Analyzing the Threat of Unmanned Aerial Vehicles (UAV) to Nuclear Facilities

Alexander Solodov[1,2,*], Adam Williams[3], Sara Al Hanaei[1], Braden Goddard[4]

[1]Department of Nuclear Engineering, Khalifa University, Abu Dhabi, UAE
[2]Gulf Nuclear Energy Infrastructure Institute (GNEII), Abu Dhabi, UAE
[3]Sandia National Laboratories**, New Mexico, USA
[4]Department of Mechanical and Nuclear Engineering, Virginia Commonwealth University, Virginia, USA

Abstract

Unmanned aerial vehicles (UAV) are among the major growing technologies that have many beneficial applications, yet they can also pose a significant threat. Recently, several incidents occurred with UAVs violating privacy of the public and security of sensitive facilities, including several nuclear power plants in France. The threat of UAVs to the security of nuclear facilities is of great importance and is the focus of this work. This paper presents an overview of UAV technology and classification, as well as its applications and potential threats. We show several examples of recent security incidents involving UAVs in France, USA, and United Arab Emirates. Further, the potential threats to nuclear facilities and measures to prevent them are evaluated. The importance of measures for detection, delay and response (neutralization) of UAVs at nuclear facilities are discussed. An overview of existing technologies along with their strength and weaknesses are shown. Finally, the results of a gap analysis in existing approaches and technologies is presented in the form of potential technological and procedural areas for research and development. Based on this analysis, directions for future work in the field can be devised and prioritized.

I. Introduction

The modern world is changing rapidly with the development of new technologies constantly emerging and revolutionizing approaches to various tasks. Together with significant benefits, come many ways of using technology for malicious purposes. Unmanned aerial vehicles (UAVs)[1] are not an exception to this trend. The recreational and commercial use of UAVs is on a steep increase. UAVs are being actively used for multiple recreational activities, such as photography, videography and the sheer enjoyment of flight. They are also gaining popularity

* Currently at Sandia National Laboratories, Albuquerque, NM, USA

** Sandia National Laboratories is a multiprogram laboratory operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. Journal Submission/Peer Review Approved.

[1] We have chosen the term 'unmanned aerial vehicles' or UAVs as a catch-all phrase for remotely-piloted or autonomously-guided small, robotic flying vehicles. Other names, which have specific connotative and denotative meanings, include: remotely piloted vehicle (RPV), unmanned aircraft (UA), unmanned aircraft system (UAS), unmanned combat aerial vehicle (UCAV) and the more pejorative 'drone'. Again, we use the term UAV to include this ENTIRE group of vehicles.

with commercial organizations. As of January 2016 US Federal Aviation Authority (FAA) had registered more than 300,000 UAV owners in the United States (FAA, 2016). Companies, like Amazon, are looking at adopting UAV technology for package delivery (Woolf and; Gibson, 2016), to provide Wi-Fi services (Harris, 2016), etc. UAVs are employed by civilian engineers for seismic risk assessments, transportation planning, disaster response and construction management (Liu, et al, 2014). Even in the nuclear industry, new uses for UAVs to fulfil operational, safety and environmental monitoring tasks are continually being explored, including taking physical, chemical and radiochemical measurements (Hofstetter, July 15-19, 1996); extending human safety capabilities by monitoring in environments where humans cannot go (e.g., use in characterizing damage at Fukushima) (Lochbaum, 2015); and, expanding the deployment of traditional security detection (e.g., sensors and cameras) and perimeter monitoring systems (Baylon, 2015). While advances in UAV technology found numerous applications and brought multiple benefits to society in general, the potential threat of the misuse of this technology should not be discounted.

Recently, the world witnessed a number of security incidents involving UAVs, some of them related to nuclear facilities. These incidents, rapid development and uncontrolled spread of technology motivated this research and the need for a closer look at the threats and means of protecting nuclear facilities. Several examples of these incidents include:

- **Fall 2014:** In France, several unidentified UAVs made flights in the restricted airspace over 13 out 19 nuclear power plants in apparently coordinated and organized manner, sometimes simultaneously over plants that are hundreds of miles apart. Currently, there is still no explanation of the flights intent and no one has been held accountable. These incidents had put the French government on high alert and some had suggested that nuclear power plants should be shut down over this threat as they are 'virtually unprotected' (Gaffey and Philips, 2015);
- **January 2015:** In Washington, D.C., a civilian UAV flew over the White House fence and crash-landed on the lawn (an incident that did not cause any injuries or property damage). The operator of the UAV was "an inebriated off-duty employee for a government intelligence agency" and the UAV was a popular commercially available 'quadcopter' (Schmidt and Shear, 2015);
- **January 2015:** In the UAE, all air traffic at the Dubai International Airport was brought to a stop for 55 minutes by a recreational UAV. There was no damage to aircrafts or passengers, but it was a significant disruption resulting in economic consequences (The National, 2015); and,
- **July 2016:** UAVs were spotted over Savannah River Site (SRS) in the USA. In late June and early July 2016, eight UAVs were spotted by the protective force and professional staff at the facility. The incident triggered an investigation by federal agencies (Gardiner, 2016). The reason for the UAV flights and who operated them is currently unknown at the time of this writing.

More ominously, former British Prime Minister David Cameron has stated that ISIL terrorists are planning to use UAVs as mobile, airborne dirty bombs (Riley-Smith, 2016). Based on the

examples above it is clear that UAV technology can pose new challenges for security systems at nuclear facilities. The purpose of this study is to identify the threats and dangers; evaluate potential measures for detecting and intercepting UAVs around nuclear facilities; and, propose future research in the areas of nuclear security and physical protection related to this potential threat.

II. UAV Applications

To help overcome the lack of literature on UAVs and nuclear security — and to better understand the threat that UAVs may pose to nuclear facilities—a detailed review of the technology, its history and classification is needed. Per these reported UAV-related security incidents, there is a need to expand the academic literature investigating the security implications to nuclear facilities resulting from UAV use.

Until the last decade, the development of UAV technology was mainly driven by government funding and military needs. Such military uses included: decoy/diversion, weapons delivery, communication relay, anti-submarine/air-borne early warning, mine detection/detonation and reconnaissance[2]. Having increased in prominence — and usage — in global military and strategic efforts since the end of the Cold War, UAVs have simultaneously increased in technical capability and decreased in the cost of production. Spurred by enhanced online communications forums and a proliferating 'do-it-yourself' paradigm, the civilian UAV community has exploded since the late 2000s—resulting not only in hobbyist UAV makers, but also in professional and commercial UAV manufacturers for the civilian community. This community uses UAVs for an ever-increasing—and creative—set of applications. Non-military governmental applications include firefighting (e.g., monitoring or locating trapped persons); surveillance and intelligence gathering; meteorology study efforts environmental and wildlife monitoring; search and rescue; disaster recovery; conservation; natural resources management; surveying (e.g., land and people); and, traffic monitoring. Commercial uses include supporting agricultural efforts (e.g., seeding, watering and crop monitoring) and transportation (e.g., Amazon's exploration of a UAV-based delivery service). Lastly, there is the widespread personal use of UAVs for photography, videography or simple recreation (Burns, I., 2014) (Gettinger, et al, 2014).

A. Challenges and Responses to Regulating UAV Use

Increasing civilian popularity, combined with an expanding technological capabilities, have resulted in significant challenges to regulating the use of UAVs. These challenges can be placed into three broad categories. First is the challenge of *where* UAVs should be allowed—and not allowed—to fly. This includes the difficulty in identifying the appropriate airspace for the different uses (and sizes) of UAVs. The second challenge relates to *who* should be allowed to use UAVs—and more specifically, who is responsible for damages to people, property or civil rights. As UAVs increase in physical size and technical capability, the level of skill required to safely operate them has dramatically decreased—presenting a broad challenge as unskilled and unsophisticated operators could still inadvertently create a dangerous scenario from losing control of a large and complex UAV. Lastly, and perhaps most difficult, is the challenge of *how*

[2] NOTE: Extensive analysis of military uses of drones are outside the scope of this paper.

UAVs should be used. As described in the introduction to this paper, commercial or personal uses are increasingly causing problems to public services, hampering transportation networks and threatening personal and social privacy (Maddox and; Stuckenberg, 2015) (Elias, 2016).

Whether concerned about the economic or transportation disruptions experienced, potential human injury to members of the public or the threats to personal privacy, the regulatory environment for UAVs has a key role to play in shaping the development, use and proliferation of UAVs. This is the broader context in which to understand the complexity of evaluating UAV-related threats to the security of nuclear facilities.

B. Gaps to be Addressed

Regulatory difficulties also challenge traditional approaches to the security of nuclear facilities. Understanding what types of UAVs are legally allowed to be in what airspace directly influences the security design and operations decisions for nuclear facilities. Similarly, these federal regulatory challenges will influence the cooperation with the host country's competent security authority for securing nuclear facilities. For example, the growing (potential) set of adversary characteristics and associated security vulnerabilities posed by the malicious (or inadvertent) use of UAVs in the airspace surrounding a nuclear facility might necessitate the host country's competent security authority to revise their national design basis threat (DBT),

> which provides a general description of the attributes of potential adversaries who might attempt to commit radiological sabotage or theft or diversion against which [the power plant] licensee's physical protection systems must defend with high assurance (Lochbaum, 2015).

Rather than evaluating across the wide disparity in UAV size and capability (e.g., weight, payload, range, flight duration, or maximum altitude), their influence on nuclear security needs to be described in terms of new, non-traditional threats that UAV pose. One method includes comparing general categories of UAV capabilities to potential threats to—or leverage points for—nuclear facility security systems. Here, potential threats refer to how either current realities or foreseeable advances in UAV capability would challenge the current emphasis in nuclear facility security on detection, delay and response. At the same time, UAV capabilities may also provide non-traditional mechanisms for stopping a potential security incident or identifying those persons responsible for instigating such incidents (e.g., potential leverage points). These capabilities are summarized in Table 1.

Table 1 goes here.

Considering these potential threats and leverage points, what follows is an overview of nuclear security concerns, approaches and proposed research framework for this area.

III. Security Concerns for Nuclear Facilities

Nuclear security experts have identified a range of security concerns for nuclear facilities—ranging from traditional to novel—stemming from the increased use of UAVs. Examples of such

potential security concerns include: adversary data collection, direct attacks, diversionary attacks, introduction/removal of contraband around access controls and 'wild-[UAV] chases' (Lochbaum, 2015) (Bunn, 2015). Even considering the resultant significant increase in security at nuclear facilities, per a top U.S. independent expert on nuclear power at the Union of Concerned Scientists

> The NRC's post-9/11 upgrades did not eliminate the suicide aircraft threat entirely, however, and multiple explosive-laden [UAVs] might be able to overwhelm the upgrades (Lochbaum, 2015).

These specific scenarios can be categorized as potential adversary goals for UAV use—or groupings of similar paths along which the security concerns from UAVs can be analyzed in traditional approaches to nuclear security. There are several envisioned potential adversary goals, including (but not limited to): reconnaissance (Bacchi; Gittleson 2014; Tucker 2015), smuggling (Brandes, 2015); kinetic attack (Finn 2011; Gettinger, et al 2014), electronic attack and distraction. These security concerns could occur individually, in multiples, or in combination with non-UAV operations, such as a ground attack.

To put this in context, according to news reports, in October 2012 a Hezbollah UAV attempted to take picture of the Dimona nuclear research center in southern Israel and was shot down 10 miles from the facility (Times-Dispatch Staff, 2012). Traditional nuclear security approaches, and developing UAV protection technologies, to help counter these UAV-related challenges to nuclear facility security systems are described in the next section.

IV. Security Approaches

4.1 IAEA Guidelines

Given all potential threats posed by UAVs to nuclear facilities, physical protection systems and approaches should be adapted and upgraded to address those threats. Per the International Atomic Energy Agency (IAEA), physical protection of nuclear facilities is the responsibility of an individual facility operator and is regulated by national authorities (typically nuclear regulators). A state regulator establishes laws and standards for the level of protection of nuclear facilities on its territory. It is then the responsibility of an operator and a response force organization to decide on how to implement security and the physical protection system to meet the security objectives. Specific goals are based on the DBT developed for a State as a whole and for each specific facility. The DBT is a confidential document which includes detailed description of all potential threats that exist in a State in terms of their

> attributes and characteristics of potential insiders and/or external adversaries, who might attempt unauthorized removal of nuclear material or sabotage, against which a physical protection system is designed and evaluated (IAEA, 2011).

The DBT is a living document and must be continuously updated as existing threats change or new potential threats arise. The advancing and evolving threat capabilities of new technologies,

like UAVs, should initiate a more in-depth analysis of the threat potential and, potentially, a revision of the DBT.

According to the legal authority established by the IAEA's 'Nuclear Security Recommendations on Physical Protection of Nuclear Materials and Nuclear Facilities' (INFCIRC/225/Rev.5), the objectives of a State's physical protection regime are: to protect against unauthorized removal of nuclear materials and against sabotage. The State's physical protection regime should seek to achieve these objectives through "management of an attempted malicious acts or a malicious act by an integrated system of detection, delay and response" (IAEA, 2011).

Detection encompasses all technical and human means to detect adversaries as early as possible and effectively verify the alarm. Delay is meant to provide enough time for the effective response to an attack. Response is a set of measures for stopping and neutralizing attackers. Since UAVs can be a potential means of either attacking a nuclear facility or smuggling nuclear materials out of it, the same 'detect-delay-respond' approach should be developed to neutralize the threat posed by them. In this section, we look at the technical measures that can be used for each step of this approach.

The 'detect-delay-respond' paradigm is predicated on modeling attack paths and protective force actions as competing adversary and response force timelines. As such, a nuclear facility is considered secure when the security system is shown capable of detecting the adversary attack early enough and delaying adversary task time long enough to allow the protective force to interrupt and neutralize (Garcia, 2008). In other words, if the response force time is longer than the adversary task time, the nuclear facility experiences a loss (either sabotage attack or theft of nuclear material). When incorporating the UAV threat to nuclear security into system design, it is useful to recognize three types of intrusions: a) accidental intrusion, b) intentional intrusion by unsophisticated operators, c) intentional intrusion by sophisticated operators (capable of assembling or modifying hardware and software) (Humphreys, 2015).

Regardless of capability or specific attack path, the logic of these traditional approaches to nuclear security suggest appropriate security mitigations to account for UAVs should include efforts to increase the ability of the nuclear facility to detect UAVs (both farther out and smaller cross-sectional objects), increase the delay time for UAVs in the airspace above nuclear facilities, or reducing response time by moving UAV-specific response capabilities closer to targets. In considering the potential UAV threat, we evaluate how these three approaches to improving security at nuclear facilities might be accomplished.

4.2 Detection and identification

Early detection and identification is the key to effective neutralization of the UAV threat. It would provide sufficient time to make a decision on the nature of the threat and deploy the means necessary to destroy or capture a rogue UAV. Although there is a number of physical phenomena associated with UAVs on which various detection technologies can be based, according to a North Atlantic Treaty Organization Industrial Advisory Group Study (NATO, 2013): "[n]o sensor type alone is able to provide sufficient tracking and identification capability to offer a reliable and effective defense against the [UAV] threat."

The expanding technological capabilities of UAVs necessitate the use of several types of detection capabilities, including: the reflectance of ultraviolet, visible and infrared photons; radar reflectance; acoustic emissions; electromagnetic emissions; and induced magnetic fields (Birch, et al, 2015).

Radar. Traditionally, radar technologies are used to detect flying objects in the sky, but classic radar technologies may not be suitable in this case since, for many years, radar technology and software was specifically tuned to avoid small objects, such as birds, and dismiss them as noise (Wall, 2015). However, some of the radar technologies can be adapted for UAV detection. One specific example is the electronic scanning radar, also known as AESA (Active Electronically Scanned Array), which is currently used in fighter jets. It is a type of phased array radar in which transmitter and receiver are made of a number of small solid-state modules. The beams are emitted by each element and reflections received by the antenna are reconstructed. Essentially AESA can scan large areas simultaneously without any moving parts (or minimum movement) (Cohen, 1994) (Pike, 2011). AESA—and similar advances in radar detection of small cross-sectional items—has the advantage of being extremely versatile, both in terms of host platforms and detection capabilities. Yet, with the variation in UAV radar cross section, even the recent advances in AESA-type detection capabilities will be challenged to regularly and accurately identify hostile UAVs.

Electro-optical. Systems based on electro-optical technology can also be used for UAV detection. They operate through visual contact with a UAV and are usually capable of detecting, tracking and also identifying. Some of the systems use infrared sensor pattern recognition to distinguish between UAVs warm batteries and motors from birds' bodies (Humphreys, 2015). Some sub-categories of electro-optical systems include: passive visible imaging (e.g., UV, visible and near-infrared) and passive thermal imaging (short-wave, medium wavelength and long wavelength infrared). The advantages of the former include the possibility to distinguish between a UAV, birds, or any other object in the sky fairly inexpensively due to commercial availability. The advantages of the latter are the reduction of background signal noise, enhanced night time detection and less susceptibility to weather degradations. Conversely, disadvantages include the need for a clear unobstructed view of the object and high susceptibility to background signal noise of the former and the need to overcome fact that most UAVs have low thermal signatures of the latter (NATO, 2013).

Radioemission. Certain types of UAVs and sensors use a radio connection to receive commands from a UAV operator through a remote or transmit data (video feed for example) back to the operator or base station. These emissions can be detected and tracked. The primary advantage of this technology is its independence from light and weather conditions, meaning that detection can be done even in dark conditions or in foggy (rainy) weather. In contrast, its disadvantages include the fact that not all UAVs will be emitting radio signal and that some can be set on an autonomous, powerless glide path.

Acoustic. These set of sensors detect specific noise signatures created by UAV motors and propellers. Despite the advantages of being a passive sensor that is relatively inexpensive, acoustic sensors would make ineffective standalone detection systems (Busset, et al, 2015). For

example, these sensors have limited range, rely on matching registered acoustic sensors to a database of known UAV signatures, suffer from high nuisance alarm rates (especially in urban environments) and are not capable of detecting gliding UAVs as those do not produce any significant noise (Peacock and Johnstone, 2013) (Vasquez and al., 2008).

Magnetic detection systems. Systems based on detection of large metal objects by their influence on electromagnetic fields. These systems are potential useful only against large UAVs, as they are only capable of detecting substantially large metal parts. Therefore, their biggest disadvantage is that most of the commercially available UAVs use minimum metal parts.

Visual. This approach includes human visual detection and computer based image analysis. To date, security personnel have been responsible for discovering rogue UAVs over nuclear facilities. Though the use of human visual detection provides "unparalleled classification performance" (Birch, et al, 2015) and almost immediate response initiation, it also requires significant man-power (and cost) and suffers from vigilance degradation resulting from persistent and monotonous tasks. This is exacerbated by the low (though increasing) probability of seeing an unanticipated UAV.

However, increased sensitivity of various detection technologies does not always guarantee timely and positive detection of a rogue UAV. As shown above the system of various sensors capable of detecting very small cross-sectional UAVs can be established, various technologies are capable of doing that, the difficulty is in data stream analysis and in the task of separating signatures of UAVs from other small objects such as birds, flying debris, vegetation, etc. Abundance of such small objects will lead to multiple false alarms. Reducing systems sensitivity to reduce alarms from non-UAV objects will lead to missed detection of smaller UAVs. This is a similar to classic PPS sensor sensitivity problem−false positives vs. false negatives (Garcia, 2008).

In support of the guidance provided by the IAEA, short term solutions for detecting UAVs would incorporate the use of multiple sensors—mixing and matching from the above to align the advantages of one with the disadvantages of another. The use of sensors in this complementary manner can improve the UAV detection and identification ability for nuclear facilities, but does not negate the need for research and development into new, novel detection mechanisms.

4.3 Delay

Delay is achieved by implementing technical or procedural barriers that extend the time an adversary would need to complete their theft or sabotage mission. The longer the delay time, the more time there is for a response force to reach the location, analyze the threat and execute an effective response (e.g., neutralization). The greatest fundamental challenge which UAVs pose to nuclear facility security is the inability to delay them. Traditional barriers to delay adversary access to nuclear facilities (e.g., fences or building surfaces) are ineffective against UAVs. Current efforts are focusing on providing delay by means of longer-distance detection. The earlier a rogue UAV is detected with long-range sensors, the more time there is available for a nuclear facility's response capabilities to mobilize against the threat.

In addition, some new approaches to UAV delay are being developed. Currently used features to delay low-flying aircraft include closely spaced telephone poles (to prevent an adversary helicopter from landing inside a facility) or mesh netting covering vital structures. These approaches could be adapted for the smaller profile and expanded (potential) adversary use of UAVs. Other approaches include, the increasing popularity of 'geofencing' (or, the use of GPS data to mark geographic locations as no-fly zones) which is being explored as a novel delay mechanism (Pratyusha and Naidu, 2015). For example, efforts to improve the use of collision avoidance for both autonomous-path and manually piloted UAVs (Gurriet and Ciarletta, 2016) could be implemented with the nuclear facility (or at least vital areas within a facility) geofence as the object with which to avoid collision. An advanced geofence algorithm might even be able to 're-route' a UAV to a predetermined landing area for response capture and evaluation. At the same time it should be noted that geofencing technologies will more than likely only deter accidental intrusions and potential attacks by unsophisticated operators. Sophisticated operators capable of hardware assembly and firmware modifications will, more than likely, be able to overcome geofencing limitations.

4.4 Response and neutralization

Lastly, response (and if necessary neutralization) is initiated after a UAV is detected and positively identified. The broad definition for response and neutralization is denial of mission, including destruction of the UAV target (Birch, et al, 2015). The options for response range from diverting the UAV in a different direction, capturing it, or to destroying it. The choice would vary based on the potential threat that is posed by the UAV and the technical means at the disposal of the response force of the facility. Several considerations should be taken into account for the response means: (1) the interception range should be greater than the stand-off range of potential UAV adversary missions (e.g., meaning that if a UAV is carrying an explosive payload it should be neutralized before the payload can damage the facility) and (2) response and detection methods must complement each other. Toward this second point, some response capabilities would dictate the requirements for detection sensors. For example, automated response technologies would require reliable sample tracking capabilities with high sampling rates. In this paper we will broadly categorize response methods into two main groups of "nondestructive" and "destructive".

Nondestructive. One of the options of responding to a UAV is capturing it without destroying the device. This would serve the purpose of neutralizing the threat, but would also aid in the investigation of the source of this threat and conducting forensics analysis. In general, nondestructive response options are relatively slow and require a longer response time, which could be problematic in a case of a fast attack. Specific options for this type of response include (but are not limited to):

- **Cyber Exploitations.** UAVs use radiowave and navigation systems (like the Global Positioning System (GPS) or other global navigation satellite system (GNSS)) for operating and communication with a remote controller. The intentional emission of extraneousradiowaves (noise) can prevent a UAV from maintaining its connectivity and potentially force a UAV to fly without operator intervention. Flying UAVs in

autonomous mode, however, can prevent use of certain types of signal interference (Gettinger, 2015). Efforts to intentionally emit extraneous signals are indiscriminate and would affect all electronic devices and communications in their range. This could pose a challenge from both a technical and legal standpoint. From a technical standpoint, a these extra signals can influence the facility's physical protections system (sensors and communication equipment), which could have even worse consequences than the attack itself. Technologies that generate such signals can also be banned in certain countries and regions. For example, their use is prohibited by the US Federal Communications Commission (Hornyak, 2015) (FCC, 2016), only special Federal agencies are allowed to operate them and only in certain conditions. In addition, these systems are vulnerable not only to the desired signals being overwhelmed by noise, but also to "counterfeit GNSS signals…generated for the purpose of manipulating a target receiver's reported position, velocity and time" (Kerns, et al, 2014). Civil GPS waveforms are unencrypted, unauthenticated, and are specified in public documentation (Global Positioning System Directorate, 2012) (European GNSS(Galileo), 2015). Therefore, it is possible to use a transmission device which would simulate those waveforms and deceive a recipient. This was shown experimentally by researchers at University of Texas and is described in (Kerns, et al, 2014). The main disadvantage of this approach is that it is indiscriminate and can affect all devices that rely on GPS in its field of influence, including aircraft, cellphones, etc;

- **UAV-on-UAV.** Another option that is being actively developed by several vendors, including French Malou (M.A.L.O.U, 2016) is using a protective UAV with a net to capture a rogue UAV. As a result, the rogue UAV is denied completion of its mission and is also captured for further investigation (Gayle, 2015). The disadvantage of this method would be in the timing of the response. The protective UAV would have to be stored in the vicinity of the attack location, or multiple UAVs should be deployed along the facility perimeter. Also, the protective force will need to be adequately trained to operate protective UAVs; and,
- **Bird-on-UAV.** An exotic measure against rogue UAVs is to use trained birds to catch them (Atherton, 2016) (Castle, 2016). Although this could be a viable defense option in certain cases, the likelihood of it being used at nuclear facilities is quite small, due to the high cost of maintaining rapidly deployable birds.

Other proposed approaches by (Birch, et al, 2015) include net-firing technologies, water-cannons and sticky foam. The range of these approaches are quite limited and the response time can be long, therefore they cannot be considered as primary response mean and can only be used in conjunction with other means.

Destructive. These options are different from the previous category as an attacking UAV would be destroyed during the neutralization process. This would still achieve the objective of stopping an attack or reconnaissance mission, but would make it more difficult to find the attacker and UAV operator. 'Destructive' techniques include: electromagnetic pulse, lasers, firearms, surface-to-air missiles.

- **Electro-magnetic pulse.** A powerful electro-magnetic pulse is sent in the direction of the UAV. This can disable some of the electronic components, causing the UAV to land. The main disadvantage of this technique is that this pulse could damage some of the surrounding electronic infrastructure. Similar to 'nondestructive' jamming technique, this approach would be dangerous for security sensors and equipment;
- **Lasers.** This technique focuses a high-power beam of photons at a UAV. Several countries have developed anti-UAV laser systems including the US (Boeing), China and the UK (Atherton, 2015) (France-Presse, 2014) (Golson, 2015) (Gettinger, 2014). These laser systems are expensive to develop, but are cheap to operate, costing around $1 per shot (Gettinger, 2014). This destructive technique could be especially useful in dealing with a swarm of UAVs coming from multiple directions. Disadvantages of this technique are that lasers are affected by adverse weather conditions, such as clouds, rain, fog; lasers can pose a hazard to humans and the surrounding infrastructure; and difficulty of keeping the laser focused on a fixed location on the UAV;
- **Firearms.** One of the classic approaches for the defense of a facility is to use conventional firearms against intruders, in this case UAVs. Some munition companies are even developing special types of munition designed to be effective against UAVs (Matyszczyk, 2015). The advantage of this technique is that security forces are already trained and equipped with conventional firearms. The main disadvantage is that this technique poses a danger to the surrounding population and staff; and,
- **Surface-to-Air Missiles.** This method had been tested and used before in a war-time conditions by several countries. Due to destructive power and costs, it is not likely to be used in domestic situation outside of a warzone.

4.5 Examples of technological needs to improve nuclear facility security

As described, there is a timely need for improving the ability of nuclear facilities to detect, delay and respond to (potential) UAV threats. Advances in detection and defense technologies to protect nuclear facilities (not to mention high-level government officials, public events, and critical infrastructure) present a strong start for identifying existing capabilities to include (and necessary capabilities to develop) toward improving nuclear facility security—with (Birch, et al, 2015) providing a good overview and summation of current counter-UAV systems.

Further, the previous subsections help identify technological advancements necessary to improve nuclear facility security against the novel (and in many ways non-traditional) threats posed by UAVs. These are summarized in Table 2, below.

Table 2 goes here.

The choice of which specific technologies or capabilities to use depends on the specific facility, operational constraints, national regulations and (at least in part) the existing DBT. For example, since many nuclear facilities are located away from densely populated areas, a wider range of response and detection technologies are available versus nuclear facilities closer to population centers or critical pieces of national infrastructure. Despite continuing advances in anti-UAV technologies, these developers might be outpaced by the evolution (and availability) of UAV

capabilities. For example, advances in acoustic or radioemission sensing capabilities may be negated by the infusion of 'micro-UAVs' whose acoustic signature falls below current detectable limits or use of cloud-computing for data transmission into the adversary toolkit. Similarly, advances in response capabilities such as lasers or geofencing can be defeated with UAV swarm attacks and cyber exploitation, respectively.

Taken together, the potential use of UAVs by adversaries significantly challenges the traditional detect, delay and response comparative timeline perspective for nuclear facility security espoused by the IAEA—suggesting a need for broader and deeper research into technologies, capabilities and frameworks to improve nuclear facility security.

V. Recommendations and Future Research

Based on the analysis of the threats posed by UAVs and existing technologies for detection, identification, delay and response to those threats, we have developed a set of recommendations that, in the view of the authors, are the priority areas for research in both technical and policy areas. The two major challenges posed by UAVs to a nuclear facility physical protection system are:

1. UAVs' ability to travel through the air, which allows to overcome most of the 'traditional' physical protection approaches
2. a very wide range of threats posed by UAVs, each one of which would require a unique mitigation approach

Table 2 in the previous section summarizes the primary technological needs to improve traditional metrics of security system performance at nuclear facilities—and serves as a list of potential research and development areas regarding technological components to better mitigate the threats posed by UAVs. These technical components do not operate in a vacuum, which suggests additional research needs to improve security against the UAV threat that include security analysis techniques that better capture 'non-traditional' threats like UAVs, facility-specific procedures, understanding factors that influence adherence to procedures, legal implications, international best practice documentation and understanding how the interdependence each of these influences overall nuclear facility security against UAVs. Table 3 summarizes some specific area research within these categories, as well as references we find useful as starting points for future work.

Table 3 goes here.

Combined with technical areas for research and development summarized in Table 2, considerations shown here provide a path for a multi-disciplinary full-scope development for improving technological, procedural and legal approaches for mitigating threats posed by UAVs. This would allow for improvement of UAV detection, identifying UAV operators and implementing appropriate punitive legal response. Also additional insights could be gained on

how to include UAV-related attack paths into traditional security analysis techniques. This is better done through international working groups, which can develop standards, recommendations and best practices for security of nuclear facilities from UAV threats.

VI. Conclusions

New technologies, as they appear and develop, bring certain advantages and benefits to the society, but they also are capable of creating new potential threats and tools for malicious attacks on critical infrastructure. One of the technologies that is becoming a 'game-changer' for security of nuclear facilities is UAV. Several recent incidents in different parts of the world have shown that the threat posed by UAVs cannot and must not be ignored. In this paper we have shown a number of ways UAV technology can be used against security of nuclear facilities: reconnaissance, smuggling, kinetic attack, electronic attack, and distraction. This wide range of threats creates unique challenges to protecting nuclear facilities from UAVs. At the same time, it should be pointed out that there is a number of potential benefits of the UAV technology for nuclear security and safety, such as, for example, low-cost monitoring/surveillance for remote facility areas of SNM in transit. In this work, a comprehensive list of technologies applicable for detection and neutralization of UAVs was compiled. A number of challenges were identified for every functional area of the defense systems, which means that current analytical approaches are limited in effectiveness. We offer this paper as a first step in coordinating a response to comprehensively and systematically identify research and development needs to improve nuclear facility security against UAVs. As UAVs advance in technological capability and spread to a wider range of usage domains, security responses must consider new, 'out-of-the-box' thinking because, as Albert Einstein put it, 'No problem can be solved from the same kind of thinking that created it.'

VII. References

Atherton, K., 2015. BOEING Unveils Iis Anti-Drone Laser Weapon. *Popular Science [Online], Available: http://www.popsci.com/boeing-unveils-compact-anti-drone-laser*, 28 August.

Atherton, K., 2016. Trained Police Eagles Attack Drones on Command. *Popular Science [Online], Available: http://www.popsci.com/eagles-attack-drones-at-police-command*, 1 February.

Bacchi, U., n.d. *Paris attacks: Jihadists secretly monitored Belgian nuclear scientist for potential Daesh dirty bomb.* [Online]
Available at: http://www.ibtimes.co.uk/paris-attacks-jihadists-secretly-monitored-belgian-nuclear-scientist-potential-daesh-dirty-bomb-1544719
[Accessed 18 Febuary 2016].

Baylon, C., 2015. *How to use drones to improve nuclear security.* [Online]
Available at: https://www.weforum.org/agenda/2015/01/how-to-use-drones-to-improve-nuclear-security
[Accessed 12 September 2016].

Birch, G., Griffin, J. & Erdman, M., 2015. *"UAS Detection, Classification, and Neutralization: Market Survey 2015,",* s.l.: Sandia National Laboratory, SAND2015-6366.

Boeke, S., Veenendaal, M. A. & Heinl, C. H., 2015. *Civil-Military Relations and International Military Cooperation in Cyber Security: Common Challenges & State Practices Across Asia and Europe.* s.l., s.n.

Brandes, H., 2015. *Drone carrying drugs, hacksaw blades crashes at Oklahoma prison.* [Online]
Available at: http://www.reuters.com/article/us-oklahoma-prison-idUSKCN0SL22220151027
[Accessed 12 September 2016].

Bunn, M., 2015. *Drones: Good News and Bad News for Nuclear Security.* [Online]
Available at: http://nuclearsecuritymatters.belfercenter.org/blog/drones-good-news-and-bad-news-nuclear-security
[Accessed 18 February 2016].

Burns, I., 2014. *Drone Technology: Exciting New Technologies are being developed for the Burgeoning Drone Industry.* [Online]
Available at: http://www.atintellectualproperty.com/drone-technology/
[Accessed 18 February 2016].

Busset, J. et al., 2015. *Detection and tracking of drones using advanced acoustic cameras.* s.l., s.n.

Castle, S., 2016. Dutch Firm Trains Eagles to Take Down High-Tech Prey: Drones. *The New York Times*, 28 May.

Charlton, J. & Hertz, R., 1989. GUARDING AGAINST BOREDOM: Security Specialists in the U.S. Air Force. *Journal of Contemporary Ethnography,* Volume 18, pp. 299-326.

Clarke, R., 2014. Understanding the drone epidemic. *Computer Law & Security Review,* 30(3), pp. 230-246.

Cohen, E. D., 1994. *Active electronically scanned arrays.* San Diego, CA, s.n.

Dove, R., Popick, P. & Wilson, B., 2013. The Buck Stops Here: Systems Engineering is Responsible for System Security. *INSIGHT,* 16(2), pp. 6-9.

Elias, B., 2016. *Unmanned Aircraft Operations in Domestic Airspace: U.S. Policy Perspectives and the Regulatory Landscape,* s.l.: Congressional Research Service. R44352.

European GNSS(Galileo), 2015. *Open Service Signal in Space Interface Control Document.* [Online]
Available at: https://www.gsc-europa.eu/system/files/galileo_documents/Galileo_OS_SIS_ICD.pdf
[Accessed 12 September 2016].

FAA, 2016. Press Release – FAA Registered Nearly 300,000 Unmanned Aircraft Owners. *Federal Aviation Administration [Online], Avaliable: https://www.faa.gov/news/press_releases/news_story.cfm?newsId=19914*, 22 January.

FAA, 2016. *Summary of Small Unmanned Aircraft Rule (PART 107),* Washington DC: s.n.

Faughnan, M. S. & et. al., 2013. *Risk analysis of Unmanned Aerial Vehicle hijacking and methods of its detection.* Charlottesville, VA, s.n.

FCC, 2016. *Jammer Enforcement.* [Online]
Available at: https://www.fcc.gov/general/jammer-enforcement
[Accessed 12 September 2016].

Finn, P., 2011. *"Mass. man accused of plotting to hit Pentagon and Capitol with drone aircraft," The Washington Post.* [Online]
Available at: https://www.washingtonpost.com/national/national-security/mass-man-accused-of-plotting-to-hit-pentagon-and-capitol-with-drone-aircraft/2011/09/28/gIQAWdpk5K_story.html

France-Presse, 2014. China unveils laser drone defence system. *The Guardian [Online], Available: https://www.theguardian.com/world/2014/nov/03/china-unveils-laser-drone-defence-system*, 3 November.

Gaffey, C. & Philips, C., 2015. Most French Nuclear Plants 'Should Be Shut Down' Over Drone Threat. *Newsweek [Online]. Available: http://europe.newsweek.com/most-french-nuclear-plants-should-be-shut-down-over-drone-threat-309019*, 24 February.

Garcia, M. L., 2008. *The Design and Evaluation of Physical Protection Systems, Second Edition.* s.l.:Butterworth-Heinemann.

Gardiner, T., 2016. Eighth drone spotted in SRS skies. *Aiken Standard [Online], Available: http://www.aikenstandard.com/article/20160706/AIK0101/160709671*, 5 July.

Gayle, D., 2015. The drone catcher: Flying net is designed to stop terrorists from flying bomb-laden gadgets into nuclear power stations. *DailyMail [Online], Available: http://www.dailymail.co.uk/news/article-2948062/The-drone-catcher-France-reveals-flying-net-stop-terrorists-flying-bomb-laden-gadgets-nuclear-power-stations-following-spate-sightings.html*, 10 February.

Gettinger, D., 2014. *What You Need to Know About Lasers.* [Online]
Available at: http://dronecenter.bard.edu/what-you-need-to-know-about-lasers/
[Accessed 12 September 2016].

Gettinger, D., 2015. *"Domestic Drone Threats," Center for the Study of the Drone, Bard College.* [Online]
Available at: http://dronecenter.bard.edu/what-you-need-to-know-about-domestic-drone-threats/
[Accessed 12 September 2016].

Gettinger, D. et al., 2014. *"The Drone Primer," Center for study of the drone,.* [Online]
Available at: http://dronecenter.bard.edu/the-drone-primer-announcement/
[Accessed 12 September 2016].

Gittleson, K., 2014. *"Data-stealing Snoopy drone unveiled at Black Hat," BBC News.* [Online]
Available at: http://www.bbc.com/news/technology-26762198
[Accessed 12 September 2016].

Global Positioning System Directorate, 2012. *Systems engineering and integration Interface Specification IS-GPS-200G,* s.l.: http://www.gps.gov/technical/icwg/.

Golson, J., 2015. Welcome to the World, Drone-Killing Laser Cannon. *Wired [Online], Available: https://www.wired.com/2015/08/welcome-world-drone-killing-laser-cannon/*, 8 August.

Gurriet, T. & Ciarletta, L., 2016. *Towards a generic and modular geofencing strategy for civilian UAVs.* Arlington, VA, s.n.

Harris, M., 2016. *Project Skybender: Google's secretive 5G internet drone tests revealed.* [Online]
Available at: https://www.theguardian.com/technology/2016/jan/29/project-skybender-google-drone-tests-internet-spaceport-virgin-galactic
[Accessed 26 September 2016].

Hartmann, K. & Steup, C., 2013. *The Vulnerability of UAVs to Cyber.* s.l., s.n.

Hofstetter, J. K., July 15-19, 1996. *Application of UAVs at the Savannah River Site (WSRC-MS-96-0319).* Orlando, FL, s.n.

Hornyak, T., 2015. California turns to jamming tech to disable pesky drones. *PCWorld [Online], Available: http://www.pcworld.com/article/2951272/robotics/california-turns-to-jamming-tech-to-disable-pesky-drones.html*, 22 July.

Humphreys, T., 2015. *Statement on the security threat posed by unmanned aerial systems and possible countermeasures.* [Online]
Available at: http://docs.house.gov/meetings/HM/HM09/20150318/103136/HHRG-114-HM09-Wstate-HumphreysT-20150318.pdf

IAEA, 2007. *Nuclear Security Series No. 4 'ngineering Safety Aspects of the Protection of Nuclear Power Plants against Sabotage',* Vienna: International Atomic Energy Agency.

IAEA, 2011. *INFCIRC/225 Rev. 5, Nuclear Security Recommendations on Physical Protection of Nuclear Materials and Nuclear Facilities,* Vienna, Austria: s.n.

IAEA, 2016. *INFCIRC/274/Rev.1/Mod.1 Amendment to the Convention on the Physical Protection of Nuclear Materials,* Vienna, Austria: s.n.

Kaufmann, S., 2016. Security Through Technology? Logic, Ambivalence. *European Journal for Security Research,* Volume 1, pp. 77-95.

Kerns, A. J., Shepard, D. P., Bhatti, J. A. & Humphreys, T. E., 2014. Unmanned aircraft capture and control via GPS spoofing. *Journal of Field Robotics,* 31(4), p. 617–636.

Kharchenko, V., Sachenko, A., Kochan, V. & Fesenko, H., 2016. *Reliability and survivability models of integrated drone-based systems for post emergency monitoring of NPPs.* Rzeszow, s.n.

Liu, P. et al., 2014. A review of rotorcraft Unmanned Aerial Vehicle (UAV) developments and applications in civil engineering. *Smart Structures and Systems,* 13(6), pp. 1065-1094.

Lochbaum, D., 2015. *Drones at nuclear power plants: enemies or helpers?.* [Online]
Available at: http://thebulletin.org/drones-nuclear-power-plants-enemies-or-helpers8132
[Accessed 18 February 2016].

M.A.L.O.U, 2016. *Malou-Tech - Groupe Assmann.* [Online]
Available at: http://www.psa-entreprise.fr/malou-tech/indexUS.php
[Accessed 12 September 2016].

Maddox, S. & Stuckenberg, D., 2015. *Drones in the U.S. National Airspace System: A Safety and Security.* [Online]
Available at: http://harvardnsj.org/2015/02/drones-in-the-u-s-national-airspace-system-a-safety-and-security-assessment/
[Accessed 26 September 2016].

Matyszczyk, C., 2015. Need to take down a drone? A munitions company offers firepower. *CNET [Online], Available: https://www.cnet.com/news/company-markets-anti-drone-munitions/*, 23 August.

Mouloua, M., Gilson, R., Kring, J. & Hancock, P., 2001. *Workload, Situation Awareness, and Teaming Issues.* s.l., s.n.

NATO, 2013. *Industrial Advisory Group Study SG-170 'The Engagement of Low, Slow and Small Aerial targets by GBAD (ground based aerial defense)',* s.l.: NATO.

Nehme, C. E., Crandall, J. W. & Cummings, M. L., n.d. *An Operator Function Taxonomy for Unmanned Aerial Vehicle.* s.l., s.n.

Oppenheimer, D., Morf, M. & Schleicher, S., 2005. *Applications of advanced sensors on unmanned aerial vehicles (UAV's) for the protection of high value targets and support of response forces.*. Salzburg, Austria, s.n.

Peacock, M. & Johnstone, M. N., 2013. *Towards detection and control of civilian.* Perth, Australia, s.n.

Pike, J., 2011. *AN/APG Active Electronically Scanned Array AESA.* [Online]
Available at: http://www.globalsecurity.org/military/systems/aircraft/systems/an-apg-aesa.htm
[Accessed 5 December 2016].

Pratyusha, P. L. & Naidu, V. P., 2015. *Geo-Fencing for Unmanned Aerial Vehicle.* s.l., s.n.

Riley-Smith, B., 2016. Isil plotting to use drones for nuclear attack on West. *The Telegraph [Online], Avaliable: http://www.telegraph.co.uk/news/2016/04/01/isil-plotting-to-use-drones-for-nuclear-attack-on-west/*, 1 April.

Ross, R., McEvilley, M. & Oren, J. C., 2016. *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, NIST Special Publication 800-160: Second Public Draft,* Gaithersburg, MD: National Institute of Standards and Technology.

Saleem, S., 2015. *Is it a bird? is it a plane? Drones in the UAE.* [Online]
Available at: http://www.tamimi.com/en/magazine/law-update/section-11/junejuly/is-it-a-bird-is-it-a-plane-drones-in-the-uae.html
[Accessed 26 September 2016].

Schmidt, M. & Shear, M., 2015. White House Drone Crash Described as a U.S. Worker's Drunken Lark. *NY Times [Online]. Available: http://www.nytimes.com/2015/01/28/us/white-house-drone.html?_r=0*, 27 January.

The National, 2015. Recreational drones bring Dubai airport traffic to a halt. *The National [Online]. Available: http://www.thenational.ae/uae/transport/recreational-drones-bring-dubai-airport-traffic-to-a-halt*, 23 January.

Times-Dispatch Staff, 2012. "Hezbollah Drone Sent to Scout Nuclear Facility, Israel says," Richmond Times-Dispatch. *Richmond Times-Dispatch [Online], Available: http://www.richmond.com/news/hezbollah-drone-sent-to-scout-nuclear-facility-israel-says/article_3490daec-c584-53a7-b1af-24e7e3a397d0.html*, 13 October.

Touaux, C., 2015. *Unidentified drones reappear over Paris at night.* [Online]
Available at: https://www.yahoo.com/news/unidentified-drones-reappear-over-paris-during-night-

080038522.html
[Accessed 26 September 2016].

Tucker, P., 2015. *In Ukraine, Tomorrow's Drone War Is Alive Today.* [Online]
Available at: http://www.defenseone.com/technology/2015/03/ukraine-tomorrows-drone-war-alive-today/107085/
[Accessed 12 September 2016].

Vasquez, J. & al., e., 2008. *Multisensor 3D tracking for counter small unmanned air vehicles (CSUAV).* s.l., s.n.

Wall, R., 2015. Next Step for Drones: Defending Against Them; Antidrone defense systems are a rising new business as military, aviation concerns mount. *The Wall Street Journal*, 23 July.

Williams, A. D., 2015. Beyond a Series of Security Nets: Applying STAMP & STPA to Port Security. *Journal of Transportation Security,* 8(3-4), pp. 139-157.

Woolf, N. & Gibson, S., 2016. *Amazon to test drone delivery in partnership with UK government.* [Online]
Available at: https://www.theguardian.com/technology/2016/jul/25/amazon-to-test-drone-delivery-uk-government
[Accessed 26 September 2016].

Young, W., 2015. *A System-Theoretic Security Analysis Methodology for Assuring Complex Operations Against Cyber Disruptions.* Cambridge, MA: Massachussets Institute of Technology, Dissertation.

Table 1. Categorical descriptions of how UAV technological capabilities serve as potential challenges and/or potential leverage points for nuclear facility security systems.

UAV Capability Category	Capability Description	Challenge(s) to Security Systems	Potential Leverage Point(s)
Launch and recovery	Specific infrastructure, terrain and skill to insert a UAV into the airspace ('launch') and (possible) infrastructure, terrain and skill for an operator to retrieve a UAV ('recovery') can vary	• Cannot assume malicious use of UAVs includes recovery • Launch point/platform might be out of nuclear facility line of site • Launch point/platform may be different from recovery point/platform •	• Detection from a launch platform would provide for early detection and easier identification
Navigation	UAVs must receive course information in real-time from either an operator or onboard navigation (which likely include a GPS device and possibly a magnetometer-disciplined internal navigation system)	• UAVs with GPS can be autonomously navigated to the nuclear facility • GPS of facility-owned UAVs hacked and turned into adversary weapon/detection tool	• Non-autonomous UAVs must have a pilot, in relative close proximity • UAVs likely have GPS device, possibility to triangulate position (and position of operator)
Sensors	UAVs often have technologies that detect and measures various physical properties	• Data recording sensors can collect sensitive or protected information • UAVs can have sophisticated sensors that collect non-traditional data (e.g., thermal imaging or heat signatures)	• Sensing phenomenology may be exploitable to detect or assess the presence of a UAV • Some sensors use active signal transmission, which would allow for early detection and successful identification
Data			

	Information — images, sounds, physical property measurements, etc. — collected by a UAV must either be stored locally or transmitted to another location	• Local storage of data increases difficulty of separating malicious intent from inadvertent activity	• Transmission/communication of data can help identify, locate or track the operator
Stealth	UAVs have varying small sizes and aerial presence, influenced by size, shape, material composition, propulsion type, and operational altitude	• Small cross-section and size make it difficult to locate UAVs until they are in relatively close proximity • UAVs are designed to challenge both radar and visual detection	• To an extent, electromagnetic, thermal and sound emissions decrease the 'stealth' ability of UAVs

Table 2. Summary of technological needs to improve the detection, delay and response functions of security systems at nuclear facilities against threats from UAVs.

Potential UAV Threat	Detection	Delay	Response
Reconnaissance	- Early detection and identification is needed - Detection capability for small UAVs is needed	- Effective Geofencing needed as the primary delay mode	- 'Nondestructive' response is preferred to further analysis of the UAV and identifying its operator
Smuggling	- Detection means for the presence of payload are needed	- Effective Geofencing needed as the primary delay mode	- 'Nondestructive' response is preferred for further analysis of the UAV, its payload and for identifying its operator
Kinetic Attack	- Detection of larger UAVs required - Detection of gliding (silent) UAVs required	- Physical means of delay are needed	- 'Destructive' response if preferable to disable the threat at the safe distance from facility
Electronic Attack	- Additional electronic attack detection means are needed	- Effective Geofencing needed as the primary delay mode	- Both 'destructive' and 'nondestructive' response options are needed, choice depends on the severity of attack
Distraction	- Early detection and identification is needed - Detection capability for small UAVs is needed	- Effective Geofencing needed as the primary delay mode	- 'Nondestructive' response is preferred to further analysis of the UAV and identifying its operator

Table 3. Additional areas proposed for research and development for improvement of security against UAV threat.

	Example Needs	Representative Points of Interest	Useful Starting References
Technological/ Analytical Considerations	Technological security-related component development	See Table 2	(Birch, *et al*, 2015)
	System design methodologies	Developing clusters of sensors or algorithms to help mitigate the 'sensitivity vs. specificity' tradeoff[3]	(Kharchenko, *et al*, 2016), (Oppenheimer, *et al*, 2005)
	Analysis methods	Expanding traditional path analysis techniques to include new attack paths posed by UAVs	(IAEA, 2007)
	Defeat Options	Demonstrating opportunities to render useless to an adversary a UAV in the nuclear facility's airspace	(Hartmann and Steup, 2013), (Faughnan, *et al*, 2013)
Organizational Considerations	Procedures	Identifying appropriate procedures for monitoring UAV detection systems or responding to UAV sightings (including generic templates to be applied at different nuclear facilities or in different countries)	(Mouloua, *et al*, 2001), (Nehme, *et al*, n.d.)
	'Anti-complacency'	Establishing lessons learned from 'false alarms' and late detections on nuclear facility security to improve vigilance against UAV threat(s)	(Kaufmann, 2016), (Charlton and Hertz, 1989)
	Legal Frameworks	Providing a framework for linking national legal responsibilities (and requirements) for responding to different categories of UAV threat (e.g., unintentional airspace violation vs. malicious act)	(Maddox and; Stuckenberg, 2015), (Elias, 2016), (Clarke, 2014)

[3] One security expert noted that the speeds at which UAVs travel when coupled with their small cross sections, makes their detection ranges a game of many seconds or few minutes—necessitating, despite its unpopularity, a focus on developing autonomous or mostly autonomous counter-UAV systems.

	International Documentation	Conducting cross-country comparison of UAV threat(s) and responses to support creation of international best practices	(Boeke, *et al*, 2015)
Interdependence	Better understanding of social & technical interactions	Invoking socio-technical system approaches to security for complex systems	(Williams, 2015), (Young, 2015), (Ross, *et al*, 2016), (Dove, *et al*, 2013)