IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received April 14, 2017, accepted April 21, 2017, date of publication April 25, 2017, date of current version June 7, 2017.

Digital Object Identifier 10.1109/ACCESS.2017.2697979

Systems Engineering Baseline Concept of a Multispectral Drone Detection Solution for Airports

RICK L. STURDIVANT[1], (Member, IEEE), AND EDWIN K. P. CHONG[2], (Fellow, IEEE)
[1]Azusa Pacific University, Azusa, CA 91702, USA
[2]Electrical and Computer Engineering Department and Mathematics Department, Colorado State University, Fort Collins, CO 80523, USA
Corresponding author: Rick L. Sturdivant (ricksturdivant@gmail.com)

ABSTRACT The baseline concept for a multispectral drone detection (MSDD) system for use in airports is generated. The baseline development process is based on a modified system of systems architecting with ilities (SAI) method. The solution uses multiple independent sensors, which when the sensor outputs are combined, provide functionality that the individual systems were never intended to provide. Also, several sensors are pre-existing and have their own funding, operations, and management. The problem of drone detection is described and examples are given, which justify the need for the system. Then the specific need for airport protection is described. The result is a feasible baseline design that is capable of meeting the need.

INDEX TERMS Drone, radar applications, sensor systems, millimeter wave radar, cameras, explosion protection.

I. INTRODUCTION

There is growing concern that drones will be used as military weapons against civilian and military targets. Recent events illustrate the existence of significant vulnerability. Take, for instance, the accidental landing of a remotely controlled drone on the U.S.A. White House Lawn. The crashed drone, shown in Fig. 1, was about 2 feet in diameter. The drone was flown by a government employee from his apartment balcony. The problem is the owner of the drone was intoxicated while flying it. He claims to have lost control at approximately 3AM while flying it for recreational purposes. Though Secret Service officers on duty at the time claim to have seen it, the radars installed around the white house were not able to detect the drone. The reason is that the installed radar systems around the white house were designed to detect larger fast moving objects like planes and missiles. A small drone is either not seen at all by these radars, or it is mistaken as a bird and ignored. Though this was an innocuous event, it reveals a serious vulnerability that exists. If the White House is not protected against these types of drones that could be weaponized with explosives, chemical, biological, or nuclear weapons, then other sites such as power generators, nuclear power plants, schools, and government buildings must be at even greater risk.

Another example of the threat is that a man landed a drone with radioactive material on the roof of the private residence of the Japanese Prime Minister [1]. The perpetrator of the incident, a 40 year old man, said he purposely landed the drone where he did as a protest against the Japanese government's nuclear energy policy.

FIGURE 1. Image of the drone that crash landed on the south lawn of the US White House.

In another example, two men were arrested by German police over a plot to use a model plane as part of a terror plot. The report said, "They are suspected of having sought to acquire information and equipment necessary to carry out 'radical Islamist explosive attacks using remote controlled airplanes,' according to a statement on the website of Germany's Federal Public Prosecutors' Office" [2].

These examples demonstrate the reality of the threat, but a possible objection to this threat is that only limited amount of damage can be caused by a single drone. While this objection underestimates the damage that 1-2kg of C4 explosives can inflict, it also misses the fact that drone attacks can be perpetrated simultaneously using multiple drones. Consider, for instance, students at the Naval Postgraduate School in Monterey, CA demonstrated that a swarm of 50 drones can be controlled by one operator [3]. This type of swarm attack poses a threat much greater than a single drone. As a result, the threat from drones is real and solutions must be developed.

The focus of this work is specifically the threat of drones to airports which is taken seriously. For instance, the USA Federal Aviation Administration (FAA) has reported that there are more than 100 sightings of unauthorized drones at airports each month [4]. As a response to the threat posed by drones to airports, the FAA developed its Pathfinder Program. The purpose of the FAA program is to evaluate procedures and technologies designed to identify unauthorized UAS operations in and around airports [5]. As part of that program, the FAA has recently signed cooperative research and development agreements with three different companies. Therefore, this is an area of active research and solutions are still being developed. This work focuses on the development of a baseline concept for a System of Systems (SoS) for the detection and thwarting of drones at airports.

The detection and tracking of drones is not new. The majority of the prior work on drone detection can be divided into three main types with some examples of overlap. The first type is detection using sound. For instance, in [6] audio classification of drones was performed using data mining techniques. They used a Hidden Markov Model for phenome analysis and consumer quadcopters were used in their experimentation. They found that data clustering similar objects and drone flight states helped speed up the analysis and improve classification of the detected drone. Another example of sound detection of drones is in [7] which used correlation methods and audio fingerprinting methods. The audio fingerprinting method leverages consumer mobile phone applications which recognize songs. These apps sample a portion of a song, create a spectrogram, and compute similarities to stored songs in a database. Their result showed the correlation method provided higher scores for detection. Another investigation [8] compares various correlation methods experimentally. For instance, the Spearman and Kendal rank-correlations were used but were not able to show sufficient differences between sound sources. However, Pearson and cross-correlation showed acceptable discrimination between sound sources.

The second type of system uses cameras for the detection of drones. In [9], for instance, a moving camera is used to track the movement of a drone and uses a regression-based approach. They achieved object-centric learning-based motion stabilization and were able to classify targets in spatio-temporal image cubes. A completely different approach is taken in [10] which uses 'humans-as-sensors' by using a smart phone application and leveraging data captured on personal smart phones. While this method is interesting, it requires cooperation of users and is prone to misuse since the application is distributed to users.

The third type uses RADAR to detect drones. For instance, in [11] the system is based on a 35GHz Frequency Modulated Continuous Wave (FMCW) radar with 0.02 to 2.0 Watts of peak transmitted power and is used to detect when a drone passes a 'barrier.' The results show that the drone was detected at ranges as far as approximately 50 meters and velocities as high as approximately 3.5 m/s. Another example is in [12] which uses an antenna array operating at L-Band with approximately 10kW of transmit power. However, the range of radar systems for drone detection is limited due to the small radar cross section (RCS) of the drones. Also radar return signal clutter makes it even more difficult to distinguish drone targets at airports. Nevertheless, prior work demonstrates that it is possible to detect drones with radar.

In addition to the three main types of systems, other workers have been proposed to combine multiple sensors. For instance, in [13] several possible detection methods are considered including audio, video, thermal, RADAR, and radio frequency detection. The demonstrated system uses video and audio detection and a radio frequency (RF) gun to disable the drone. The audio method uses a template matching method and the video method uses an absolute difference method between consecutive frames to detect color and motion. The results show that motion was detected as long as the drone occupied a threshold minimum number of pixels.

However, the prior demonstrate varying levels of performance but take a narrow view on integrating sensor functions for the purpose of detecting drones. Furthermore, the prior work fails to utilize existing sensors and instead propose the development of custom sensors tailored specially to drone detection. Also, a systems engineering approach has not been taken for developing solutions for drone protection at airports let alone a SoS approach.

For these reasons, an alternative is to take a bigger perspective—A SoS perspective and consider how multiple systems can be used together to meet the need. This approach will assess methods to sustain value delivery over time, system value propositions, non-functional requirements, customer/ user needs, already existing systems, possible new systems, and architecture alternatives. This type of SoS approach is expected to be more responsive to changes in the operational environment and increase the likelihood of the system meeting customer needs. The ability to adapt is important for this system since drone technology is still maturing and expanding. The SoS approach has the potential to provide a viable solution and the first step is the development of a feasible baseline concept which is the focus of this work.

There are at least five categories of drones [14] and some of their critical characteristics are summarized in Table 1. The first type is called the nano drone with a maximum mission radius of 100-500 m and a payload of less than 0.2 kg. The second type is the micro drone which weights less than 2 kg

TABLE 1. Drone Categories Used In This Work (based upon [14]).

Drone Category	Maximum Mission Radius	Payload
Nano	100-500 meters	< 0.2 kg
Micro	5 km	0.2-0.5 kg
Mini	25 km	0.5-10 kg
Small	50-100 km	5-50 kg
Tatical	> 200 km	25-200 kg

FIGURE 2. Major steps in the systems engineering process consist of Concept Development, Engineering Development, and Post Development (After [15]).

with a maximum mission radius of 5 km and a maximum payload of 0.2-0.5 kg. The third type is a mini drone with a maximum mission radius of 25 km and a maximum payload of 0.5 to 10 kg. The fourth type is a small drone with a maximum mission radius of 50-100 km and a maximum payload of 5-50 kg. The fifth type is the tactical drone with a maximum mission radius of 200 km and a maximum payload of 25-200 kg. The focus of this work is on mini drones and larger because their payload capacity means they can carry explosives that can cause significant damage.

This work is divided into thirteen sections. In Section II the System of Systems Architecting using Ilities (SAI) method for concept development is described. In Sections III to X the eight steps to the SAI method are applied to the drone detection system. Section XI describes some methods for drone thwarting and Section XII is the conclusions and recommendations for additional work.

II. CONCEPT DEVELOPMENT USING THE SAI METHOD

System architecture is an important step in the development of a baseline concept. This is because it sets many important aspects of the solution and guides future development. This work utilizes the SAI method for determining the baseline concept solution. Therefore, it is important that a definition of SoS architecting is provided. As a starting point, consider the definitions:

1) In IEEE Std 610,12 architecture is defined as ''the organizational structure of a system or component'' [15].

2) In the ISO/IEC/IEEE 24765 International Standard, it is defined as ''fundamental organization of a system embodied in its components, their relationships to each other, and to the environment, and the principles guiding its design ad evolution ... the organizational structure of a system and its implementation guidelines'' [16].

3) In [17], the authors define ''architecting as the process of structuring the components of a system, their interrelationships, and their evolution over time.''

Though all three of these definitions are useful, the last definition includes the aspect of the system evolving over time. This is an important factor for SoS and as our society becomes more interconnected through data networks, this aspect of the architecture being adaptable to change is critical.

An output from successful system architecture is a baseline concept. The concept development step in a system's life cycle is shown in Fig. 2 as the first systems engineering step for a new system [18]. Also shown in the figure is the SAI approach [19]. A simplified version of this method will be used for the Multi-Spectral Drone Detection (MSDD).

The details of the SAI method will not be repeated, but its eight steps are provided here for completeness. They are [19]:

Step1-Determine Value Proposition and Constraints: This step requires the identification, understanding, and documentation of overall SoS architecture value propositions.

Step2-Identify Potential Perturbations: This is the identification and categorization of possible perturbations that can interfere with the SoS value delivery.

Step3-Identify Initial Desired Ilities: In this step, the ilities are identified that promote the long-term behavior of the SoS. Combining possible perturbations with desired ilities can begin to distinguish ilities.

Step4-Generate Initial Architecture Alternatives: The purpose of this step is to generate value-driven (values from Step 1) alternatives for the SoS architecture. The alternative definitions will include design variables and operational variables along with concepts of operation.

Step5-Generate Ility-Driving Options: This step is concerned with the generation of and selection of options that can be added to architecture alternatives to achieve desired ilities.

Step6-Evaluate Potential Alternatives: This is the modeling of various alternatives (generated in Step 4) in terms of relevant metrics. Example metrics are value (attributes and cost), and ility metrics. This may include quantitative modeling and simulation, but can also occur at higher levels of abstraction.

Step7-Analyze Architecture Alternatives: This is the deep analysis of data generated in Step 6 for the purpose of developing understandings of the possible trade-offs that exist with the alternative SoS architectures.

Step8-Trade-off And Select ''Best'' Architecture With Ilities: This step uses the deep analysis results from Step 7 to make decisions about the preferred architecture. The output from this final step is the baseline solution that will be carried forward into detailed design. This last step will use ilities with Quality Function Deployment (QFD) trade study approach as described in [20].

The eight steps start with an operational needs description which is a statement of the operational goals of the SoS. For the drone detection SoS, it is ''the main operational goal of the MSDD SoS is to provide information to enhance protection of airport assets against attack by drones.'' The attributes needed for the system are derived from this statement.

III. SAI METHOD STEP1: DETERMINE VALUE PROPOSITION AND CONSTRAINTS

This step requires the identification, understanding, and documentation of overall SoS architecture value propositions. This step in the process can be broken down into six sub steps.

A. DEVELOP VALUE PROPOSITION STATEMENT

During this step, the value proposition is explored and written down. The value proposition for the MSDD system is that it will provide the information necessary to protect key airport assets. The value of this lies in the assets that are at risk. A few of the assets that are vulnerable to drone attack are [21]:

- Passengers and visitors
- Aircraft (with or without passengers aboard)
- Cargo and mail terminals
- Airport traffic control tower
- Parking garages
- Fuel Facilities
- Airline buildings
- Airport information systems
- Electric power supply facilities

The value of the systems is that it provides information needed for the protection of these key assets.

B. IDENTIFY AND ASSESS CONSTITUENT SYSTEMS

The goal of this step is to determine possible assets that may be combined to form the SoS. This includes new systems and already existing ones that have relevant capability and availability. It is important that this step not prematurely eliminate systems from consideration so the focus is upon generating an exhaustive list which will be culled later.

In the case of airport, the existing assets are a combination of technology and human. Some exist now and are found at many airports. Others considered here would require development. The list of existing assets are:

1) SURFACE MOVEMENT RADAR (SMR)

These radar systems detect aircraft and vehicles and plot their location in real time on a map displayed on a computer screen. An example is the Airport Surface Detection Equipment, Model X (ASDE-X) developed and sold by SAAB-Sensis [22]. It consists of a radar, multilateration technology, and satellites to enable air traffic controllers to track the ground movement aircraft and vehicles. The system has been deployed in 35 airports in the U.S.A [23]. Similar solutions have been deployed at other major airports worldwide. It provides proper operation in daylight or nighttime.

2) VIDEO SURVEILLANCE (VISUAL IMAGING)

Most airports have video surveillance for security. The video cameras are distributed around the airport and the video feeds are available for security.

3) AIRPORT SECURITY PERSONNEL

Airports have ground patrols actively providing security for the airport. They are an asset that can be used for the detection of drones.

4) AIR TRAFFIC CONTROLLERS

Air traffic controllers have access to multiple airport sensor outputs and can be used as an asset in the detection of drones.

In addition to existing assets, new sensors can be developed and deployed to detect drones. They are:

5) AUDIO SENSORS

Audio sensors can be used to detect drones. Most airports do not use audio sensors sufficient for drone detection so that this type of sensor would have to be developed and deployed.

6) INFRARED (THERMOGRAPHIC) CAMERAS

These cameras have the benefit of being able to detect objects that generate heat and can operate at night time. This is because the sensor detects heat signature in the infrared range. Since drones generate heat at their motors and in their electronics, the heat signature can be detected.

7) LIDAR (LIGHT DETECTION AND RANGING)

This can be used for optical imaging in the ultraviolet, visible, or near infrared spectrum. It provides operation in daylight or nighttime.

8) MILLIMETER-WAVE (mmW) RADAR

In addition to the existing radar sensors, other sensors can be developed that have attractive capability. For instance, millimeter-wave radars can be used for target tracking since they can have very narrow antenna beam widths. Also, the target size and features are larger compared to the wavelength at mmW frequencies. An example is a 35GHz FMCW radar proposed for drone detection in [23]. It provides proper operation in daylight or nighttime.

9) LOW COST RADAR

An option for the radar sensor is to use multiple smaller radars with less capability than the SMR radar. A benefit of using smaller radars is they can provide coverage in areas that a single SMR cannot achieve. For instance, the SMR coverage will be shadowed by buildings, trees, and other obstructions. In these instances, low cost radars can be distributed throughout the airport to augment the capabilities of the SMR. In other cases, such as smaller airports with lower operating budget, low cost radar can provide the capability the SMR replacement capability. It provides proper operation in daylight or nighttime.

C. LIST KEY ORGANIZATION AND POLICY CONSTRAINTS LIMITING ARCHITECTURES

There are two key organizations who will have policy influence on the solution. The first is the airport authority. For the Long Beach, CA airport, the authority is the Airport Advisory Commission and the airport management. The role of the advisory committee is to guide the overall airport mission and long term planning. The airport management are concerned with execution of the airport purpose.

The second organization is international and national regulatory groups. At the international level, the International Civil Aviation Organization (ICAO) has recognized the need for protection against unlawful use of drones around airports. In fact, a recent report from them state that drones introduce, ''new considerations with regard to fulfilling safety-related responsibilities such as incorporation of technologies for detect and avoid, command and control, communications with [air traffic control]ATC, and prevention of unintended or unlawful interference'' [25] In Europe, the European Civil Aviation Conference (ECAC) provides international rules about airport safety. In the U.S.A., the FAA, Transportation Security Administration (TSA), and Department of Homeland Security (DHS) provide leadership at a national level to provide a safe and efficient airport system. Other government agencies with interest in these systems are the national and international communication commissions such as the Federal Communications Commission (FCC) in the USA. They have regulatory control over any radar systems because they will be generating electromagnetic radiation in the spectrum under their control. These national and international groups have interest in airport security.

Since these groups recognize the threat of drones they are actively involved in investigating solutions. This is a key benefit since it means that they are motivated to be actively involved.

D. LIST KEY PHYSICAL AND GEOGRAPHIC CONSTRAINTS

The emphasis is on physical and geographic constraints that limit potential SoS architectures. The main physical and geographical constraint for this type of system is that it must be contained within the airport property boarders. Fig. 3 illustrates a typical airport layout.

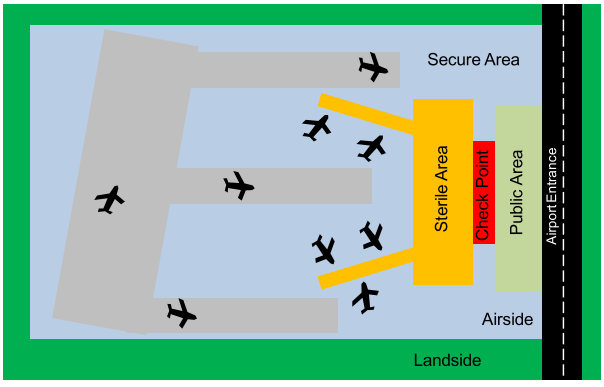

FIGURE 3. Typical layout of an airport.

E. IDENTIFY AND CLASSIFY STAKEHOLDERS

During this step it is important to distinguish between stakeholder types. For this work, we have identified government agencies, airport personnel, airport users, airlines, and airline passengers as system stakeholders. Government officials include the F.A.A. and the Department of Homeland Security in the U.S.A.

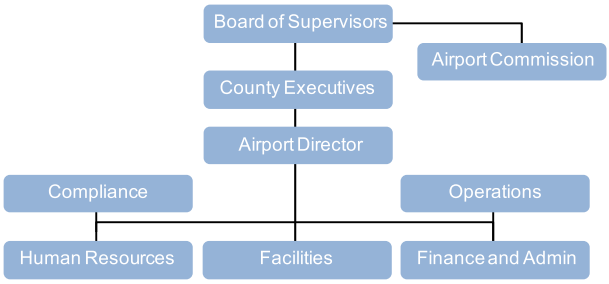

FIGURE 4. Typical airport organizational chart.

Airport employees are often organized into a structure similar to Fig. 4. The employees who will be most actively involved in executing on airport security are the Facilities and Operations groups. The Airport Director is responsible for developing airport policy and the administration of airport activities. The airport employees and executive team are important stakeholders.

Each airport supports a number of different airlines, cargo carriers, private plane groups, and government agencies. These user groups depend upon reliable airport access and so they have an interest in airport security as external stakeholders.

Another stakeholder group is airline passengers. This group is concerned with airport and air plane security, efficient operation of the airport (to limit time spent at the airport), and airport cost that affects their airline ticket.

F. ELICIT STAKEHOLDER VALUE AND DESIGN SPACE PREFERENCES

For the purposes of this work, stakeholder value and design space preferences have been obtained through surveys of stakeholders and experts. For this work, the stakeholder groups surveyed is airport operations and safety personnel. Informal interviews were conducted to determine their value and design space preferences. In addition, a team of engineers, sensor technology experts, and retired sensor company executives was gathered to develop value and design space preferences. The results from each group are summarized in Table 2. The column in the table 'Existing (Y/N)' means has the system already been deployed to meet previously identified needs.

Informal interviews with airport operations and safety personnel at four airports were conducted. The purpose of the conversations was to illicit stakeholder value and design space preferences. The identities of the interviewees and the airports are not being revealed in this report to respect the privacy of the conversations. There are several important results from those conversations.

The first is that it is very clear that airports are well aware of the threat posed by drones and they are actively working with local groups, private industry, and federal agencies to understand the threat and to develop ways to respond. For instance, one of the airports has agreed to be a beta test site for a drone detection system developed by a technology startup

TABLE 2. Ranking of Anticipated Value Delivery.

Rank	Existing (Y/N)	System Name	Justification For Ranking
1	Y	Surface Movement Radar	Sensing in adverse weather
2	N	Low Cost Short Range Radar	Covers shadowed areas
3	Y	Video Surveillance	Detection using video processing
4	N	mmWave Radar	Additional target information
5	N	LIDAR	Additional optical imaging
6	N	InfraRed Cameras	Night time operation
7	Y	Human Observation	Visual confirmation
8	N	Audio Sensors	Additional target information

company. In addition, that same airport is part of a local organization that is being developed to study drone use in their county and local cities.

Second, airports operations and safety organizations desire the ability to provide drone detection, but they are not thinking about thwarting drone attacks. A common thought is that the airports don't have the charter of disabling or destroying drones that pose a threat.

Third, a common theme was that optical systems are perceived as too costly and ineffective. Prior experience with custom optical detection systems has left airport personnel with the opinion that the value offered by them does not justify their expense. That said, the idea of using their existing optical camera's as part of a SoS solution had not been considered and they were open to such a solution. However, the logistics of implementation were unclear.

Fourth, there is a uniform desire for highly accurate detection and low false detections.

Fifth, there is a desire to provide a comprehensive security solution but no master plan to achieve it. The threat posed by drones was acknowledged, but airport personnel are not empowered due to budget and regulatory reasons to implement large scale change.

Sixth, all of the personnel interviewed were only working on methods to manage local drone users. In other words, the current activities on drones at airports is on providing licenses or other authorization to local drone users and development of rules for drone use.

These results are summarized in Table 3 and though the results do provide insight into the airport operations and security personnel value and design space preferences, it is with a relative small sample size. Therefore, a more extensive survey should be conducted.

There are a few results of this step in the SAI method. One result is it provides insight into expectations of stakeholders. This is important since expectations can drive system non-functional requirements. Another result is that it provides insight into possible existing solutions and systems that

TABLE 3. Summary of Airport Stakeholder Preferences.

#	Description	Value-Space Preference	Design-Space Preference
1	Aware of the threat & new technology	Recognize the value to airport security and operations to detect drone	Open to new technologies and willing to be beta test site
2	Not considering thwarting methods	Value of thwarting or disabling drones is not a high value	No design space preferences for drone thwarting
3	Custom optical detection is too costly	Custom optical drone detection systems don't provide enough value	Prefer a concept that does not use custom optical detection systems
4	Desire accurate detection of drones	High value attached to accurate detection	Important objective is high accuracy.
5	Systems must be deployed within the regulatory environment	High value placed on solutions that are deployed within the regulatory boundaries	Concept must be capable of being approved by existing regulatory organizations
6	Existing activities focused on drone user regulation & management	High value placed on management of local drone users	Design should accommodate drone management systems

stakeholders may have knowledge of. In addition, this step aids in defining the problem scope. Finally, this step can also identify external forces and even their impact to system value delivery.

IV. SAI METHOD STEP2: IDENTIFY POTENTIAL PERTURBATIONS

For the MDSS there are many perturbations that can interfere with value delivery over system lifetime for most systems. The perturbations are changes in the system's design, context, or stakeholder needs which can put value delivery at risk. One output from this step is a table of perturbations which categorizes each according to type, space, origin, intention, nature, consequence, and effect. The purpose of this step is to identify and categorization them so that they can be used in later steps to develop ilities and approaches to maintain value delivery over time.

Table 4 is a taxonomy of identified perturbations to the MSDD system. The perturbations are found from interviews with domain experts and team brainstorming activity. The table provides a way to organize and compare them.

Each is categorized according to seven descriptors. The first is type which can be a shift which is a long term change in context or stakeholder needs, a disturbance which is a short term change that requires action for resolution, or a disruption which is a transient effect that requires no action for resolution. A shift means the SoS is not likely to return to its prior state while disturbances or disruptions are temporary. The second category is the space which is the design itself, the context of operation, or the needs of the stakeholders. It is where the perturbation is occurring. The third is origin which refers to the source of the perturbation which can be internal

TABLE 4. Taxonomy of Perturbations to the MSDD SoS.

Perturbation Name	Type	Space	Origin	Intentional	Nature	Consequence	Effect
Weather	Disruption	Context	External	No	Natural	Negative	Reduced Detection
Regulations	Shift	Context	External	Either	Artificial	Either	Various
Response Time	Disturbance	Design	Internal	Either	Artificial	Either	Change in Value
System Maintenance	Disruption	Context	Internal	Yes	Artificial	Negative	Temporary Value Loss
Attack	Disturbance	Context	External	Yes	Artificial	Negative	Change in Value
Communication Disruption	Disruption	Design	External/ Internal	Either	Artificial or Natural	Negative	Temporary Value Loss
System Decommissioned	Shift	Design	Internal	Yes	Artificial	Negative	Change in Value
Incompatible Upgrades	Shift or Disturbance	Design	Design	Yes	Artificial	Negative	Change in Value
Drone Types Change	Shift	Needs	External	Yes/No	Artificial	Negative	Change in Value

to the SoS or one of its systems, external to them, or either. The fourth is the intentionality of the perturbation which can be yes, no, or either. The fifth is nature and should not be confused with the fourth. Nature refers to agency behind the perturbation which can be natural or artificial. A perturbation can be artificial (created by humans) and still be intentional or unintentional. However, all natural ones are unintentional. The sixth is the consequence which is a rating of positive, negative, or either. It is what follows from by the perturbation. The effect is produced by the cause (the perturbation). It is a description of the changes that occur to value delivery resulting from the perturbation. The idea behind this step is that knowledge of perturbations helps SoS architects develop systems that avoid, mitigate, and recover from them.

A. WEATHER

The weather can impact the performance of sensors. For instance, optical systems are essentially disabled by fog. Weather can also impact the performance of radar systems. It also impacts the ability of human observers to detect drones. Therefore, weather can negatively impact value delivery.

B. RESPONSE TIME

The response time is combination of the time required for the SoS to identify a possible drone threat and the time required for drone thwarting systems to be deployed. If the response time is too slow, this will impact effectiveness and other metrics. The SoS response time of the individual systems is out of the control of the SoS, and yet changes in their individual response times affects the SoS. The response time of the system may also improve over time due to added capabilities to the system. Therefore, understanding and accounting for response time changes is important for value delivery sustainment over the SoS life cycle.

C. SYSTEM MAINTENANCE

The systems must be maintained properly which is the responsibility of system management. For instance, optical glass covering visual sensors must be periodically cleaned to maintain high resolution images. Since the MSDD is a SoS, the maintenance of each of the systems is out of the control of the SoS itself. Therefore, value delivery of the MSDD SoS depends upon proper maintenance of each system.

D. ATTACK

An attack is a willful act meant to disrupt the performance of one or more of the systems. The attack can be a random act of vandalism or an intentional act meant to disrupt the system. The attack can be physical or non-physical. An attack can affect value delivery.

E. COMMUNICATION DISRUPTION

Changes in communication status covers events that eliminate or diminish the ability of the system to transfer data (such as sensor data). There are multiple possible causes such as lighting strikes, equipment failure, to name a few. Proper operation of the communication functions in the SoS is essential for value delivery.

F. SYSTEM DECOMMISSIONED

If one of the systems in the SoS is decommissioned by its operators, then there will be shift in SoS value deliver.

G. INCOMPATIBLE UPGRADES TO SYSTEMS

If one of the systems in the SoS is upgraded and its outputs or functioning is incompatible with the SoS, then this will require the SoS to adapt to maintain value delivery or it will impact value delivery.

H. DRONE TYPE CHANGES

As technology changes, the types of drones available will change. As a result, value delivery of the SoS may be impacted if it cannot adapt to changes in technology.

V. SAI METHOD STEP3: IDENTIFY DESIRED ILITIES

In this step, a list of potential ilities is identified that promote the long-term behavior of the SoS. Ilitiy development is important since they are used in subsequent steps in SoS

TABLE 5. List of SoS Ilities With Description and Basis for Including as an Ility.

Perturbation Name	Type	Space
Compatibility	Functions in conjunction with existing drone management systems	Driven by stakeholder survey
Functionality	The ability of the SoS to maintain value delivery over the system life cycle by preserving system functions.	Driven by definition of a SoS Driven by perturbations
Reliability	Provides accurate detection of drones in with low failure rate and low maintenance requirement.	Driven by stakeholder survey
Evolvability	The system must be adaptable to changes in drone technology, regulations, and airport physical changes	Drive by brainstorming sessions Driven by perturbations
Quality	The SoS is well constructed to achieve the desired functions.	Driven by stakeholder survey Drive by brainstorming sessions
Flexibility	The ability to change or adapt to new circumstances.	Driven by stakeholder survey Drive by brainstorming sessions Driven by perturbations
Resilience	The degree to which the SoS can recover quickly from a major disruption while maintaining a high degree of value sustainment.	Drive by brainstorming sessions Driven by perturbations
Adaptability	The capacity of SoS changes to be driven by the external environment. Reconfigurations of the system are driven by external changes.	Drive by brainstorming sessions Driven by perturbations
Interoperability	This is the capacity of the constituent parts of the SoS to work together as a whole.	Driven by definition of a SoS

architecting. They directly impact the priority of system functionality.

In this work, the potential ilities are developed in two ways. First, they are gathered from direct expressions and implied requests from stakeholders. During interviews in Step 1, stakeholders explicitly stated desired ilities. They also expressed them indirectly using language that implies certain ilities. Second, the perturbation analysis in Step 2 revealed ilities. Together these two methods are used to generate system ilities.

Table 5 summarizes the list of potential ilities. It also shows the source of the ility whether it is stakeholder driven, team brainstorming session driven, or perturbation driven.

VI. SAI METHOD STEP4: IDENTIFY DESIRED ILITIES

The purpose of this step is to generate value-driven (values from Step1 alternatives for the SoS architecture. The alternative definitions will include design variables and operational variables and may include basic concepts of operation. Fig. 5 shows the matrix of alternatives. It lists the eight available systems that can be used in this SoS. In theory, if we assume that the SoS will consist of 3 of the systems, then there are 56 combinations of possible SoS alternatives using combinatorial mathematics.

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} \tag{1}$$

Where n is the number of things available which is 8 possible systems for the SoS and k is the number of things selected which is the actual number of systems that make up the SoS. This means that (1) can be used to determine the number of combinations of systems that can be generated given the number of systems out of the available 8 systems that will be used to construct the SoS.

One option for reducing the number of possible combinations is to restrict the SoS to systems that already exist and are deployed. If this is done and all available sensors

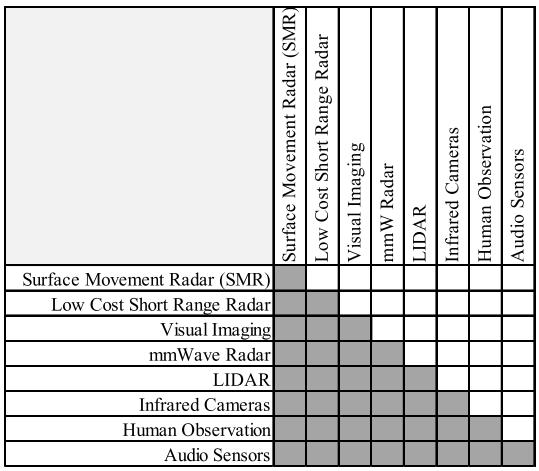

FIGURE 5. Matrix of possible SoS combinations given the available systems.

are used, then one SoS architecture is the SMR + Visual Imaging + Human Observation. As mentioned earlier, state of the art SMR systems have been deployed in the U.S.A. and at major airports worldwide, visual imaging systems exist at airports as part of existing security systems, and human observation exists in the form of airport security and air traffic control operators. This combination of systems will be called Option 1 for the SoS.

Another option for selecting architectures for the MSDD system is based upon their ranking. Referring back to Table 2, it lists the available systems ranked on effectiveness. If the first four systems are selected, then this can provide another option. It will consist of SMR + Low Cost Short Range Radar + Video Surveillance (Visual Imaging) + mmWave Radar. This approach will be called Option 2 for the SoS.

Another option is to combine Option 1, the already deployed sensors, with the top ranked option that is not already deployed. This results in a SoS consisting of SMR +

Video Surveillance (Visual Imaging) + Human Observation+ Low Cost Short Range Radar. This combination will be called Option 3 for the SoS.

Another option is to add infrared sensing to Option 3. In this case the sensors involved would be SMR + Video Surveillance (Visual Imaging) + Human Observation + Low Cost Short Range Radar. The benefit, of course, is the detection capability of infrared cameras. This combination will be called Option 4 for the SoS.

All four of the options identified share a few common features for their concept of operations. First, each of the SoS options will require a method for interconnecting the systems. This will require software for integrating the sensor outputs. The software will need to be flexible in its interfaces and data formats so that new systems can be added. Second, the SoS will require a control room for monitoring the results. It may be that the system is integrated with existing FAA control room systems. Third, the SoS will require personnel for monitoring the fused sensor output which also may be FAA personnel such as air traffic control. All the options identified so far share these common features for the fusion of their data and management.

VII. SAI METHOD STEP5: GENERATE ILITY-DRIVING OPTIONS

This step is concerned with the generation and selection of options that can be added to architecture alternatives to achieve desired ilities. In other words, options at the system level must be developed that will enable the achievement of the ilities identified in step 3. The procedure in this step is the ilities will be grouped together according to common themes and then options in the system to achieve the ilities will be generated.

A. RELIABILITY AND QUALITY

The first grouping of ilities is reliability and quality. They are concerned with how the system is produced, engineered and maintained. Reliability can be measured such as failure rate per year, or mean time to failure. It is the probability that the system will continue to deliver value to the customer over some period of time. Quality is more difficult to measure since it is based upon more subjective criteria. It characterizes the level of superiority and excellence of the system. One criterion used to determine quality of a system is based upon its reliability. Quality can also mean the level to which the system is fabricated to its required standards. In other words, quality can mean that the product is produced in fashion that all the manufacturing requirements such as tolerance are achieved. The baseline concept must include methods for determining the reliability of the SoS and a way to maintain quality.

The concept for achieving quality can be challenging for a SoS that uses existing systems. This is because the quality of the existing systems is not under its control. However, what can be controlled for quality is the fusion of the various systems that make up the SoS. The fusion is enabled through software, interfaces (both hardware and software), and computing hardware. Therefore, these parts of the SoS must be developed and produced using standards to yield a quality product. Furthermore, any systems that are produced under the control, budget, and management of the SoS will be designed and manufactured to the quality levels that are necessary. In these two ways, the SoS can achieve quality.

Achieving reliability in the SoS is also dependent upon the reliability of the existing systems, systems developed under the control of the SoS, and fusion of all sensor data. As with quality, the reliability of new systems and of the fusion hardware/software is under the control of the SoS. Therefore, those items will be developed, managed, and maintained to achieve the required reliability.

B. INTEROPERABILITY AND COMPATIBILITY

Interoperability refers to the ability of the data from constituent systems of the SoS to be fused together so that the required functionality is achieved. Therefore, it refers to connectivity within the SoS. Interoperability is part of the definition of a SoS and will therefore be achieved by definition.

Compatibility is different and refers to the ability of the SoS to function in conjunction with systems outside the SoS such as other drone management systems like the FAA UAS Rule (Part 107) and the FAA Pathfinder program. One concept for how this can function is that detected drones can be checked against the drone flying scheduled in the FAA or local database. A drawback of this approach is that nothing keeps a malicious group from registering a drone, scheduling it for a flight near an airport, and using it for attack on the airport. Nevertheless, as external systems are developed, the SoS must be compatible with them.

C. RESILIENCE, AGILITY, EVOLVABILITY, FLEXIBILITY, ADAPTABILITY

These five ilities all describe the SoS in terms of its ability to change dynamically in response to external factors. The external factors create perturbations to the system as described in Step2. The system must respond to them to maintain value delivery.

Resilience and Agility both refer to how rapidly the system can respond to changes. The nuance of resilience is that it means the system can not only respond quickly, but that the SoS can maintain value delivery during the time it takes to adapt. In other words, the act of adaption of a system to changes rarely occurs instantaneously but instead requires some finite amount of time. During the time of adaption the SoS has the capacity to continue value delivery.

Evolvability and adaptability both refer to the capacity of the SoS to change, reconfigure, or modify. The slight nuance of evolvability is that the changes are external to the system. Adaptability, on the other hand, includes the capacity to change due to internal or external perturbations.

Flexibility is a high level ility which exists above resilience, agility, evolvability, and adaptability. Simply stated it is the capacity of the system to change in reaction to perturbations.

The concept of operation for these change ilities is that the SoS includes the capacity for the individual systems to provide extended functionality when one of the other systems are non-operational or provide are providing reduced functionality. For instance, if the SMR radar is down for repairs or maintenance, then the lower cost radars distributed throughout the airport must provide functionality that maintains value delivery of the SoS. On this approach, the SoS is developed in a fashion that there is overlap between the capabilities of the constituent systems which allows the system respond to change.

D. FUNCTIONALITY

This is the capacity of the SoS to maintain value delivery over the system life cycle by preserving system functions.

VIII. SAI METHOD STEP6: EVALUATE POTENTIAL ALTERNATIVES

This is the modeling of various alternatives (generated in Step 4) in terms of relevant metrics. Example metrics are value (attributes and cost), and ility metrics. For this analysis, each of the individual systems will be considered, then the four options for the SoS will be evaluated.

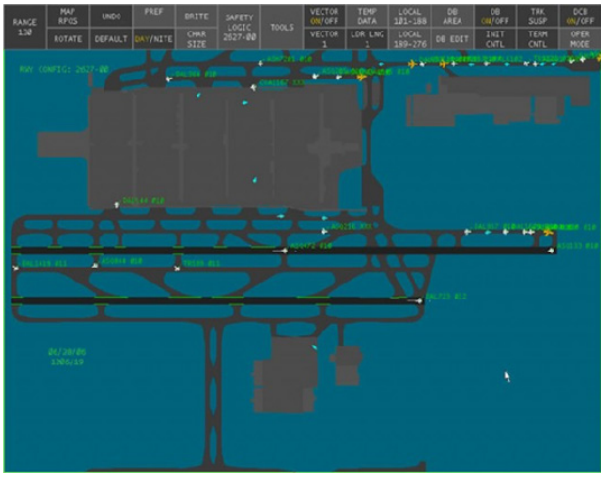

FIGURE 6. ASDE-X system computer display showing ground traffic at Hartsfield-Jackson Atlanta International Airport (public domain image).

A. REVIEW INDIVIDUAL SYSTEMS

1) SURFACE MOVEMENT RADAR

Airport air traffic controllers use SMR to track the movement of aircraft and vehicles on the ground at airports [26]. An example system is the radar that is part of the ASDE-X and its next generation called the SR-3 both sold by Sensis SAAB. The radar is part of a multilateration system that includes sensors and transponders. Fig. 6 shows the computer display from the ASDE-x system. The range of the radar is approximately 12,000 feet, but it operates to an altitude of 200 feet above ground.

The ASDE-X antenna creates a fan beam pattern with a horizontal beam width of 0.35 degree and vertical beam width of 10 degrees. It operates at a frequency of 9.0 to 9.2GHz and the antenna provides 37dB of gain. The antenna is

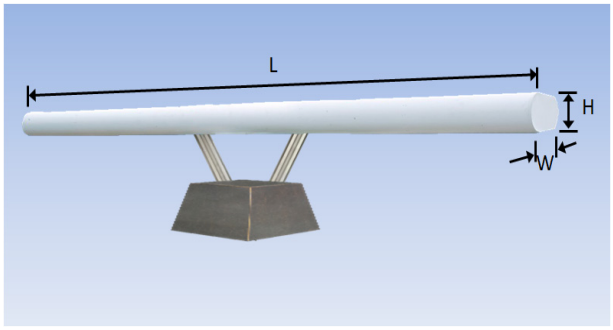

FIGURE 7. Illustration of an antenna type used in the ASDE-X system.

mechanically scanned at a rate of 60Hz and it is approximately 6.5 meters long (L), 1.0 meter wide (W), and 0.5 meters high (H) as shown in Fig. 7.

The ADSE-X radar is intended to detect rather large targets with radar cross section in the range of 0.5 m^2 (-3dBsm) at a range of approximately 4-5 km with guaranteed performance during rain fade conditions.

2) LOW COST SHORT RANGE RADAR

Typical systems are based upon FMCW radar, but some may be pulsed Doppler. An example is the A2000 from Spotter RF which is specifically designed for the detection of drones and provides detection up to 1.0 km [27]. It is small at approximate 0.25 m square and 6.6 cm thick.

One alternative is to distribute Low Cost Short Range Radars in the coverage area which is an approach taken in [28]. The system uses optical fiber links between the radar transmitter and receiver which reduces leakage, distortion, and propagation losses. The demonstration showed that it was possible to link distributed radars with fiber optics. A similar approach was taken in [29] which used multiple receivers to create a multistatic radar for the purpose of detecting drones. These examples demonstrate the usefulness of distributing multiple radars for drone detection.

3) VIDEO SURVEILLANCE (VISUAL IMAGING)

Visual imaging can be used for detection of drones. There are multiple variations of optical cameras such as fixed cameras, pan tilt zoom (PZT), and wide band cameras. An example of a camera system that offers 180 degree imaging at 30 frames per second is the MEGApix PANO 48MP Camera from Digital Watchdog. One of the benefits of this system is that it provides continuous camera coverage of large areas which is an advantage over PZT cameras which must rotate to from one sector to another. Also, with two MEGApix units installed, this system is able to deliver 96 mega pixels of video for continuous coverage over 360 degree.

4) RADAR SENSORS AT MILLIMETER-WAVE (mmWAVE) FREQUENCIES

Millimeter-wave radar sensors have several attractive benefits. First, the bandwidth available is much greater than for microwave and lower frequency radars. This is important

since a wide band waveform can be use to obtain additional target information. Second, the antennas can be small for the same gain and beam width. This is a benefit for installation since the antennas will be lighter and will be more aesthetically appealing at the airport. Third, small UAVs are a larger portion of a wavelength or multiple wavelengths in dimension so that they will scatter more energy. These benefits make mmWave radars an attractive option.

However, they do have some drawbacks. First, components and subsystems are more expensive at mmWave frequencies. This situation is starting to change due to the explosion of high data rate back haul and satellite systems which use components in the 20-80GHz range. Nevertheless, mmWave radars are more expensive. Second, it is more challenging to generate high power levels at these frequencies. This is another reason that high power radars can be expensive at mmWave. Third, atmospheric attenuation is higher in these frequency bands. As a result more of the signal is absorbed by the atmosphere than at lower frequencies. Although these are important drawbacks, the benefits of mmWave radars make the an attractive option for drone detection.

An example system is described in [30] which describes a 35GHz FMCW system designed for drone detection. The systems were analyzed for velocity detection in the range of 15 to 37.5 m/s. The presented measured results were for short ranges (<100m), but the result does demonstrate the usefulness of mmWave radar for drone detection.

5) LIDAR

This is a combination of the words light and radar. The idea behind this technology is that light energy can be used in the same way as radio wave. Since the wavelength of light is so small, it can create high resolution images. Fig. 8 shows a LIDAR image of the Marching Bear Mound Group in Iowa.

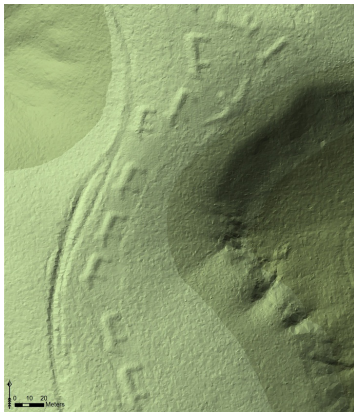

FIGURE 8. LIDAR image of the Marching Bear Mound Group in Iowa (public domain image).

The idea behind using LIDAR is that it is a possible sensor to provide high resolution images for the detection of drones. Low cost LIDAR sensors are being developed. For instance, LeddarTech (http://leddartech.com/) is developing low cost LIDAR systems for use on drones and other application. Their goal is to use their LIDAR sensors for autonomous vehicles. However, this same technology can be used to detect drones. Also, low cost LIDARs are being developed by Infineon for use in self driving cars through the acquisition of LidarExpertise located in the Netherlands [31]. Though the present cost of LIDAR systems may make them a challenge for low cost drone detection systems, the cost is expected to be reduced significantly in the near future.

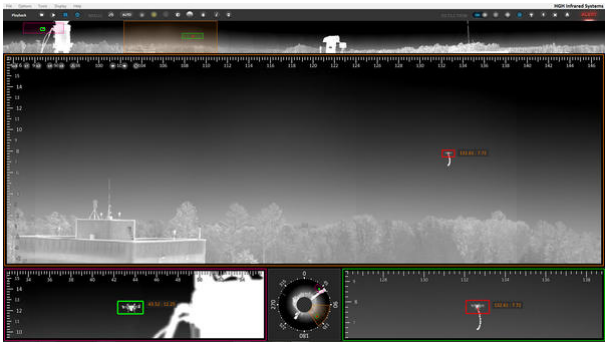

FIGURE 9. Infrared camera image of a drone taken using the Cyclope system from HGH Infrared (http://www.hghinfrared. com/News/Press/Eyes-on-the-Horizon).

6) INFRARED CAMERAS

These cameras have the ability to detect targets at night and use radiation from target in the infrared spectrum. An example system is the infrared sensors from HGH Infrared Systems (http://www.hgh-infrared.com/) with an image of their Cyclope systems tracking a drone in Fig. 9. Their cameras can detect drone sized target to several km. Their system can cover a 360 degrees field of view. In addition, signal processing has been developed for the simultaneous detection and tracking of targets.

7) HUMAN OBSERVATION (AIRPORT PERSONNEL AND AIR TRAFFIC CONTROLLERS)

Human observers can be used to perform rapid assessment and classification of potential drone targets. A benefit is that this resource already exists at the airports. A drawback is that human observation can is unpredictable and not always accurate.

8) AUDIO SENSORS

Audio sensors have the potential of detecting drones. One of the concerns is that airports are noisy environments so the effectiveness of audio sensors is questionable. An advanced development effort may be necessary to assess their effectiveness.

B. EVALUATE ALTERNATIVE SoS OPTIONS

With a better understanding of the individual systems, it is possible to evaluate the SoS alternatives. Table 6 shows the four options previously identified. A benefit of Option 1 is that it uses only systems that already exist. This is important since it means that the SoS can be deployed without development of any new systems. The focus of the SoS development will then be on interconnection and integration of the outputs

TABLE 6. SoS Options With benefits and drawbacks.

Option Name	Systems	Benefits	Drawbacks
Option1	• SMR (Such as ASDE-X) • Visual Imaging • Human Observation	• All Existing Systems • Lower Deployment Cost	• Limited radar altitude coverage • Limited SoS Redundancy
Option 2	• SMR (Such as ASDE-X) • Low Cost Short Range Radar • Visual Imaging • mmWave Radar	• Improved Detection Probability • Large Coverage Area • Improved Altitude Coverage	• mmWave Radar Is Expensive • Requires Two New Systems
Option 3	• SMR (Such as ASDE-X) • Visual Imaging • Human Observation • Low Cost Short Range Radar	• Improved Detection Probability • Large Coverage Area • Improved Altitude Coverage • Ease Of Integration (only one new system)	• Less SoS Redundancy Since Only One New System • Requires One New System
Option 4	• SMR (Such as ASDE-X) • Visual Imaging • Human Observation • Low Cost Short Range Radar • InfraRed Sensor	• Improved Nighttime Detection • High SoS Redundancy	• Requires Two New Systems • Integration Is More Complex

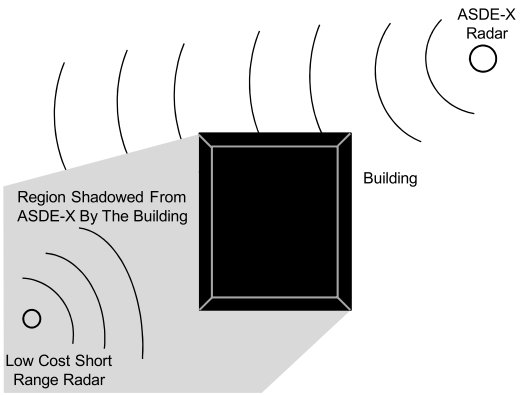

FIGURE 10. The ASDE-X radar provides coverage to several km, but its radar signal can be shadowed by airport buildings and structures (which is true for all radars). Low cost and short range radars can operate in those areas to improve the coverage area.

from the sensors, analysis of the results, operation system, and associated management and maintenance.

One of the concerns for the concept of operations of Option 1 is that the SMR will have shadow areas in the airport due to buildings and other airport infrastructure. This is illustrated in Fig. 10. If this occurs, then the drone can fly in a path behind the building and avoid detection by the ASDE-X system. This is because the SMR signal is scattered by the building anything in the shadowed area will not be detected.

Options 2-4 overcome this limitation by using low cost short range radar as illustrated in the figure. An approach to overcome this limitation is for the low cost short range radar to be placed in the shadow areas of the airport as shown in the figure. This will allow for increased detection of drones. Furthermore, if the data from ASDE-X radar is unavailable, the SoS can still deliver value by detecting drones using the the low cost short range radars. Furthermore, the altitude of detection for the low cost short range radar can be much higher (up to 500m-2km) than the 200 feet specified for the ASDE-X system.

The mmWave radar as part of Option 2 is also a back-up system and provides detection that the SMR radar cannot. The concept of operation is the mmW radar can operate if the data output from the ASDE-X is unavailable for whatever reason such as maintenance or data interruptions. Also, the shorter wavelength of the mmW radar means that it has the potential to detect smaller drones since the drone will be larger compared to the operating wavelength.

A drawback of Option 2 is that it requires two new systems to be deployed beyond the already existing ones. This requires development funds for the prototype development and increases the recurring cost of each system deployed. It also means that there is more sensor information being generated that needs to be connected, analyzed, and used. This adds more complication to the system compared to Option 1 and Option 3.

Option 3 also has the benefit of the low cost short range radar to enhance drone detection coverage compared to Option 1. However, it does not include the mmWave radar which reduces functionality compared to Option 2. One obvious benefit is the reduced prototype development and lower recurring cost compared to Option 2 since the human observers used in Option 3 are already existing. Theoretically, additional training and reporting of findings is required. Therefore, Option 3 can be considered a compromise of cost and functionality between Options 1 and 2.

Option 4 has the benefits of Option 3, but with the addition of an infrared sensor. The concept of operations for the infrared sensor is it's an enhancement to the optical sensors. They provide the ability to extend optical sensing into night time and to detect the heat generated by the motor, battery, and electronics in the drone. This provides an additional layer of functionality and capability to the system.

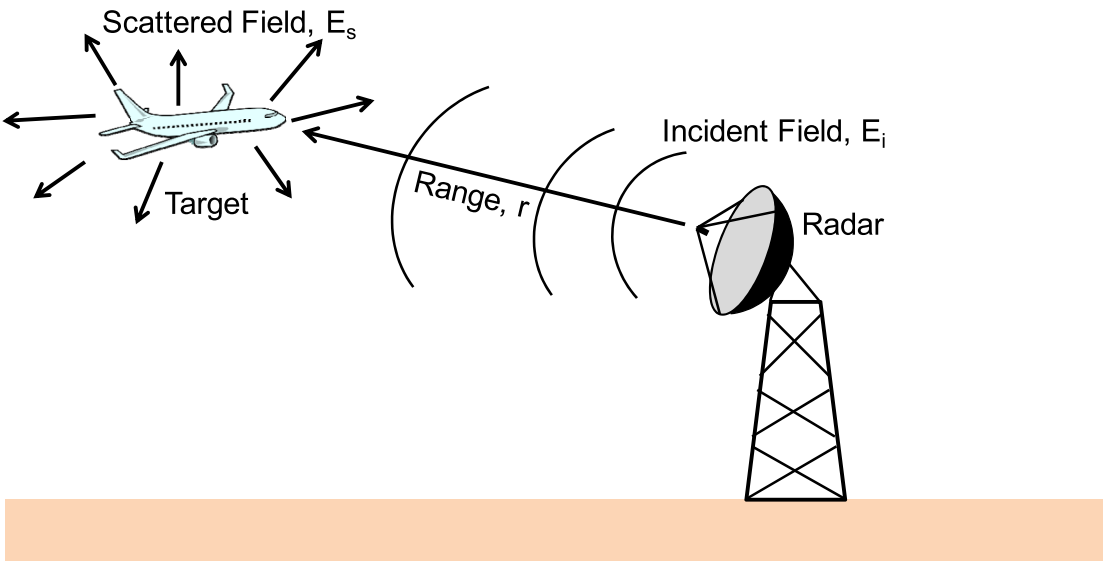

FIGURE 11. The radar transmits an incident electric field (Ei) toward the target at a range (r) which causes a scattered field (Es) off the target.

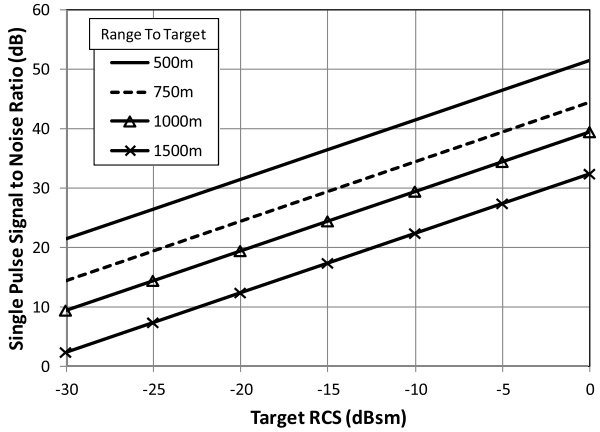

FIGURE 12. Calculated single pulse signal to noise ratio as a function of target RCS and range to the target.

IX. SAI METHOD STEP7: ANALYZE ARCHITECTURE ALTERNATIVES

This is the deep analysis of data generated in Step 6 for the purpose of developing understandings of the possible trade-offs that exist with the alternative SoS architectures.

A. RADAR DRONE DETECTION AND THE RCS CONCERN

One of the concerns for detecting drones using radar is their small radar cross section (RCS) and this is a concern for all four options. This is because radar cross section is dependent upon the size, material, shape, and movement of the target. Smaller targets have a smaller RCS and are more difficult to detect. Targets fabricated of mostly metal have larger RCS while plastic targets have a smaller RCS. Targets with smooth edges and rounded corners have a lower RCS. The fundamental reason for these characteristics of targets is that RCS is due to the reflection of the radar signal off the target. Given as an equation, RCS in dimensions of area is given by

$$RCS = \underset{r\to\infty}{LIM}\left(4\pi r^2 \frac{|E_s|^2}{|E_i|^2}\right) \tag{2}$$

Where E_s is the scattered field off the target, E_i is the incident field from the radar, and r is the range from the radar to the target as illustrated in Fig. 11. Often, the RCS of targets is given in log format which is calculated as with units of dBsm (decibels square meter) with RCS is given in square meters.

The RCS of drone targets has been investigated by several workers. For instance, in [32] small consumer drones are measured in an antenna chamber at 12-15GHz and at 3-6GHz. The results show that the RCS varies from approximately -3 to −24dBsm depending upon the drone type, orientation of the drone, and frequency. The results also showed that there was approximately a 10dB increase in RCS at 12-15 GHz compared to 3-6GHz operating frequency.

Another investigation into drone detection in [33] used both simulation and measurement to determine the RCS of micro-drones and specifically the effect of blade rotation on RCS. The work examined RCS as a function of radar signal polarization, frequency, and drone blade movement. They showed that the RCS of just the blade on a drone varies by 30-50dB depending upon the polarization of the transmit and receive radar signal and the frequency of operation

B. DRONE DETECTION AND THE RADAR EQUATION

Using the measured RCS numbers from [32], it is possible to calculate the signal to noise ratio for a low cost microwave radar. The calculations use the radar equation which is given by:

$$\mathrm{SNR} = \frac{\mathrm{P_r G_p}}{\mathrm{k_B T_s B_n}} = \frac{\mathrm{P_t G_t}\sigma\lambda^2}{(4\pi)^3 \mathrm{R}^4}\frac{G_p}{\mathrm{k_B T_s B_n}} \tag{3}$$

Criteria	Option 1	Option 2	Option 3	Option 4
Reliability	5	3	3	1
Quality	1	3	3	3
Interoperability	5	3	3	3
Compatibility	5	3	3	1
Resilience	1	5	3	5
Agility	1	5	3	5
Evolvability	1	3	3	3
Flexibility	1	5	3	5
Adaptability	1	5	3	5
Functionality	1	5	3	5

Key
5 = High
3 = Medium
1 = Low

Descriptions Of Options
Option 1
SMR (such as ASDE-X)
Visual Imaging
Human Observation
Option 2
SMR (such as ASDE-X)
Low Cost Short Range Radar
Visual Imaging
mmWave Radar
Option 3
SMR (such as ASDE-X)
Visual Imaging
Human Observation
Low Cost Short Range Radar
Option 4
SMR (such as ASDE-X)
Visual Imaging
Human Observation
Low Cost Short Range Radar
InfraRed

		Option 1		Option 2		Option 3		Option 4	
Criteria	Weighting	Value (v_k)	Score ($w_k \cdot v_k$)	Value (v_k)	Score ($w_k \cdot v_k$)	Value (v_k)	Score ($w_k \cdot v_k$)	Value (v_k)	Score ($w_k \cdot v_k$)
Reliability	2	5	10	3	6	3	6	1	2
Quality	2	1	2	3	6	3	6	3	6
Interoperability	3	5	15	3	9	3	9	3	9
Compatibility	3	5	15	3	9	3	9	1	3
Resilience	1	1	1	5	5	3	3	5	5
Agility	1	1	1	5	5	3	3	5	5
Evolvability	1	1	1	3	3	3	3	3	3
Flexibility	1	1	1	5	5	3	3	5	5
Adaptability	1	1	1	5	5	3	3	5	5
Functionality	3	1	3	5	15	3	9	5	15
	18		50		68		54		58

FIGURE 13. The QFD decision matrix for choosing the SoS option as the baseline.

Where:

P_r = received power (W)
P_t = transmit power (W)
G_r = gain of receive antenna
G_t = gain of transmit antenna
σ = radar cross section of the target (dBsm)
λ = wavelength of operation (m)
R = range to target (m)
G_p = processing gain (such as pulse compression gain)
k_B = Boltzmann's constant = $1.38 \times 10 - 23$ (Joules/K)
T_s = total noise (background and system noise)
B_n = receiver bandwidth (Hz)

The SNR for a short range drone detection radar was calculated. The calculations assume an operating frequency of 9GHz, a peak output power of 1000 W, antenna gain of 30dB on transmit and receive, a noise figure of 2dB, and 0dB of processing gain. The results are shown in Fig. 12 for a range of drone RCS from −30 to 0 dBsm.

From this analysis, if the minimum signal to noise ratio for reliable detection is taken to be 13.4 dB [34], [35] to achieve a probability of detection of 95% and a probability of false alarm of 10-6, then for the design described, it is possible to detect drones with an RCS of at least −25 dBsm to a maximum range of 1 km.

X. SAI METHOD STEP8: TRADE OFF AND SELECT BEST ARCHITECTURE WITH ILITIES

This step uses the analysis results from Step 7 and a quality function deployment (QFD) method based on ilities decisions about the preferred architecture. The output from this final step is the baseline solution that will be carried forward into the next phases of the system lifecycle such as advanced development, detailed design, etc.

The approach in this section is a modification to the SAI since it uses ilities in a QFD to choose the best SoS option. The approach is based upon work in [20] which used a QFD style decision matrix with ilities as the criteria. The same approach is taken here were the SoS ilities are used as the criteria for choosing the SoS option.

Each of the criteria is given a weighting, W_k, which is related to its importance to the mission of the system. Each of the energy generation options is assigned a value, V_k, for its ability to achieve each of the criteria. If this is done, then the score for each option is given by:

$$Score = \sum_{k=1}^{n} W_k V_k \tag{4}$$

Where n = the number of criteria which is seven in our case. The trade study was implemented in a spread sheet and is shown in Fig. 13.

Based upon the QFD matrix, the baseline solution should be Option 2 which is the SMR + Low Cost Short Range Radar + Visual Imaging + mmWave Radar option with a score of 68.

The next highest rated is Option 4 with a score of 58 and there are two primary reasons that it received a lower score. First, it will have lower reliability than the other options since there are more systems in the SoS. True enough that the increased number of systems means that the SoS will continue to deliver value if one is unavailable. However, the resilience of the system takes this capability into account.

FIGURE 14. Image of (a) police officer with hand held drone thwarting weapon, and (b) close up of the unit (Image courtesy of Icarus Technologies, Inc.).

Reliability, in this case, is measure of the full SoS and the likelihood of one system being unavailable increases as the number of systems increases. Second, is the compatibility of the systems that comprise the SoS is lower as the number of systems increases. Since Option 4 contains the largest number of systems, it received a lower compatibility rating. For these reasons, Option 4 was rated as second.

XI. DRONE THWARTING

Drone thwarting is the action taken to eliminate the threat posed by a particular drone. There are many different alternatives for stopping drones [36] and a few of them are:

- Attach Of Drone Ground Control: Use of Signal Intelligence (SIGINT) may be useful to pinpoint the location of the drone ground operations.
- Drone Signal Jamming: Jamming of the UAV's ground to air or GPS guidance and control.
- Drone Killing Drone: Launching another drone which tracks and kills the drone.
- Drone Killing Small Missiles: Small but highly accurate munitions.

An example system thwarts drones is the Icarus Hunter$^{(tm)}$ which is shown in Fig. 14 [37]. It is a commercially available hand-held radio-frequency counter-drone effector that senses the transmissions of drones and their operators, and then disrupts the communications links used for command and control. The unit looks like a compact machine gun. According to the manufacturer, the unit is 6 lbs. and compatible with security/tactical gear. It is rated for 60+ minutes of ''active disruption'' and several days of ''passive detection'' using commercial batteries. Though the system is capable of GPS based attack on drones, operation in that mode requires approval from the federal government (such as the Federal Communications Commission). As an example of its usefulness, the manufacturer said that their units have been deployed to protect against drone attacks.

Airport security personnel could be outfitted with these types of units which can be used to bring down unauthorized drones that enter the airport air space.

XII. CONCLUSIONS

Drones pose a serious threat to military and civilian targets. They can be used to carry explosives which can be delivered by the drone with high precision to targets such as bridges, public events with high population concentration, nuclear power plants, schools, and hospitals. The focus of this work is on the development of a concept for the detection of drones used to attach airports.

Specifically, this work describes the baseline concept for a SoS solution to airport protection from drone attack. The system concept was developed by following the SAI method. Its eight steps terminate in a QFD trade study that is used to choose the baseline among several options.

The baseline concept development for a system such as this is a complicated process and much more work can and should be done. For instance, if standard system development methods are followed, after the baseline concept is developed, then advanced development efforts will follow. Important advanced development efforts will include testing of the SMR radar to ensure its drone detection capabilities. Also, several options for the Low Cost Short Range Radar should be evaluated to determine if a customer system needs to be developed.

Possibly the most important advanced development effort for this project is a proof of concept for the integration of the sensor outputs. One option may be to use the ASDE-X system user terminal or a variant of it to display detected drones.

Another benefit of this work is it provides an example of using the SAI method for SoS development.

REFERENCES

[1] Bolton. (2015). *Man Arrested for Landing "Radioactive" Drone on Japanese Prime Minister's Roof*, accessed on Nov. 21, 2015. [Online]. Available: http://www.independent.co.uk/news/world/asia/man-arrested-for-landing-radioactive-drone-on-japanese-prime-ministers-roof-10203517.html

[2] Spiegel Online. (2013). *German Police Shoot Down Model Plane Terror Plot*, accessed on Nov. 21, 2015. [Online]. Available: http://www.spiegel.de/international/germany/german-police-suspect-remote-controlled-airplane-terror-plot-a-907756.html

[3] G. Mcdonald. (2015). *Drone Swarm! 50 UAVs Controlled by One Pilot*, accessed on Oct. 15, 2015. [Online]. Available: http://news.discovery.com/tech/robotics/drone-swarm-50-uavs-controlled-by-one-pilot

[4] *UAS Sightings Report*, accessed on Jan. 15, 2017. [Online]. Available: https://www.faa.gov/uas/resources/uas_sightings_report/

[5] *FAA Expands Drone Detection Pathfinder Initiative*, accessed on Jan. 15, 2017. [Online]. Available: https://www.faa.gov/news/updates/?newsId=85532

[6] M. Nijim and N. Mantrawadi, "Drone classification and identification system by phenome analysis using data mining techniques," in *Proc. IEEE Symp. Technol. Homeland Secur.*, May 2016, pp. 1–5.

[7] J. Mezei, V. Flaska, and A. Molnar, "Drone sound detection," in *Proc. IEEE Int. Symp. Comput. Intell. Inf.*, Nov. 2015, pp. 333–338.

[8] J. Mezei and A. Molnar, "Drone sound detection by correlation," in *Proc. IEEE Int. Symp. Appl. Comput. Intell. Inf.*, May 2016, pp. 509–518.

[9] A. Rozantsev, V. Lepetit, and P. Fua, "Detecting flying objects using a single moving camera," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 39, no. 5, pp. 879–892, May 2016.

[10] S. K. Boddu, M. McCartney, O. Ceccopieri, and R. L. Williams, "A collaborative smartphone sensing platform for detecting and tracking hostile drones," in *Proc. SPIE 8742, Ground/Air Multisensor Interoper., Integr., Netw. Persistent ISR IV*, May 2013.

[11] J. Drozdowicz *et. al.*, "35 GHz FMCW drone detection system," in *Proc. Int. Radar Symp.*, May 2016, pp. 1–4.

[12] M. Jahangir and C. Baker, "Robust detection of micro-UAS drones with L-band 3-D holographic radar," in *Proc. Sensor Signal Process. Defense Conf.*, Sep. 2016, pp. 1–5.
[13] S. R. Ganti and Y. Kim, "Implementation of detection and tracking mechanism for small UAS," in *Proc. Int. Conf. Unmanned Aircraft Syst.*, Jun. 2016, pp. 1254–1260.
[14] G. C. Birch, J. C. Griffin, and M. K. Erdman, "UAS detection classification and neutralization: Market survey," Sandia Nat. Lab., Albuquerque, NM, USA, Tech. Rep. SAND2015-6365, 2015.
[15] *(R2002) IEEE Standard Glossary of Software Engineering Terminology*, IEEE Standard 610.12-1990, Feb. 1983.
[16] *ISO/IEC/IEEE International Standard, Systems and Software Engineering-Vocabulary*, 1st ed. IEEE Standard 12-15-2010, Dec. 2011.
[17] C. H. Dagli and N. Kilicay-Ergin, "Systems of systems architecting," in *Chapter 4 in System of Systems Engineering*, M. Jamshidi, ed. Hoboken, NJ, USA: Wiley, 2009, p. 77.
[18] A. Kossiakoff, W. N. Sweet, S. J. Seymour, and S. M. Biemer, *Systems Engineering Principles and Practice* Hoboken, NJ, USA: Wiley, 2011.
[19] N. Ricci, M. E. Fitzgerald, A. M. Ross, and D. H. Rhodes, "Architecting systems of systems with ilities: An overview of the SAI method," *Proc. Comput. Sci.*, vol. 28, pp. 322–331, Jan. 2014.
[20] S. Corpino and F. Nichele, "An ilities-driven methodology for the analysis of gaps of stakeholders needs in space systems conceptual design," *IEEE Syst. J.*, to be published.
[21] *Airport Infrastructure Security Towards Global Security: A Holistic Security Risk Management Approach, Thales Group Report*, accessed on Dec. 17, 2016. [Online]. Available: https://www.thalesgroup.com/sites/default/files/asset/document/Thales%20WP_Airport%20Security%20Risk%20Management_HR_January08.pdf
[22] *SAAB Sensis*, accessed on Jan. 15, 2017. [Online]. Available: http://saab.com/saab-sensis/
[23] *Airport Surface Detection Equipment, Model X (ASDE-X)*, accessed on Jan. 15, 2017. [Online]. Available: https://www.faa.gov/air_traffic/technology/asde-x
[24] J. Drozdowicz *et. al.*, "35 GHz FMCW drone detection system," in *Proc. Int. Radar Symp.*, vol. 10. May 2016, pp. 1–4.
[25] *Unmanned Aircraft Systems (UAS)*, Int. Civil Aviation Org., Montreal, QC, Canada, 2011.
[26] E. Perl, "Review of airport surface movement radar technology," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 21, no. 10, pp. 24–27, Oct. 2006.
[27] [Online]. Available: https://spotterrf.com/commercial-products/spotterrf-radars/a2000/
[28] D. H. Shin, D.-H. Jung, D.-C. Kim, J.-W. Ham, and S.-O. Park, "A distributed FMCW radar system based on fiber-optic links for small drone detection," *IEEE Trans. Instrum. Meas.*, vol. 66, no. 2, pp. 340–347, Feb. 2017.
[29] F. Hoffmann, M. Ritchie, F. Fioranelli, A. Charlish, and H. Griffiths, "Micro-Doppler based detection and tracking of UAVs with multistatic radar," in *Proc. IEEE Radar Conf.*, May 2016, pp. 1–6.
[30] J. Drozdowicz *et al.*, "35 GHz FMCW drone detection system," in *Proc. Int. Radar Symp.*, May 2016, pp. 1–4.
[31] C. Hammerschmidt, "Infineon acquires lidarexpertise through innoluce takeover," in *Proc. EETimes*, Oct. 2016. [Online]. Available: http://www.eetimes.com/document.asp?doc_id=1330613
[32] C. J. Li and H. Ling, "An investigation on the radar signatures of small consumer drones," *IEEE Antennas Wireless Propag. Lett.*, vol. 16, pp. 649–652, Jul. 2016.
[33] M. Ritchie, F. Fioranelli, H. Griffiths, and B. Torvick, "Micro-drone RCS analysis," in *Proc. IEEE Radar Conf.*, Oct. 2015, pp. 452–456.
[34] G. L. Charvat, *Small and Short-Range Radar Systems*. Roca Baton, FL, USA: CRC Press, 2014, p. 32.
[35] M. I. Skolnic, *Introduction to Radar Systems*. New York, NY, USA: McGraw-Hill, 1962, p. 34.
[36] D. B. Mirkarimi and C. Pericak, "Countering the tactical UAV threat," in *Proc. AMOR*, Jan. 2003, pp. 43–44.
[37] *ICARUS Hunter is a Trademark*, ICARUS Technol., Signal Hill, CA, USA, 2016.

RICK L. STURDIVANT (M'97) received the B.A. degree in religion from Vanguard University in 1986, the B.S. degree in electrical engineering from California State University at Long Beach in 1989, the M.S. degree in electrical engineering from the University of California at Los Angeles in 1992, and the Ph.D. in systems engineering from Colorado State University, Fort Collins, CO, in 2017.

He is currently an Assistant Professor with Azusa Pacific University and Founder of MPT, Inc. He has co-authored the books *Transmit/Receive Modules for Communication and Radar Systems* (Norwood, MA: Artech House, 2015), and *Microwave and Millimeter-Wave Electronic Packaging* (Norwood, MA: Artech House, 2013). He serves on the IEEE MTT-12 Technical Subcommittee on Microwave and Millimeter-Wave Packaging and Manufacturing.

EDWIN K. P. CHONG (F'04) received the B.E. degree (Hons.) from the University of Adelaide, South Australia, in 1987, and the M.A. and Ph.D. degrees in 1989 and 1991, respectively, both from Princeton University, where he held an IBM Fellowship. He joined the School of Electrical and Computer Engineering at Purdue University in 1991, where he was named a University Faculty Scholar in 1999. Since 2001, he has been a Professor of Electrical and Computer Engineering and Professor of Mathematics with Colorado State University. He has co-authored the best-selling book *An Introduction to Optimization* (4th ed.; Wiley-Interscience, 2013). He received the NSF CAREER Award in 1995 and the ASEE Frederick Emmons Terman Award in 1998. He was a co-recipient of the 2004 Best Paper Award for a paper in the journal *Computer Networks*. In 2010, he received the IEEE Control Systems Society Distinguished Member Award.

Dr. Chong was the Founding Chairman of the IEEE Control Systems Society Technical Committee on Discrete Event Systems, and served as an IEEE Control Systems Society Distinguished Lecturer. He is currently a Senior Editor of the IEEE TRANSACTIONS ON AUTOMATIC CONTROL, and has also served on the Editorial Boards of *Computer Networks*, *Journal of Control Science and Engineering*, and *IEEE Expert*. He served as a member of the IEEE Control Systems Society Board of Governors and as Vice-President for Financial Activities until 2014; he currently serves as President-Elect. He was the General Chair for the 2011 Joint 50th IEEE Conference on Decision and Control and European Control Conference.