated with other systems to improve detection. It is important to note, however, that their effectiveness is diminished when the light is poor or when it is long distances (Famili et al. 2021).

A radio frequency detection system allows drones and their controllers to be identified through the signals they emit. However, they may not be effective against drones that operate in stealth mode or use encrypted or frequency-hopping signals (Famili et al., 2021). While these technologies form the backbone of modern counter-UAS strategies, their limitations highlight the need for integrated, multilayered detection systems tailored to nuclear facility security requirements.

Policies and regulations need to address gaps.

Due to evolving regulations complexities, traditional security frameworks for nuclear facilities are increasingly challenging. The absence of clear, harmonized policies outlining which types of UAVs are permitted in specific airspace is a major gap. Security decisions for nuclear facilities are directly impacted by regulatory ambiguity. Operating unmanned aerial systems (UAS) near nuclear facilities, particularly during material transport, has a complex and evolving regulatory landscape. Furthermore, international operations involving UAS may be governed by bilateral or treaty agreements in addition to local government restrictions. Private property owners have limited legal authority to restrict drone flights over their property under federal airspace area. Critical infrastructure managers, including nuclear power plants, face challenges due to the fragmented regulatory framework. By understanding federal, state, and local laws, they can ensure full compliance and avoid legal liability. To prevent unauthorized or malicious drone attacks on nuclear facilities, a coordinated regulatory approach may be necessary. Furthermore, these regulatory challenges complicate collaboration with the host nation's competent security authorities, who set and enforce physical protection standards. Increasing threats include both malicious and inadvertent UAV use,

causing existing national policies to not adequately reflect current risks. As the threat environment evolves, key security frameworks, such as the DBT, must be revised. Nuclear licensees must develop robust physical protection against adversaries with DBT. Nuclear facilities remain vulnerable to emerging aerial threats if UAV-related vulnerabilities are not addressed in these frameworks (Solodov et al., 2024).

Operational & Procedural Improvements

An effective response to emerging threats posed by small Unmanned Aircraft Systems (UAS) will require comprehensive, well-organized improvements to nuclear security procedures and operations. To enhance real-time situational awareness and ensure accurate identification and tracking of potential threats, multi-sensor detection systems such as radar, optical, acoustic, and radiofrequency (RF) sensors are deployed as a key component of this strategy (Swinney & Woods, 2021). When combined with continuous monitoring platforms, these systems reduce the probability of undetected intrusions and enable faster response times (Jurás, 2023). Once a threat is detected, it is crucial to have coordinated neutralization methods in place. A layered defence approach that combines soft-kill techniques, such as jamming and spoofing, with hard-kill methods, including net-based interceptors or kinetic drones, offers flexible options depending on the scenario (Horváth, 2024). As an example, advanced systems such as Drone-Cop integrate surveillance and interceptor drones, demonstrating how autonomous platforms can work together to defend high-value targets (Shin et al., 2023). As well as technology, effective implementation requires structured operational planning, such as conducting regular threat assessments, developing pre-emptive response protocols, and enforcing drone exclusion zones with automated alerts. Security personnel must receive specialized training in implementing these plans. They should also participate in regular simulation drills and joint exercises to ensure they are prepared for diverse threat scenarios. Also, interagency coordination is critical to streamlining communications and responding to incidents between facility operators, local law enforcement, and national regulatory bodies. Additionally, UAS can be used as vectors for cyberattacks or data intercepts as well as for physical intrusions. Cybersecurity integration is another layer of protection. Lastly, any operational improvements must be aligned with the legal and regulatory frameworks, so counter drone technologies comply with airspace laws, privacy concerns, and the lawful authority to interfere with signals. To combat evolving aerial threats, nuclear facilities can align technological tools, personnel readiness, interagency collaboration, and legal compliance.

Recommendations

The increasing capabilities and accessibility of Unmanned Aerial Systems (UAS) present complex challenges to nuclear security. Effective mitigation requires multi-layered strategies that integrate technology, operational practices, and regulatory measures. Recommendations are organized according to four primary threat categories: surveillance, smuggling, kinetic attacks, and operational disruption.

Surveillance Threat Mitigation

- Integration of Multi-Modal Detection Systems by Combine radar, radiofrequency, acoustic, and electro-optical sensors into a unified real-time detection framework to identify unauthorized UAS incursions.
- Algorithmic Threat Assessment: Employ machine learning and artificial intelligence to detect anomalous flight patterns and support predictive threat analysis.
- Airspace Control and Geofencing: Establish controlled airspace zones around facilities and implement monitoring systems to enforce no-fly areas.

Smuggling and Illicit Delivery Prevention

- Enhanced Perimeter Detection through Utilize ground-based sensors, low-altitude radar, and motion-triggered cameras to detect drones approaching sensitive areas.
- Conduct regular testing of perimeter security and simulated smuggling attempts to evaluate detection effectiveness.
- Develop clear national and facility-specific protocols for responding to unauthorized drone deliveries.

Kinetic and Explosive Threat Mitigation

- Deploy automated interception technologies, such as drone-capture mechanisms or direct-energy systems, to neutralize hostile drones with minimal collateral damage.
- Reinforce critical facility infrastructure to withstand explosive or kinetic impacts, including blast-resistant containment and electromagnetic shielding.
- Develop detection algorithms and rapid-response protocols to counter coordinated multi-drone attacks.

Operational Disruption and Psychological Risk Mitigation

- Conduct regular simulated UAS incidents to enhance decision-making under stress and improve inter-agency coordination.
- Align physical security and cybersecurity protocols to address blended attacks that exploit both domains.
- Establish rapid alert and coordination mechanisms among facility operators, airspace regulators, and law enforcement to ensure timely threat mitigation.

Cross-Sector and International Collaboration

- Facilitate cooperation between technologists, policymakers, behavioral scientists, and nuclear security professionals to develop comprehensive security strategies.
- Harmonize security practices, incident reporting, and training programs across facilities and countries to enable shared preparedness.
- Regularly assess technological trends, operational procedures, and regulatory frameworks to ensure defenses remain effective against evolving UAS threats.

Conclusion

Due to the proliferation of small unmanned aerial systems (UAS), nuclear facility security is seriously threatened. As demonstrated by recent incidents and evolving tactics, drones have become capable of surveillance, delivering payloads, and facilitating hyperphysical attacks. These attacks are conducted with ever enhanced precision and stealth. Several current security frameworks lack the capability to detect, intercept, and provide legal authority, leaving strategic weaknesses that adversaries can exploit. To address these vulnerabilities, technological advancements, policy reforms, and operational readiness are required. To build a resilient defense posture against aerial intrusions, the nuclear sector can invest in detection systems, strengthen infrastructure, and conduct scenario-based training. It will be imperative to continue research and cross-sector cooperation to protect nuclear assets from drone-enabled threats.

References

Afonin, I. E., Makarenko, S. I., & Ivanov, M. S. (2024). Unmanned aerial vehicles as a reconnaissance object, Journal Achievements of Modern Radioelectronics, №5, https://doi.org/10.18127/j20700784-202405-06

Al Jazeera. (2022). Two dead in Abu Dhabi fuel tank explosion after suspected drone attack, available at: https://www.aljazeera.co m/news/2022/1/17/two-dead-in-abu-dhabi-after-fuel-tank-explodes (accessed 24 May 2025)

Araujo, K. (2017). Disruptive Change in Unmanned Aerial Systems, Nuclear Facilities, and Radiological Protection: A Review of U.S. and French Developments

Barka, E., Kerrache, C. A., Benkraouda, H., Shuaib, K., Ahmad, F., & Kurugollu, F. (2019). Towards a trusted unmanned aerial system using blockchain for the protection of critical infrastructure, https://doi.org/10.1002/ETT.3706

Famili, A., Stavrou, A., Wang, H., Park, J.-M., & Gerdes, R. M. (2021). Securing your Airspace: Detection of Drones Trespassing Protected Areas, arXiv: Signal Processing, https://arxiv.org/abs/2111.03760

Federal Aviation Administration. (2023). Unmanned Aircraft Systems (UAS) regulations and airspace restrictions, U.S. Department of Transportation, https://www.faa.gov/uas

Gardiner, J. (2016). UAV sightings over Savannah River Site prompt federal probe', *The Augusta Chronicle*, 15 July.

Grossi, R. (2023). IAEA Director General Statement on Khmelnytskyi Attack, International Atomic Energy Agency, available at: https://www.iaea.org (accessed 24 May 2025)

Horváth, G. (2024). No Drone's Sky: Full Spectrum Drone Surveillance and Neutralization Concept for Enhanced Counter-UAS Framework, Hadmérnök, 19(2), pp. 107-121, https://doi.org/10.32567/hm.2024.2.9

International Atomic Energy Agency. (2025). IAEA Reports. (2024 – 2025). Updates on Ukraine Nuclear Safety Incidents, available at: www.iaea.org

Jurás, Z. (2023). Relevant Tasks for UAV Protection Systems in Relation to the Aerial Scenario of Nuclear Facilities, Science & Military, 18(1), pp. 39-44, https://doi.org/10.52651/sam.a.2023.1.39-44

Kallenborn, Z. (2022). A Plague of Locusts? A Preliminary Assessment of the Threat of Multi-Drone Terrorism, Terrorism and Political Violence, pp. 1-30, https://doi.org/10.1080/09546553.2022.2061960

Liaquat, S., Faizan, M., Chattha, J. N., Butt, F. A., Mahyuddin, N. M., & Naqvi, I. H. (2024). A framework for preventing unauthorized drone intrusions through radar detection and GPS spoofing, Ain Shams Engineering Journal, https://doi.org/10.1016/j.asej.2024.102707

Lochbaum, D. (2015). Unidentified Drones Over French Nuclear Plants: How Big Is the Risk?, Union of Concerned Scientists.

Łukasiewicz, J. (2020). Drones in the context of nuclear security – risk analysis, Journal of Konin University, [online], available at: https://konin.edu.pl (accessed 19 May 2025)

Łukasiewicz, J. (2020). Security Implications of Drones in Nuclear Facilities, Polish Institute of International Affairs.

Maksimovic, G. (2023). Countering the threat of unmanned aerial systems to critical infrastructure, https://doi.org/10.70995/cyoj3379

Meliana, A., Sari, Y. M., Junianto, I. D., & Intaningrum, D. (2024). Review of unmanned aerial vehicle (UAV) threat preparedness in the nuclear facility in Serpong area of the national research and innovation agency, https://doi.org/10.1063/5.0192910

Moore, J. (2016). Brazil arrests 10 suspected ISIS supporters ahead of Rio Olympics, Newsweek, 21 July, available at: https://www.newsweek.com

NRC. (2019). UAV Activity Over Palo Verde NPP, Incident Reports.

Nuclear Regulatory Commission. (2022). Security requirements for nuclear facilities and radioactive material, U.S. Government Publishing Office, available at: https://www.nrc.gov/security

OECD Nuclear Energy Agency. (2023). Emerging risks: The use of unmanned aerial systems around nuclear facilities, OECD Publishing, available at: https://www.oecd-nea.org

Pettit, D. M. (2020). Cyber Risk Assessment and Scoring Model for Small Unmanned Aerial Vehicle, available at: https://scholar.afit.edu/cgi/viewcontent.cgi?article=4592&context=etd

Popova, V., & Chechulin, A. (2023). Ranking Countermeasures Against Cyberattacks in Cyberphysical Systems of Critical Infrastructure Facilities, pp. 522-527, https://doi.org/10.1109/uralcon59258.2023.10291141

Pradier, J. (2018). Greenpeace drone crashes into French nuclear plant to show security flaws, Reuters, 3 July, available at: https://www.reuters.com (accessed 19 May 2025)

Puranik, T. G. (2021). The Impacts of Proliferation and Autonomy of Small Unmanned Aircraft Systems on Security, Springer, Cham, pp. 33-52, https://doi.org/10.1007/978-3-030-73655-2_4

Roy, F. Le, Roland, C., Le Jeune, D. and Diguet, J.P. (2019). Risk assessment of SDR-based attacks with UAVs, International Symposium on Wireless Communication Systems, pp. 222-226, doi:10.1109/ISWCS.2019.8877144.

Shin, H., Choi, S. C., Kim, S., & Cho, S. (2023). Anti-drone System and Operation Framework for the Security of National Major Facilities, 29(8), pp. 592-598, https://doi.org/10.5302/j.icros.2023.23.0050

Solodov, A. A., Williams, A. D., Hanaei, S. A., & Goddard, B. (2018). Analyzing the threat of unmanned aerial vehicles (UAV) to nuclear facilities, Security Journal, 31(1), pp. 305-324, https://doi.org/10.1057/S41284-017-0102-5

Solodov, A.A., Williams, A.D., Al Hanaei, S., and Goddard, B. (2024). Analyzing the Threat of Unmanned Aerial Vehicles (UAV) to Nuclear Facilities, Khalifa

University, Gulf Nuclear Energy Infrastructure Institute (GNEII), Sandia National Laboratories and Virginia Commonwealth University.

Solodov, A.A., Williams, A.D., Al Hanaei, S. and Goddard, B. (2017). Security Implications of Civilian UAVs at Nuclear Facilities, Proceedings of the Institute of Nuclear Materials Management Annual Meeting.

State Aviation Administration of Ukraine. (2023). Emergency measures on unmanned aircraft use during martial law, Government of Ukraine, available at: https://avia.gov.ua

Swinney, C. J., & Woods, J. C. (2022). A Review of Security Incidents and Defence Techniques Relating to the Malicious Use of Small Unmanned Aerial Systems, (How to prevent malicious use of intelligent unmanned swarms?), IEEE Aerospace and Electronic Systems Magazine, 37, pp. 14-28, https://doi.org/10.1109/MAES.2022.3151308

Slimeni, F. and Dalleji, T. (2022). RF-based mini-drone detection, identification and jamming in no-fly zones using software-defined radio. Center for Military Research, https://doi.org/10.21203/rs.3.rs-1781329/v1

Tavares, R. L., Albuquerque, R. de O., & Giozza, W. F. (2022). Effective evaluation of a nuclear facility security system under a cyber-physical attack scenario, 17th Iberian Conference on Information Systems and Technologies (CISTI), pp. 1-6, https://doi.org/10.23919/cisti54924.2022.9820179

The National. (2015). Drone crashes on White House lawn, raises security questions, The National, 26 January.

The National. (2015). Drone Halts Air Traffic at Dubai International Airport for Nearly an Hour, The National, 23 January.

Wilson, B., Tierney, S., Toland, B., Burns, R. M., Steiner, C. P., Adams, C. S., Nixon, M., Khan, R., Ziegler, M. D., Osburg, J., & Chang, I. (2020). Small Unmanned Aerial System Adversary Capabilities, RAND Corporation, https://doi.org/10.7249/RR3023

Zhang, X., & Chandramouli, K. (2019). Critical Infrastructure Security Against Drone Attacks Using Visual Analytics, Springer, Cham. pp. 713-722, https://doi.org/10.1007/978-3-030-34995-0_65