SAND2018-8561C

CUAS Security Education

Jaclynn J. Stubbs*, Camron G. Kouhestani †, Bryana L. Woo‡, and Gabriel C. Birch§
Sandia National Laboratories
1515 Eubank SE, Albuquerque, NM, USA
*jstubbs@sandia.gov †cgkouhe@sandia.gov ‡blbaird@sandia.gov §gcbirch@sandia.gov

***Abstract*—Unmanned aircraft system (UAS) technologies have gained immense popularity in the commercial sector and have enabled capabilities that were not available just a short time ago. Once limited to the domain of highly skilled hobbyists or precision military instruments, consumer UASs are now widespread due to increased computational power, manufacturing techniques, and numerous commercial applications. The rise of consumer UASs and the low barrier to entry necessary to utilize these systems provides an increased potential for using a UAS as a delivery platform for malicious intent. This creates a new security concern which must be addressed. The contribution presented in this work is the realization of counter UAS security technology concepts viewed through the traditional security framework and the associated challenges to such a framework.**

***Index Terms*—CUAS, counter unmanned aircraft systems, physical security, education**

I. Introduction

The domain of counter unmanned aircraft systems (CUAS) remains a speculative, emerging space in both government and industry. Due to the rapidly changing unmanned aircraft system (UAS) capability and increasing availability, a strong need for an equivalent CUAS program is required. UAS represent a fundamentally distinct challenge for security in ways that past threats have not; there are no known practical delay techniques, UAS move in all three dimensions, a person of limited technical background can construct, operate, and execute complex tasks with minimal skill, UAS can attain very high speeds, and UAS can be designed to carry payloads of notable weight.

In addition to these current capabilities, UASs are rapidly changing as commercial markets push for longer flight times, heavier payloads, and more autonomy. Future UAS capabilities will likely increase exponentially as major commercial companies have identified the cost-savings and increased revenue available from autonomy technology. The Federal Aviation Administration (FAA) is projecting 7 million small drones to be occupying U.S. airspace by 2020 [1]. The collection of these new and rapidly changing threat capabilities requires a re-evaluation of traditional security design processes.

II. Security Education Setup and the DEPO Process

The Design and Evaluations Process Outline (DEPO) developed by Sandia National Laboratories, shown in Figure 1, is an internationally accepted methodology for designing and analyzing a physical protection system (PPS). DEPO is a systematic approach consisting of three major steps, which iterate until the PPS yields acceptable results [2].

1) Determine requirements of the PPS with consideration for site operation and safety.
2) Design and characterize the PPS in terms of detection, delay, and response. The goal is a balanced and robust system.
3) Analysis. Quantify both component and overall PPS performance.

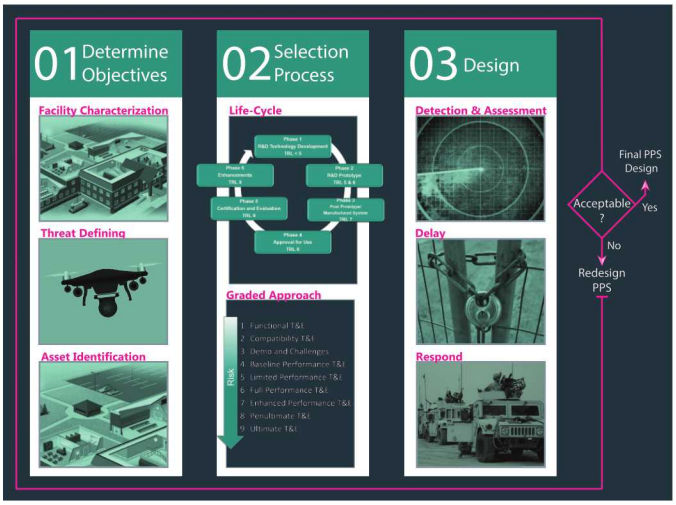

Fig. 1. Design & Evaluation Process Outline (DEPO).

III. Determine PPS Objectives

A. Facility Characterization

It is essential that the facility being protected is understood fully in terms of physical conditions, operations, legality, and its surrounding environment. Knowing the physical conditions such as site boundaries, building locations, and existing physical protection features within a complex is key. CUAS is unique in that most sites do not have an integrated PPS system built to detect, delay, or respond to UAS threats. If a site does have a CUAS technology, it is usually separate from the existing infrastructure and requires additional manpower to operate and maintain. UASs also complicate the issue of site boundaries. Site boundaries have traditionally been defined as a two-dimensional paradigm that that could use components such as barriers, doors, and fences to mitigate threats of interest. UAS mobility in all three dimensions thus elevates the site boundary to extend to three dimensions.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Several challenges in both technical and legal domains emerge under this new paradigm. The most visible and complex aspect of facility characterization is the legal issues that should be considered when designing and implementing a PPS. The FAA includes UASs under a law that states "United States jurisdiction over aircraft sabotage to include destruction of any aircraft in the special aircraft jurisdiction of the United States" [3]. In short, this law makes shooting down a drone a federal crime.

Lastly, knowing what kind of environments are near your site can drastically change how you perceive a UAS. With the widespread personal use of UASs for photography, or simple recreation, a long-distance detection of a UAS poses a much larger threat in rural environments compared to urban environments.

B. Threat Defining

A design basis threat (DBT) is used as a management and design tool to help decision-making executives and establish technical requirements for designers. Knowing the capability of an adversary can greatly impact the DBT. For example, knowing the number of UAS intruders, if these UAS carry a payload, what make and model of the UAS, estimated flight time, or if the pilot has insider information would greatly assist in determining the severity of threat imposed by a UAS.

An adversary can use UASs for a wide array of actions, Cansler et. al [4] has identified several potential and/or proven cases where UASs have been used to carry out adversary actions.

1) Trespassing - In July 2015 a government employee told the Secret Services that he lost control of a small recreational drone before it crashed on the White House Lawn. It is illegal to fly in the restricted air space above and around the White House, and the complex was put under lock-down until the device was examined and cleared [5]. While in this example the pilot did not have any adversarial motives, this was still trespassing into a restricted zone. In July 2016, UASs were spotted over the Savannah River Site (SRS). Eight UASs were spotted by the protective force and professional staff at the facility. The incident triggered an investigation by federal agencies [6]. The reason for the UAS flights and who operated them is currently unknown.
   While these are just a few incidents that did not results in any known harm, the potential threats include: a goal of disruption, damage to employees, operational interference, and a waste of resources [4].
2) Surveillance Incidents - U.S. Customs and Border Control have noted how criminals are now using UAS to watch Border Control officers to identify gaps and radio to their counterparts where to go to avoid being arrested. Other criminal organizations have begun using UASs to survey police departments for witness intimidation schemes to see who might be working with the police [7]. Potential threats include the goal of intelligence collection, adversary information gathering, corporate or political espionage. Reconnaissance technologies include quiet/high altitude flight capability, audio, visible video, thermal video, LIDAR, and electronic cyber sniffing [4].
3) Event Disruption Incidents - In July 2018, Greenpeace activists crashed a superman shaped UAS into the wall of a French nuclear site. The UAS was harmless but was able to enter into the facility without resistance. The state-controlled company operating the nuclear facility is planning on filing a police complaint in response to the incident [8].
   In the winter of 2017 the FBI's Hostage Rescue Team was thwarted by a swarm of UASs. The FBI has set up an observation post to assess an unfolding situation, when UASs starting making series of high-speed low passes at the agents essentially blinding them [7]. While many of the details of this incident are not public, the technology of UAS swarms and their relative ease of use heighten the need for better CUAS technologies.
   Potential threats include the goal of disruption, direct/indirect interruption, and unauthorized broadcast [4].
4) Cyber Espionage Incidents - In Singapore 2014, during the security conference, Black Hat, which provides security consulting, training, and briefings, a security firm, SensePot unveiled its Snoopy UAS. This particular UAS has software integrated in that can be used to hack smartphones and steal the users personal data exploiting the wireless signal. Developers were able to demonstrate this functionality to attendees by pulling data and from hundreds of conference attendees and presenting it to them. While this technology is not necessarily something new, combining the software to a UAS gives many more delivery options to hackers, including covering large areas, and entering facilities that a person with a laptop could not easily enter [9].
   Potential threats include the goal of intelligence collection, illegal corporate competition exploitation, and criminal agents. Methodologies include hiding drones in inaccessible locations, and electronic eavesdropping with Wi-Fi and cellular snooping [4].
5) Contraband Delivery Incidents - On July 29, 2015 a drone was used to deliver contraband to Mansfield Correctional Institute. The drone flew over the yard and dropped the package. The package was picked up by an unwitting inmate causing a brawl between more than 200 inmates [10]. Two years later, in December of 2017, ten men were found guilty of smuggling drugs into a prison in Worcestershire, England. The group was convicted of organizing 49 drone flights with an estimated 1.3 million dollars worth of prohibited items [11]. While these are only a few of the multiple incidents, the rise in the number of incidents and the scale suggests a growing trend.
   Potential threats include smuggling contraband such as phones, narcotics, weapons, or even satellite television [4].
6) Weapon/Payload Attack - September 2011, a man was arrested and charged with plotting to attack the Pentagon

and the U.S. Capital using UASs. Undercover investigations led the FBI to the man, who then supplied him with fake C-4 explosives and non-functional rifles and grenades [12]. This incident, though not successful, shows how a person of limited technical background become a threat to an entire nation. For the first time since the Korean War 65 years ago, U.S. ground forces are under attack from enemy aircrafts. In particular small quadcopter UAS what are essentially grenades. In a single month during the Battle of Mosul, enemies flew over 300 UAS missions with about one-third being armed strike missions [13].

Potential threats include hostile intention, state actor attack, terrorism, and swarm attacks with multiple drones [4].

C. Asset Identification

It is not possible or practical to protect all assets within a facility. A criteria for selecting items to protect depends on the undesirable consequences to be prevented, identifying the critical assets that require protection, and knowing where these assets are located in the facility will change how the PPS is designed to protected against UASs.

IV. CUAS Selection Process

Prior to doing a PSS design, a CUAS technology needs to be selected to meet desired performance per the facility DBT. A credible, consistent, and comparable T&E methodology that can be leveraged by industry, academia, and government agencies is necessary to effectively select a CUAS technology for a PSS. This T&E methodology will help identify CUAS capability gaps that require further technology development to meet the security needs for critical infrastructure.

A. Life-Cycle

Technology Readiness Levels (TRL) range from basic research (TRL 1) to an evaluated and certified system (TRL 9). Figure 2 shows the life-cycle phases of CUAS technology along with the corresponding TRL. The majority CUAS are still relatively low in TRL, residing in phase 2, but are being implemented as if they are in phase 4. This is due to the emerging nature of CUAS and the need to field elements capable of mitigating UAS at any level.

Once at the analysis stage of the DEPO process, the component and overall CUAS PPS performance will be evaluated and given a TRL level. If this TRL level is not higher than the approval for use phase in the life-cycle, the PPS is deemed not acceptable and the DEPO process will loop back to providing enhancements and redesigns necessary to correct for system inadequacies. Re-evaluation of existing CUAS systems should also be done on a regular bases, as both targets and threats adapt and change rapidly in this emerging space.

1) Research & Development Technology Development - While industry is developing CUAS technologies that address the current threat. Academia and/or national laboratories investigates higher risk, far reaching research that address emerging threats as well as future threats, leveraging their resources, capabilities, modeling, and expertise. Often far leaning low TRL, this technology aides the commercial industry, and usually span multiple year efforts.
2) Research & Development Prototype - When the CUAS developer has created the prototype, developer testing and evaluation (T&E) will be required prior to commercialization. This is usually the first "real" demonstration of the device outside of internal developer testing. This represents a major step forward, however, the device may still be composed of elements that are not optimally organized.
3) Post Prototype/Manufactured System - Once a CUAS developer has completed the R&D prototype phase, the system is now considered a manufactured system and therefore, third party validation testing is required. It is important that third party validation be performed for the entity utilizing the CUAS technology in order to make a risk based decision.
4) Approval for Use - Performing the T&E in this phase is important to reduce the risk of deployment, as well as, re-evaluation of significant enhancements prior to deployment. The additional T&E that may be performed in this phase includes degradation, vulnerability, and/or blackhatting.
5) Certification and Evaluation - Certification and Evaluation is important in order to try to detect any premature failures and latent defects in the equipment as well as assessing the adequacy of logistics support. Re-evaluation of significant enhancements should also occur in this phase prior to those upgrades being deployed.
6) Enhancements - After the certification and evaluation is completed, the threat will continue to change and new technologies will emerge, which will require enhancements to the existing CUAS technology. As these enhancements are introduced, the cycle continues in order to mature, evaluate, and certify those enhancements for deployment.

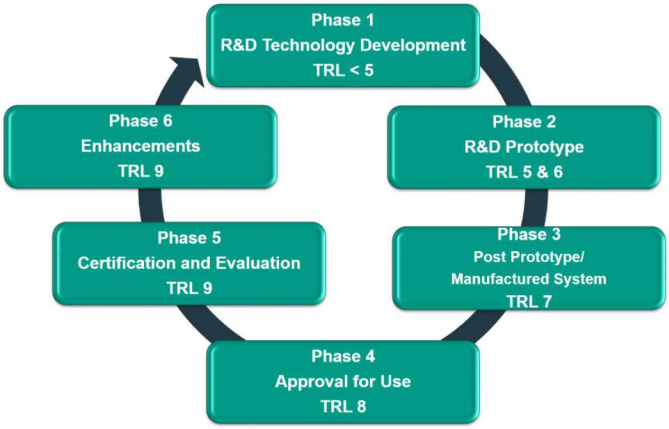

Fig. 2. Life-cycle of Product.

The facility (or licensee) will need to redesign/upgrade the technology to correct noted inadequacies and re-evaluate to determine that the inadequacies are corrected. Re-evaluation should be done on a regular basis, as targets and threats change, both locally and globally.

B. Graded Approach T&E Levels

The graded approach has nine levels corresponding to the levels of T&E that can be done when testing a CUAS system.

1) Functional T&E - This level of testing will validate the specific scenarios that the CUAS is effective and basic functions. This involves pass/fail requirements in a scenario based test. If this is the only level of testing that is performed prior to deployment, the CUAS owner accepts many unknowns and therefore a high amount of risk.
2) Compatibility T&E - Temporary limited deployment in a controlled environment to identify impacts to normal operations.
3) Demo and Challenges - This task reduces risk by identifying the scenarios or conditions that may be effective. It does not tell you how the system may perform in more realistic situations.
4) Baseline Performance T&E - Standard testing suite to establish baseline performance including: sensing points, assessment points, and neutralization points. With this level of testing you begin to quantify the performance of the CUAS on when sensing, assessment, and neutralization will occur.
5) Limited Performance T&E - Standard testing utilizing a repeatable test methodology to expand baseline performance to include: mapping out the volumes, probability of sensing, assessment, detection, and neutralization. This level of T&E also includes limited nuisance and false alarm rate (NAR/FAR) testing.
6) Full Performance T&E - In this six month testing window extensive NAR/FAR testing will be performed in a relevant environment similar to where the system will be deployed.
7) Enhanced Performance T&E - Vulnerability and degradation testing is performed trying to identify where an adversary could bypass the system. This is typically done after full performance T&E. This is where most government agencies agree is the minimum amount of testing needed to deploy a system and have an acceptable amount of risk.
8) Penultimate T&E - Blackhatting is performed in one of the following areas: software, hardware or cybersecurity. Full performance and enhanced performance T&E are required prior to penultimate T&E in order to confirm that the CUAS technology under test in capable of meeting required performance metrics.
9) Ultimate T&E - Blackhatting is performed in all of the following areas: software, hardware and cybersecurity after full performance and enhanced performance T&E.

C. Life-Cycle Phase versus T&E Level

There is a strong link between the Life-Cycle Phase and the Graded Approach levels, as seen in Figure 3. For example, there is a high level of probability that you will do a Level 1 Functional T&E while your vendor is in Phase 1 R&D Technology Development in the life-cycle. Baseline sensing volumes, NAR/FAR testing, and extensive performance testing is done when the system is in Phase 3 Manufactured System, indicated in the orange. Phase 4 Approval for Use is not typically done until after vulnerability testing, and blackhatting.

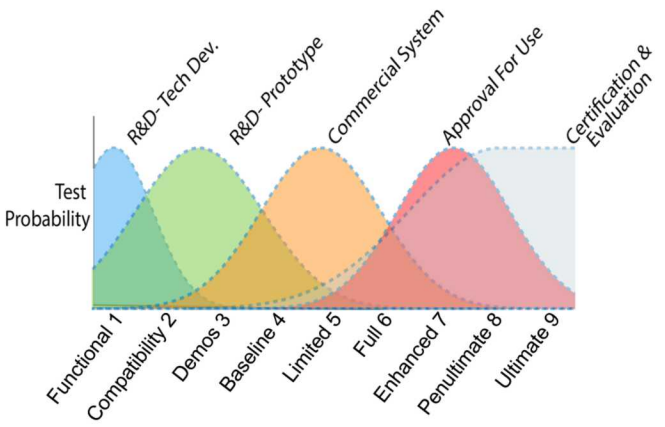

Fig. 3. Life-Cycle Phase versus T&E Level.

V. Designing PPS

The 'detect-delay-response' paradigm used in the DEPO process is predicated on the fact that a site is considered secure when the PPS is shown capable of detecting the adversary attack early enough and delaying the adversary long enough to allow the security to interrupt and neutralize the threat [2].

A. Detection & Assessment

Early detection and identification is the key to effective neutralization of the UAS threat [14]. In order to discover an adversary action the following events must occur [2].

1) A sensor reacts to a stimulus and initiates an alarm.
2) The information from the sensor and assessment subsystems is reported and displayed to a security operator.
3) A person assess information and judges the alarm to be valid or invalid.

The North Atlantic Treaty Organization (NATO) Industrial Advisory Group Study SG-170, "The Engagement of Low, Slow and Small Aerial targets by GBAD (ground based aerial defense)" stated that "No sensor type alone is able to provide sufficient tracking and identification capability to offer a reliable and effective defense against the [UAS] threat" [15]. With the expanding technological capabilities of UASs, multiple types of detection capabilities will need to be leveraged including visible and infrared imagers, radar, acoustic emissions, electromagnetic emissions, and/or induced magnetic fields [16].

B. Delay

In PPS, delay is defined as the slowing down of adversary progress after detection. This is where traditional PPS and a CUAS PPS differ the most. With the current state of technology, there are minimal delay options for UAS and no effective options to delay from entry within a site's three dimensional boundary. Current CUAS efforts are focusing on longer-distance detection. The earlier a UAS is detected with long-range sensors, the more time there is available for a sites response capabilities to respond to the threat.

C. Response & Neutralization

The broad definition for response and neutralization is denial of mission, including destruction of the UAS target [16]. Non-destructive response to a CUAS threat would serve the purpose of neutralizing the threat, but would also aid in the investigation of the source of the threat and conducting forensics analysis. In general, non-destructive response options are relatively slow and require a longer response time, which could be problematic in a case of a fast attack. Alternatively, destroying the UAS would prevent successful completion of the adversaries mission, but could results in difficulties finding the adversary operator [14].

VI. Analysis

PSS is a complex configuration of security elements, an analysis should be performed on the PSS to evaluate the effectiveness of the design. The goal of the UAS threat is to complete a path to a target with the least likelihood of being detected or neutralized by the CUAS technology. The measure of effectiveness for neutralizing an adversary is dependent on timely detection. In order to effectively analysis the purposed CUAS design, the analysis will leverage the CUAS T&E performance metrics results to verify the design meets the requirements outlined in the DBT prior to implementation.

VII. Conclusion

With the rise of consumer UASs and the limited technical background necessary to utilize these systems, a new security concern is realized. This paper highlights the challenges to the traditional physical security framework when a new kind of threat is introduced. With the wide range of threats created by UASs, all new and innovative CUAS must be tested and challenged before being added into existing PPS. We have presented a comprehensive methodology to define the threat, design the PSS, select the CUAS technology, identify the capability gaps, expose associated risks via analysis, and provide a comparative, repeatable and quantifiable methodology to implementing this emerging technology.

Acknowledgment

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energys National Nuclear Security Administration under contract DE-NA0003525. This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government.

References

[1] F. ADMIN., "Faa releases 2016 to 2036 aerospace forecast," last updated Mar. 24, 2016.

[2] M. L. Garcia, *Design and evaluation of physical protection systems*. Elsevier, 2007.

[3] "Destruction of aircraft or aircraft facilities. 18 u.s. code § 32," 2006.

[4] J. Cansler, N. Ruff, and M. Schreiber, "Drone use and defense by enterprise security management: Uas applications, concerns, and countermeasures," Presented at ASIS International 2017 Annual Seminar, Dallas, Texas, 2017, September.

[5] B. Jansen, "Drone crash at white house reveals security risks," *USA Today, January*, vol. 26, 2015.

[6] T. Gardiner, "Eighth drone spotted in srs skies," *Aiken Standard*, 2016, July 5.

[7] P. Tucker, "A criminal gang used a drone swarm to obstruct an fbi hostage raid," *Defense One*, 2018, May 3.

[8] M. Greenwood, "Greenpeace activists fly 'superman' drone in to french nuclear site," *The Hill*, 2018, July 4.

[9] K. Gittleson, "Data-stealing snoopy drone unveiled at black hat," *BBC News*, 2014, March 28.

[10] T. Liddy, "Drone dropping drugs over prison yard sparks brawl at mansfield correctional institution in ohio," *ABC News*, 2015, August 4.

[11] BBC, "Ten sentenced for smuggling drugs into prisons by drones," *BBC News*, 2017, December 13.

[12] C. W. Staff, "Man, 26, charged in plot to bomb pentagon using model airplane," *CNN*, 2011, September 29.

[13] M. Pomerleau, "How $650 drones are creating problems in iraq and syria," *C4ISRNET*, 2018, January 5.

[14] A. Solodov, A. Williams, S. Al Hanaei, and B. Goddard, "Analyzing the threat of unmanned aerial vehicles (uav) to nuclear facilities," *Security Journal*, vol. 31, no. 1, pp. 305–324, 2018.

[15] NATO, "Industrial advisory group study sg-170 'the engagement of low, slow and small aerial targets by gbad (ground based aerial defense)'," 2013.

[16] G. C. Birch, J. C. Griffin, and M. K. Erdman, "Uas detection classification and neutralization: Market survey 2015," Sandia National Laboratories (SNL-NM), Albuquerque, NM (United States), Tech. Rep., 2015.