Implications of Cyber Threats for the Design of Unmanned Air Traffic Management System

Vasily Sidorov*, Wee Keong Ng†, Kwok Yan Lam‡, Mohamed Faisal Bin Mohamed Salleh§
*†‡School of Computer Science and Engineering, §Air Traffic Management Research Institute
Nanyang Technological University
Singapore
Email: *vsidorov@ntu.edu.sg, †awkng@ntu.edu.sg, ‡kwokyan.lam@ntu.edu.sg, §mohd.faisal@ntu.edu.sg

***Abstract*—Unmanned aircraft are quickly gaining credibility as an efficient tool for a wide range of tasks. With the increase in the amount of UAVs in the sky, the need for the UAV traffic management arises. Unmanned air traffic management system (UTMS), especially in the urban airspace, could be considered as a critical infrastructure, which—if disrupted—can lead to severe monetary losses and even casualties. As a computerized system, UTMS is susceptible to cyber attacks ranging from cyber vandalism to cyber warfare. This work considers cyber threats to the UTMS, and how it should be designed in order to be resilient to these threats. The work was performed as a part of the early design of an urban UTMS in Singapore; however, the findings are applicable to designing UTMS for any urban environment.**

***Index Terms*—unmanned aircraft; cyber security; air traffic management;**

I. Introduction

In creating a UTMS that is resilient to cyber threats, we need to consider cyber resiliency of all components of the UTM eco-system, including remote pilot stations and UAVs, and communication links between all the components. There has been many works on cyber security of specific components of the eco-system, such as UAVs [1] or GNSS positioning [2]. ADS-B, an aircraft position tracking system widely used in aviation, has been a target for cyber security analysis by many researchers, with concerns that aircraft positions could be easily spoofed or corrupted due to lack of authentication and encryption in the ADS-B protocol [3]–[6].

In this work we try to go beyond examining components and links between them for cyber vulnerabilities, especially considering that the UTMS in question is at the early design stages. Instead, we rather try to identify a comprehensive set of design-time issues and decisions that would have a strong impact on cyber security of the resulting system. A UTMS and UTM eco-system design that addresses all of the identified issues will possess inherent cyber resiliency and provide sufficient capabilities for cyber forensics.

This work was done within the first stage of creating a fully operational UTMS for an urban airspace; it reflects and opens for discussion our current findings, with more findings and more practical results to follow in the near future. More details on our analysis of this topic could be found in a full technical report of the first stage of the project [7].

Below we introduce the terminology used in this work:

ADS-B (*Automatic Dependent Surveillance – Broadcast*) is a surveillance technology in which an aircraft determines its position via GNSS and periodically broadcasts it, enabling it to be tracked. The information can be received by air traffic control ground stations in addition to (or in lieu of) secondary radar. It can also be received by other aircraft to provide situational awareness and allow self separation.

ATC (*Air Traffic Control*) A service operated by appropriate authority to promote the safe, orderly, and expeditious flow of air traffic. ICAO explicitly appends to this definition the duty to prevent aircraft–aircraft and aircraft–obstruction collisions [8].

ATM (*Air Traffic Management*) A term encompassing all systems that assist aircraft to depart from an aerodrome, transit airspace, and land at a destination aerodrome, including air traffic control (ATC), air traffic safety electronics personnel (ATSEP), aeronautical meteorology, air navigation systems (aids to navigation), Air Space Management (ASM), Air Traffic Services (ATS), and Air Traffic Flow Management (ATFM), or Air Traffic Flow and Capacity Management (ATFCM).

C2 link (*Command and Control link*) The data link between the remotely piloted aircraft and the remote pilot station for the purposes of managing the flight [9]. C2 link typically supports the following communication tasks:

1) control uplink to UAV: data to modify behavior and state of the UAV;
2) control downlink from UAV: data to indicate the position and status of the UAV;
3) DaA uplink: sensor selection/control and, if applicable, auto response state select (on/off) and override (remote pilot option to cancel the maneuvers);
4) DaA downlink: sensor data and processed sensor information (related to traffic, weather, terrain, airport visual data, etc.), conflict alert and terrain/obstacle alert

This work was supported by Civil Aviation Authority of Singapore.

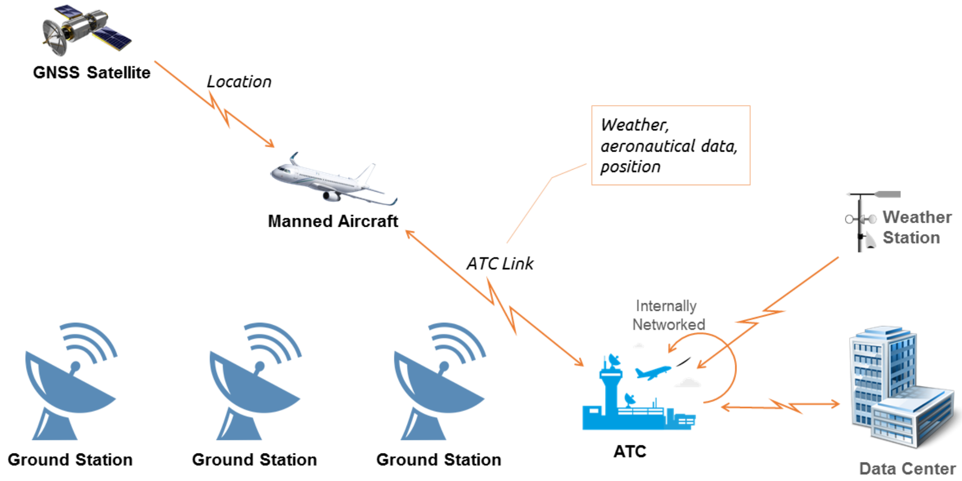

Fig. 1: Topology of a regular ATM

and maneuver advisories (MA) and, if applicable, DaA automatic response (initiation and description), etc.;

5) data to support UAV handover, uplink and downlink;
6) data to support flight data recording requirements, uplink and downlink.

CA (*Collision Avoidance*) A maneuver UAV performs to avoid collision with other UAVs, static objects, or other aerial entities.

DaA (*Detect-and-Avoid*) As defined by ICAO, detect-and-avoid is a set of technologies that provide a capability to see, sense or detect conflicting traffic or other physical hazards and take appropriate actions in order to ensure the safe execution of the flight of an RPA and to fully enable integration of UAVs into the shared airspace.

GNSS (*Global Navigational Satellite System*) A unified term for all of the global navigational systems: GPS (USA), GLONASS (Russia), Galileo (EU), BeiDou/COMPASS (China), NAVIC (India).

ICT (*Information-Communication Technology*) This refers to any systems and devices comprising hardware (integrated circuits) and software (computer codes). Most of these systems and devices have a network interface allowing them to connect to the Internet or with other ICT-based systems and devices. Computers, laptops, mobile phones, tablets, wearables, UAVs, etc., are all ICT-based products.

LoWC (*Loss of well clear*) Situation when another object enters the well clear area of ownship. See also: *well clear*.

RPS (*Remote Pilot Station*) A properly equipped location of a remote pilot from where he controls the UAV.

Self-separation An ability of an aircraft to perform *DaA* without guidance from the traffic control center.

UAV (*Unmanned Aerial Vehicle*) An aircraft that operates with no pilot onboard [9]. It could be an RPA or a pre-programmed autonomous aircraft.

UTM (*Unmanned Traffic Management*) A term referring to a specific type of future ATM, which fully and solely controls UAVs. UTM systems (UTMS'es) are supposed to be substantially more autonomous systems compared to typical ATMS'es. *Exempli gratia*, UTMS should not require human interaction to control each and every UAV; however when needed, UTMS should hand control over a specific or a group of UAV to a human operator.

UTMC *or* UTM GCS (*UTM Center* or *Ground Control Station*) A ground facility that hosts the UTMS [10].

Well clear A separation standard for aircraft. Is "non-specific in nature and allows for a pilot's subjective assessment when performing maneuvers for this purpose" [11]. Requires more strict definition for UAV traffic [12]. Some researchers have endeavored to provide an appropriate definition [13], [14].

The rest of the work is organized as follows: section II considers general requirements for a UTMS; section III is dedicated to establishing what is a cyber threat; section IV discusses main implications of the cyber threats for the design of UTMS.

II. Unmanned Air Traffic Management System

To understand the cyber threat surface of UTMS, which is an emerging development in the global arena of UAV traffic management, we need to understand the differences between conventional ATMS that regulates manned aircraft traffic, and UTMS which manages traffic for UAVs in the way they function, communicate, and the way they are designed architecturally. Awareness of these differences provides us with a deeper understanding of the additional challenges inherent to UTMS, and the corresponding additional cyber threat surfaces that need to be protected. We examine these differences in this section.

Here are the general characteristics of manned ATM operation (see Fig. 1):

- Manned aircraft's position is tracked by GNSS satellite.
- ATC maintains duplex ATC link with manned aircraft.
- ATC has air traffic controllers working on computer terminals running traffic control software (ATMS) and communicating with pilots aboard aircrafts.
- ATMS receives weather information from weather stations and communicates (via 802.1x link) with external ICT systems in the airport.

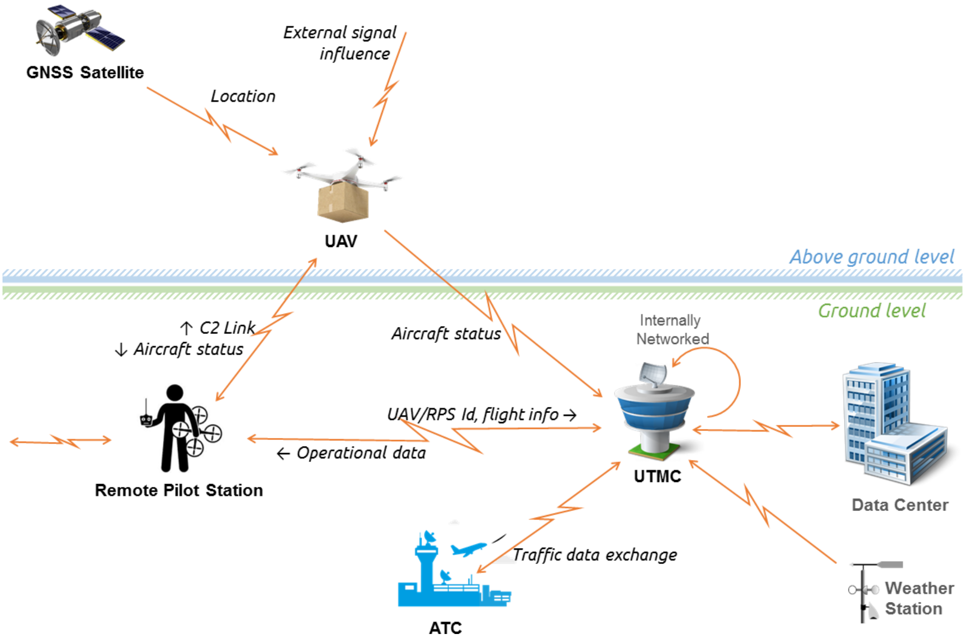

Fig. 2: General topology of a UTMS

Where UAVs are concerned, the communication architecture (in different variations) for UTM may be conceptualized as shown in Fig. 2:

- UAV receives location data from a GNSS satellite.
- RPS controls the UAV via C2 radio link.
- UAV status information is relayed to RPS and UTMC via radio link.
- UTMC and RPS maintain a duplex communication link.
- UTMC has air traffic controllers working on computer terminals running traffic control software (UTMS) and communicating with pilots *not* aboard aircrafts.

The most distinct difference is that UTMC communicates with the remote pilot in RPS on the ground. UTMC does not maintain a link with the UAV; it only passively receives UAV status updates either directly from the UAV itself, or from the RPS.

In addition to remotely piloted UAVs, UTMS should also be ready for more autonomous UAVs in the near future. Increase in autonomy leads to increased complexity, which expands the attack surface. In addition to remotely piloted aircraft, we distinguish three subclasses of autonomous aircraft, in order of increasing autonomy and complexity:

- **Autonomous Navigation**: The aircraft during flight is able to navigate its way to the next waypoint given by the RP.
- **Autonomous Flight**: The aircraft has an automated control system that controls the *take-off*, *flight*, and *landing* phases of the flight. The aircraft is able to perform a full flight after it is given its destination. The aircraft is also able to include automatic negotiation of the flight plan with the UTMS.
- **Autonomous Operation**: The aircraft has an automated control systems that controls all phases of the flight: *pre-flight*, *take-off*, *flight*, *landing*, *after-flight*. The aircraft knows the purpose of its operation and is able to decide when to take off, what route to take, and when and where to land. The aircraft exchanges messages and cooperates with other autonomous aircraft and with the UTMS.

III. Cyber Threats

To understand cyber threats, it is necessary to first define what a cyber threat is, and what should and should not be considered as a cyber threat. In this chapter, we want to give a concrete definition as well as examples of what a cyber threat is.

The notion of a cyber threat has many definitions. One of the more widely used definitions is the one given by ISO 27005:

> *A **cyber threat** is a potential cause of an incident, that may result in harm of systems and organization* [15].

A more comprehensive definition, tied to an information assurance point of view, can be found in "Federal Information Processing Standards (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems" by the U.S. National Institute of Standards and Technology (NIST):

> *A **cyber threat** is any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. It is also the potential for a threat-source to successfully exploit a particular information system vulnerability* [16].

In the context of this work on air traffic management, we derive a more targeted definition of cyber threats:

A ***cyber threat*** *is a potential cause of an incident that may adversely*

- *impact the provisioning of safe and stable unmanned air traffic*;
- *affect data assets, including aircraft data* (*IDs, status data*), *air traffic data* (*past, current and planned flights, air traffic surveillance, meteorological data*), *pilot data* (*pilot IDs, station IDs, UTMS–pilot communications*);
- *affect information systems in UTMS, physical assets, or individuals*;

via cyber means and mechanisms such as network intrusion; unauthorized access; destruction, disclosure, and/or modification of assets; denial of service; etc.

It is important to note that in this definition, the emphasis is on the means of delivery of the threats, and the artifacts affected. For a threat to be considered cyber, at least one of them must be of cyber nature. The cause of the threat may not necessarily be cyber. For example, a fallen tree that incapacitates over-the-air communications should be considered a cyber threat even though the reason is purely physical: it affects one of the information system assets in use. On the other hand, a completely non-physical entity such as a computer virus is also a cyber threat.

IV. Implications

Before we go into more complex implications for the design of the UTM eco-system, we would like to list several simple rules that a required to even discuss cyber security of the system.

1) Each UAV must have a unique ID that can be authenticated by the remote pilot and by the UTMS.
2) Each remote pilot (RP) must have a unique ID that can be authenticated by the UTMS. One RP may be controlling more than one UAV.
3) A remote pilot station (RPS) must have a unique ID that can be authenticated by the UTMS. An RPS may host more than one RP.
4) UAVs must be built with mechanisms to support law enforcement operations (e.g., safely bringing down a UAV for inspection).

The requirements of IDs is an implication of a ground rule that any entity in a cyber-resilient system must be identifiable. This enables informative logs of events in the system, attribution of actions, privilege separation, etc. Generally speaking, it gives fundamental control over cyber security of the system and its components as well as ability to trace the chain of events in case of a cyber security incident.

The amount of cyber threats to UTMS is very high, as it is a large and complex system with a large attack surface, and realization of cyber threats to UTMS leads to, mainly, full or partial disruption of unmanned air traffic. It could affect only certain areas, or certain groups of UAVs, or it could affect the whole eco-system.

This would typically be a result of the more blunt (and therefore more probable) attacks (as well as hardware/software failures), which, if successful, will incapacitate the UTMS and lead to full or partial loss of control over the traffic.

More sophisticated attacks could try and affect the traffic management in a specific way. This could include diverting traffic to/from specific areas, assigning UAVs flight plans that increase probability of collisions with other aircraft or static obstacles, issuing an approved flight plan for smuggler UAVs, lifting geo-fences, masking presence of unauthorized UAVs, and many others.

In order to secure itself from these, the UTMS has to be designed to include infrastructure redundancy, data integrity technologies in place, tightened hardware and software security policies, personnel education, security incident event management systems (SIEM), and detailed security incident response guidelines.

Design of the UTM system involves decisions on the architecture of the system, internal and external communication protocols, software, hardware, as well as requires development of custom hardware, software, and protocols. In particular, development of custom software and hardware requires implementation of proper SDLs[1]. Development of custom protocols requires meticulous cyber security analysis on all stages.

Fundamental points in UTMS design that require careful consideration in connection with cyber security issues include:

- How UAV authentication is performed? UTMS needs to be able to reliably authenticate UAVs (as well as RPs and RPSs) that are in the airspace under control. Can adversaries impersonate legitimate UAVs? Can they prevent authentication of legitimate UAVs?
- Can UTMS detect rogue UAVs? UTMS needs to be able to detect UAVs that are not authenticated, registered with UTMS, or are displaying other kinds of rogue behavior. UTMS therefore needs to have a secondary source of air traffic surveillance, which would enable it to verify traffic information collected directly from UAVs (e.g. through ADS-B) and RPSs. Such secondary sources could be small object radars, low altitude radars, video surveillance, etc.
- What models are used to predict air traffic? Are the models susceptible to adversarial manipulation? Can an adversary find and exploit edge cases of the models?
- Is UTMS software and hardware resilient to cyber threats? Do the critical systems have redundancy? Are security incidents and other activity properly logged? Is the system able to detect intrusion? Is the critical data backed up and are the backups secured?
- Is data secured? UAV flight trajectories could be highly confidential information of businesses that operate the UAVs [17]. Is critical data stored redundantly? Do systems provide data integrity verifiability? Is data verifiably coming from authorized sources? Is the issue of data availability addressed?

[1] Secure Development Lifecycles

- Are there clear procedures in response to security incidents? Are the procedures different for different types of security incidents (e.g., physical tampering, network attack, virus, etc.)? Is personnel familiarized with the procedures? Does the system need a "kill switch" in the event of a massive attack, and if yes, how should it be implemented?

A. Implications of Cyber Threats to C2 Design

Modern UAVs require the guidance from a remote pilot at least to a certain extent. Certain UAVs require more than one RP to operate them [18]. However, the trend is to invert the ratio towards one-RP-many-UAVs [19]. The guidance is delivered from the pilot to the UAV through a C2 (command & control) support infrastructure.

C2 is one of the most seminal components of the UTM ecosystem. Issues with C2 could lead up to complete disruption of the UTM. Apart from full or partial disruption of UTM, one of the major consequences of compromised C2 infrastructure is the unknown or compromised UAVs in the airspace of the city.

Scenario 1. Unknown UAVs: Unknown UAVs may not necessarily have a malicious intent (e.g., an amateur flying a UAV to take aerial photos) but regardless of that they could cause serious damage. Since an unknown UAV does not cooperate with the UTMS and generally could not be expected to cooperate with other UAVs through systems like ADS-B, it could disrupt local UAV traffic and require the UTMS to take actions to divert the cooperative traffic away from the area with the unknown UAVs in the air. Either through malicious intent or not, an unknown UAV could collide with other UAVs in the air and cause them to fall on the ground, which may lead to people injuries and casualties as well as property damage. In addition to that, unknown UAVs could have a wide range of malicious intent including smuggling and terrorist attacks.

Lastly, unknown UAVs could be "ghost" UAVs, which are only present on the UTMS navigation equipment but do not exist in reality. This could be a result of interfering with ADS-B, radars, air traffic surveillance systems; tampering with UTMS hardware or software; result of a software or hardware error; and many other potential reasons.

The UTM regulator must be ready for the event of unknown UAVs. Ecosystem design must include policies on managing traffic in affected areas, steps to isolate (e.g., through dynamic geo-fencing of the area) and neutralize the unknown UAVs, ways to confirm existence of a UAV in the sky (e.g., through secondary traffic surveillance systems) to eliminate false alarms from "ghost" UAVs.

The design of mitigation steps might even employ "cyber weapons" to neutralize the unknown UAVs. As an example, in several countries the protected state objects are equipped with GPS spoofers that broadcast coordinates of an airport. Most of the off-the-shelf UAVs have a database of the world airports in their firmware, and would automatically land if they find themselves in a vicinity of an airport.

Scenario 2. Taken over UAVs: Adversaries could take over a cooperative UAV and transform it into the state of an *unknown UAV* with all or most of the implications discussed above. This mostly depends on cyber resiliency of the C2 link technology in place.

Both the carrier media of the wireless C2 link between the RPSs and UAVs, and the communication protocol could make it easier or harder for adversaries to gain control over the UAV. The regulator should consider carefully which communication technologies to allow, and authentication/authorization capabilities of the communication protocols.

It is also worth keeping in mind that in certain scenarios the regulator might have a need to take over the control of a UAV if that would be deemed necessary, therefore, the C2 communication infrastructure should have the capability for transfer of control from a pilot to the UTMS.

Scenario 3. Influenced UAVs: Lastly, the UAVs that do not behave completely as they are supposed to. This might be a result of defects or tampering with the UAV's hardware or software, interference with the C2 link, external attacks on UAVs sensors, etc. Some examples include partial loss of control over the UAV, slightly or completely inaccurate status reports from the UAV (e.g., position, altitude, speed, sensor readings).

This could lead to erratic behavior of the UAV in the air, failure of detect-and-avoid (DaA) subsystems and consequential collision with other participants of the air traffic or with static objects, entering geo-fenced areas, falling on the ground.

The regulator might consider requiring regular servicing of the UAVs (similar to civilian cars that are subject to regular vehicle inspection), automatic UAV software integrity checks, DaA design mindful of cyber threats, backup C2 channels, tamper-resistant C2 protocols, and many other approaches to alleviate the threat.

Creating a stable and cyber-resilient C2 infrastructure requires, among others, careful consideration of the following topics of importance:

- How is the C2 signal communicated between RPS and UAV? Radio frequency and an overall radio link infrastructure plays a large role in ensuring that the link is stable in the changing environment (e.g., weather), has enough throughput to support large fleets of UAVs in the sky, has acceptable performance metrics such as packet loss rate and latency, is resilient to noise/jamming/data traffic peaks, etc.
- How is C2 data protected? Protocols that are used for C2 should provide cyber security guarantees from ground up, including verifiable integrity, authentication/authorization primitives, optional encryption, optional delivery guarantees, etc.
- What is the procedure for full or partial loss of C2? There should be clear procedures and guidelines on actions that need to be taken in the event of full or partial C2 loss. Guidelines must include actions for pilots as well as actions for traffic management officers. Design might as well include a backup C2 infrastructure that uses different

technology stack and provides if not full replacement, then at least ways to do graceful and safe degradation of UTM.

- What is the control paradigm? Some of the major control paradigms include [19]:
  - **Direct control.** RP sends commands to the UAV, and the UAV is reporting its status to the RP. Can an adversary impersonate the RP and issue C2 messages to the UAV? Can an adversary impersonate the UAV and send forged status updates to the RP?
  - **Management by consent.** UAV performs planning and requests approvals for its decisions from the RP. Can an adversary approve/reject the decision in the RP's stead? Can an adversary influence UAV's decision making?
  - **Management by exception.** UAV performs planning and execution of its plan, the RP is able to intervene and amend the plan. Can an adversary influence UAV's decision making? Can an adversary impersonate the RP and amend the UAV's flight plan?

B. Implications of Cyber Threats to Detect-and-Avoid Design

Ability of a UAV to avoid static or dynamic obstacles is not only a valuable feature that increases the safety of air traffic, but also a requirement by global and local regulations. E.g., Title 14 Code of Federal Regulations, section 91.113 (14CFR91.113, 2004) requires that the operator of an aircraft "sees and avoids" other aircraft. This could not be directly applied to UAVs as the pilot is not onboard and might not have a clear visual on the UAV's immediate surrounding. Therefore, UAVs *must* be equipped with a system that resolves the issue [20]. The system of that kind is called a Detect-and-Avoid (DaA) system.

To be more specific, UAVs must be able to perform *self-separation* (SS), i.e., stay *well clear* of other objects either through choosing the flight path or through performing a *collision avoidance* (CA) maneuver [21]. Some of the important metrics for DaA include statistical probability of a *loss of well clear* (LoWC) situation, frequency of initiating a CA maneuver, amount of DaA traffic alerts issued by UTMS, aggregate time required to recover from the LoWC. There is a multitude of factors that could affect these metrics. The metrics highly depend on whether the UTMS or the pilot are involved in the DaA or the UAV is taking care of that in a fully autonomous way; what kind of DaA equipment is in use by the UAV; what kind of equipment is in use by the pilot; which technique is used to detect LoWC or potential LoWC; reaction time for between the DaA alert and the CA maneuver [22]; and many others.

Implementations of Detect-and-Avoid techniques could be classified into *cooperative* and *uncooperative*. Cooperative techniques are the ones that work in cooperation with other UAVs. ADS-B In is a typical example of a cooperative DaA technique, as it requires UAVs to share their location information with each other.

Uncooperative techniques are the ones that do not rely on external parties and are in full done by the UAV itself. They usually rely on sensors and are divided into *active*, i.e., the ones that issue a sonar-like signal and then read the response profile (radar, laser, IR); and *passive*, i.e., the one that receive external reflected signal (such as a visual sensor).

As it was mentioned above, ADS-B is prone to spoofing attacks, and therefore a DaA system that only relies on ADS-B is vulnerable. Sensors of the UAV could be physically tampered with, could be remotely blinded, or could potentially be deceived.

One of the ways to improve resiliency of the DaA is to use at least two different methods at once. DaA resiliency may also be aided by feeding the UAVs the general air traffic information from the UTMS: established flight routes and flight plans, information on static objects (e.g., buildings), etc.

Issues of the DaA design that are coupled with the cyber security issue include:

- Who is involved in the DaA procedure: is it just the UAV itself, is it UAV and the pilot, or is it UAV, pilot, and UTMS? Including the pilot in the DaA could be necessary in certain cases as not all UAVs might be equipped with sophisticated DaA systems. Involving UTMS in the DaA is likely to reduce the overall amount of LoWC situations and the effect of CA maneuvers on the traffic as a whole; at the same time it is likely to increase the reaction time. From the cyber security point of view, the more agents there are and the more distributed they are, the more careful and resilient design is required to provide quality of service enough to achieve the predefined airspace safety threshold (AST).
- What is the required DaA equipment for a UAV to operate in the urban airspace? Cooperative DaA equipment is yielding better performance but is not always applicable as it requires that all aircraft have it. It also is not applicable to avoiding static obstacles or non-UAV aerial objects.
- If DaA involves the pilot, what are the requirements for DaA equipment in the RPS? Research shows that choice of RPS DaA equipment (e.g., DaA displays) plays a major role in achieving good DaA metrics [21], [22].
- Are UAVs required to have DaA equipment redundancy? I.e., are they required to have at least two sets of DaA equipment that works through different sets of sensors? That would help mitigate the risk of intentful or accidental blinding of the UAV's DaA system but would increase the entry threshold into the airspace.
- Which models are used to determine whether LoWC has or will happen? Different models have their pros and cons. Some models may not be adjusted to certain edge cases; some may be too sensitive and initiate CA maneuvering when it is not required; some may be intrinsically vulnerable and be spoofed or fooled by an adversary [13].
- If a pilot and/or UTMS are involved in the DaA, what is the communication topology? What is the communication protocol? Reliability, resiliency, speed, and integrity of communication is critical to successful DaA procedures.

C. Implications of Cyber Threats to Geo-Fencing Design

A geo-fence is a closed virtual 3-dimesnional shape that separates the airspace into the *inside* and the *outside*. In air traffic management, geo-fences are used to restrict flights in certain areas—either to keep the aircraft within certain area, or to keep them outside certain area. Respectively, geo-fences are called *keep-in* and *keep-out*. Geo-fences do not necessarily include ground objects and could be located at higher altitudes.

Geo-fences could be static and dynamic. Static geo-fences—the ones that either never or very rarely change—could be used to fence off the UAVs from flights around government/military objects, etc. Dynamic geo-fences could be the ones that turn on and off on schedule or the ones that are dynamically created by UTM officers as reaction to certain events.

Geo-fencing cyber-attack vectors include:

- **Denial of UAVs'/pilots' access to geo-fencing information**
  This could be achieved through Denial of Service attacks on communication channels or on geo-fencing information systems, as well as other attack methods.
- **Unauthorized adding/removing/modifying of geo-fences in the UTMS**
  This could be done through exploitation of UTMS vulnerabilities that would allow an attacker to elevate his privileges or impersonate another agent of the system, through direct access to geo-fencing information system, through malicious or negligent employees and ex-employees, and other methods.
- **Affecting UAVs' perception of geo-fences or their position in relation to geo-fences**
  This could be achieved through spoofing GPS signal in the area, impersonating the UTMS to deploy fake updates on geo-fencing to UAVs/pilots, through use of unauthorized geo-fencing beacons (if this geo-fencing technology is in place).

Design issues of a resilient geo-fencing technology includes:

- How geo-fencing information is being delivered to RPs and UAVs? Communication protocols should employ proper authorization/authentication in the UTMS–RPS/UTMS–UAV communication to provide integrity of the information during transmission and ensure that geo-fencing information originates from the UTMS and not from an unauthorized source.
- Is geo-fencing information available when needed? If the communication channel is down or the UTMS is experiencing a DoS situation, RPs/UAVs might not be able to receive the geo-fencing information. UTMS should be DoS attack resilient, communication channels should be capable of high rate data transmission, and possibly have redundancy. Static and scheduled dynamic geo-fence information should probably be distributed to pilots beforehand, and not immediately before flight.
- How are geo-fences described? Generally, a geo-fence is a complex 3-dimesnional shape that must possess certain properties: being a closed shape, not to have self-intersections, etc. If the UTMS or the UAV encounters information about a geo-fence that violates some of these properties, they might enter a state of failure. Data structure that holds geo-fence information should be verifiable for correctness and completeness.
- Are geo-fences respected by UAV first or by RP first? Should the pilot have the ability to trespass a geo-fence in the event of a need, or should the UAV be enforcing geo-fences by overriding RP's input [23], [24]?

V. Conclusion

An important notion of systems engineering is a design approach called "secure by design", meaning that the system has been designed from the ground up to be secure. An emphasis on building security into products counters the all-too-common tendency for security to be an afterthought in development. Addressing existing vulnerabilities and patching security holes as they are found can be a hit-and-miss process and will never be as effective as designing systems to be as secure as possible from the start.

The security by design model contrasts with less rigorous approaches including *security through obscurity*, *security through minority* and *security through obsolescence*, which have proven themselves to be ineffective.

It is important to note that cyber security does not fully comprise technological solutions, and is actually a three-fold notion based on *technology*, *people*, and *processes*. Properly designed and setup technology takes care of all the heavy lifting in ensuring cyber security: encryption, resiliency, fool-proofing, filtering, reducing human factor, etc.

People are considered one of the most influential factors in cyber security. They could knowingly or unknowingly compromise systems, could willfully or by negligence violate protocols, and might not be aware of consequences of their actions from the point of view of cyber security. Therefore, approaches to human resources management and personnel education need to be designed with cyber security in mind.

Lastly, processes are required to ensure *sustainable* cyber security. Internal processes of the organization need to be designed to include technology maintenance, security incident response actions, security incident information management, self-adjustments in view of changes in cyber threat landscape, etc. It is also important to ensure that people and processes are connected, every process has a manager accountable, who has the authority to enforce the process.

References

[1] A. Kim, B. Wampler, J. Goppert, I. Hwang, and H. Aldridge, ser. Infotech@Aerospace Conferences. American Institute of Aeronautics and Astronautics, Jun 2012, ch. Cyber Attack Vulnerabilities Analysis for Unmanned Aerial Vehicles. [Online]. Available: http://dx.doi.org/10.2514/6.2012-2438

[2] J. S. Warner and R. G. Johnston, "GPS Spoofing Countermeasures," *Homeland Security Journal*, vol. 25, no. 2, pp. 19–27, 2003.

[3] D. L. McCallie, "Exploring Potential ADS-B Vulnerabilites in the FAA's Nextgen Air Transportation System," DTIC Document, Tech. Rep., 2011.

[4] D. McCallie, J. Butts, and R. Mills, "Security analysis of the ADS-B implementation in the next generation air transportation system," *International Journal of Critical Infrastructure Protection*, vol. 4, no. 2, pp. 78–87, 2011.

[5] B. Kovell, B. Mellish, T. Newman, and O. Kajopaiye, “Comparative analysis of ADS-B verification techniques,” *The University of Colorado, Boulder*, vol. 4, 2012.

[6] J. Krozel and D. Andrisani, ser. Aviation Technology, Integration, and Operations (ATIO) Conferences. American Institute of Aeronautics and Astronautics, Sep 2005, ch. Independent ADS-B Verification and Validation. [Online]. Available: http://dx.doi.org/10.2514/6.2005-7351

[7] V. Sidorov, W. K. Ng, K. Y. Lam, and M. F. Bin Mohamed Salleh, “A study of cyber security threats to traffic management of unmanned aircraft systems,” Air Traffic Management Research Institute, NTU, Tech. Rep., 2017. [Online]. Available: https://doi.org/10.13140/RG.2.2.31340.36484

[8] Federal Aviation Administration, “Pilot/Contorller Glossary,” Web resource: https://www.faa.gov/air_traffic/publications/media/pcg_4-03-14.pdf, accessed on 21 May 2016.

[9] International Civil Aviation Organization, “ICAO’s circular 328 AN/190 “Unmanned Aircraft Systems (UAS)”,” Web resource: http://www.icao.int/Meetings/UAS/Documents/Circular%20328_en.pdf, accessed on 21 May 2016.

[10] T. Prevot, J. Rios, P. Kopardekar, J. E. Robinson III, M. Johnson, and J. Jung, ser. AIAA Aviation. American Institute of Aeronautics and Astronautics, Jun 2016, ch. UAS Traffic Management (UTM) Concept of Operations to Safely Enable Low Altitude Flight Operations. [Online]. Available: http://dx.doi.org/10.2514/6.2016-3292

[11] FAA Sponsored “Sense and Avoid“ Workshop, “Sense and Avoid (SAA) for Unmanned Aircraft Systems (UAS),” October 2009.

[12] Cook, Stephen P and Brooks, Dallas and Cole, Rodney and Hackenberg, Davis and Raska, Vincent, “Defining well clear for unmanned aircraft systems,” *Proceedings of AIAA Infotech @ Aerospace, AIAA*, vol. 481, 2015.

[13] S. M. Lee, C. Park, M. A. Johnson, and E. R. Mueller, “Investigating Effects of Well Clear Definitions on UAS Sense-And-Avoid Operations in Enroute and Transition Airspace,” in *2013 Aviation Technology, Integration, and Operations Conference*. American Institute of Aeronautics and Astronautics (AIAA), aug 2013. [Online]. Available: http://dx.doi.org/10.2514/6.2013-4308

[14] M. Johnson, E. R. Mueller, and C. Santiago, “Characteristics of a Well Clear Definition and Alerting Criteria for Encounters Between UAS and Manned Aircraft in Class E Airspace,” 2015.

[15] O. I. de Normalización, *ISO/IEC 27005: Information technology-Security techniques – Information security risk management*. ISO, 2008. [Online]. Available: https://books.google.com.sg/books?id=K1HbZwEACAAJ

[16] C. Furlani, *FIPS 200: Minimum Security Requirements for Federal Information and Information Systems*. DIANE Publishing Company, 2009. [Online]. Available: https://books.google.com.sg/books?id=sDUZMDTNfSMC

[17] P. H. Kopardekar, “Unmanned Aerial System (UAS) Traffic Management (UTM): Enabling Low-Altitude Airspace and UAS Operations,” 2014.

[18] M. L. Cummings, S. Bruni, S. Mercier, and P. Mitchell, “Automation architecture for single operator, multiple uav command and control,” DTIC Document, Tech. Rep., 2007.

[19] J. L. Franke, V. Zaychik, T. M. Spura, and E. E. Alves, “Inverting the operator/vehicle ratio: Approaches to next generation UAV command and control,” *Proceedings of AUVSI Unmanned Systems North America*, vol. 2005, 2005.

[20] F. Friedman-Berg, J. Rein, and N. Racine, “Minimum visual information requirements for detect and avoid in unmanned aircraft systems,” in *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 58, no. 1. SAGE Publications, 2014, pp. 54–58.

[21] C. Santiago and E. Mueller, “Pilot Evaluation of a UAS Detect-and-Avoid System’s Effectiveness in Remaining Well Clear,” in *Eleventh UAS/Europe Air Traffic Management Research and Development Seminar (ATM2015)*, 2015.

[22] L. Fern, R. C. Rorie, J. S. Pack, R. J. Shively, and M. H. Draper, “An Evaluation of Detect and Avoid (DAA) Displays for Unmanned Aircraft Systems: The Effect of Information Level and Display Location on Pilot Performance,” in *Proceedings of 15th AIAA Aviation Technology, Integration, and Operations Conference*, 2015.

[23] E. M. Atkins, “Autonomy as an enabler of economically-viable, beyond-line-of-sight, low-altitude UAS applications with acceptable risk,” pp. 200–211, 2014.

[24] M. N. Stevens, B. Coloe, and E. M. Atkins, “Platform-independent geofencing for low altitude UAS operations,” in *15th AIAA Aviation Technology, Integration, and Operations Conference*. American Institute of Aeronautics and Astronautics (AIAA), jun 2015. [Online]. Available: http://dx.doi.org/10.2514/6.2015-3329