

Unauthorized UA in the Vicinity of Airports

Guidance Material



Contents

1.	Introduction	3
2.	Definitions	4
3.	Classification of Events.....	5
4.	Actors Involved: Roles and Responsibilities.....	6
5.	Detection.....	10
6.	Procedures.....	12
7.	Reporting, Investigation and Trend Analysis	19
8.	Counter-UAS Technologies	27
9.	Training & Awareness.....	32
	Appendix 1 - Risk Assessment Matrix.....	33
	Appendix 2 - Initial Assessment Checklist	36
	Appendix 3 - Stakeholder Matrix	38
	Appendix 4 - Case Studies	41
	Appendix 5 – Template for Tabletop Exercises	44

1. Introduction

With the expanded use of unmanned aircraft (UA), there has been an increase in the number of unauthorized UA events in close vicinity of aircraft and airports. Some of these events have resulted in extensive disruption to airline and airport operations and have had a large impact on the travelling public. Disruptions to aircraft operations caused by unauthorized use of UA, have raised multiple questions for regulators and aviation stakeholders on how to manage such events and ensure safe and secure operations at airports.

Even when encountering a minor or an unconfirmed unauthorized UA event, States and their stakeholders have often been forced to temporarily cease aircraft movements at airports. Inadequate preparation has hampered aviation stakeholders in limiting the operational impact of these events. In order to reduce the impact of disruptions caused by unauthorized UA, it is recommended that procedures as well as roles and responsibilities are clearly defined at a local level and that agreed protocols and procedures are implemented. Counter-UAS technology and associated measures are still in a development stage and have some limitations. At this time, such technology cannot provide a comprehensive defense for the aviation system. In addition, the implementation of any Counter-UAS technology and measures must not create unintended safety hazards and unmitigated risks to aircraft, authorized UA operators, and aviation infrastructures and personnel.

This guidance material provides best practices to ensure harmonization, to the extent possible, in how events involving unauthorized UA are managed and mitigated. The local airport, regulator, and Air Navigation Service Provider (ANSP) may implement additional or different measures due to national requirements that remain applicable. The focus of this guidance material is on the unauthorized operation of UA in close vicinity of airport and/or aircraft, that poses a threat to aviation safety and security. Authorized or known UA operation are expected to follow the rules and regulations as defined by the local authority, therefore, the recommendations contained in this document are not applicable to this category of operations

2. Definitions

Cooperative UA: A UA that broadcasts its position to other aircraft and ATC/UTM throughout its flight.

Event Phase (Phase): any of the phases of an event involving an unauthorized UA including the initial assessment, detection and identification, response, recovery and investigation.

Non-cooperative UA: A UA that does not broadcast its position or communicate with other aircraft throughout its flight.

Unmanned Aircraft (UA): an aircraft intended to be operated with no pilot on board

UAS Emergency Response Group (UERG): a group of stakeholders responsible to assess the impact and manage the response to an unauthorized UA affecting airport operations.

Note: It is recommended that the UERG include stakeholders beyond ATC and Airport management.

Weaponized UA: Unlike combat or strike UA used for military purposes, weaponized UA from a civil aviation perspective include any UA that is used to create harm to people, aircraft or infrastructure through deliberate action.

Note: A Weaponized UA may carry harmful material, chemicals, bombs, or guns.

3. Classification of Events

The type of an unauthorized UA event and impact level can determine the level of involvement of the different stakeholders and what procedures need to be followed. This chapter outlines a proposed classification of events which can be tailored to meet local requirements by airports, ANSPs and regulators. The classification of events is used to assess the level of response adequate to the impact level.

3.1 Types of Events

Events involving an unauthorized use of UA can affect aviation safety and security and can be the result of:

1. Use of a UA by an operator who is not aware of the UA's proximity to an aircraft, airport, or aerodrome.
2. Unlawful interference with aviation such as malicious use of a UA, using a UA to penetrate the secure perimeter of an airport or other aviation security sensitive areas or UA weaponization.
3. A report by the UA operator of a cyber-attack/hacking of a cooperative UA, rendering it uncooperative. Such an event when reported by the UA operator is considered a high impact level event.
4. Unauthorized use of a UA to collect images or information about the aerodrome.
5. Leveraging an UA to drop harmful payload or inflict damage via collision.
6. Using UA payloads to remotely control and spoof unsecured devices.
7. Wilful disruption of airport operations, such as for protests.

3.2 Parameters and Impact Level Identification

The following parameters can be considered in determining the impact of the event and by extension the level of response:

1. Intent/type of operation.
2. UA Specs; size, weight, payload, colour.
3. Proximity to airport, aerodrome, heliport, aircraft.
4. Height at which UA is operating.
5. UA trajectory.
6. Flight Phase of the aircraft involved in the encounter.
7. Traffic volume at the airport and type of traffic.
8. Near critical infrastructure, e.g. warehouse with dangerous goods or Instrument Landing System (ILS).
9. Type of sighting / detection (visual observation by pilot, airport staff, system detection, etc.).
10. Payload carried.

Depending on the level of impact on airport infrastructure and flight operations, unauthorized UA events can be categorized into:

1. **Low Impact Event.**
2. **Medium Impact Event**
3. **High Impact Event**

The steps taken in responding to an event involving an unauthorized UA depend on the event classification. Additional details about initial assessment, and response procedures are included under Chapter 6.

4. Actors Involved: Roles and Responsibilities

4.1 Involved Stakeholders in an Unauthorized UA Event

The following sections provide an overview of the stakeholders that are typically involved in an event in which an unauthorized UA came in close vicinity of an aircraft, an airport, or its critical infrastructure affecting the safe operation of aviation. The level of involvement of these stakeholders depends on the event impact level and on the phase of the event, whether it is in the detection or identification, during the response, during recovery or during the investigation phase. The response to unauthorized UA event is also guided by the national threat levels and the legal framework in place within each State which will determine the actors that are involved and their level of involvement. Details about the procedures to be following in the response to an authorized UA event are included under Chapter 6.

1. The Role of the National Aviation Authority (NAA) or Regulator

The National Aviation Authority (NAA) or the regulator is responsible for developing the national regulations and guidance in accordance with the provisions of the ICAO Chicago Convention and its Annexes except where it has filed a Difference to any of those provisions. It is recommended that the regulator be involved in the planning and investigation phases related to unauthorized UA. In some jurisdictions, the regulator is directly involved in the detection, identification, and response. The regulator also has a role in assessing lessons learned and enhancing the risk assessment and mitigation methodology for continual improvements of the local procedures related to unauthorized UA.

It is also recommended that the regulator works closely with industry representatives, ANSPs and airport operators to better understand technology developments and evolving operational requirements. It is important that the initial and further development of UA regulations involve industry to allow operators of UA to take joint 'ownership' of national regulations.

2. The Role of the Airport Operator (Airport Manager)

The airport operator has an overall responsibility for the safety and security of the airport infrastructure and operations, and all organisations and persons present in or using the facilities. The airport operator is directly affected by all unauthorized UA events on or in the vicinity of the airport. The airport operator is therefore at the center of all phases of the management of these events in close collaboration with the ANSP and other relevant stakeholders.

The main responsibilities of the airport operator can include:

- completing an initial assessment, and work with the ANSP, when an unauthorised UA is reported;
- initiating the first response to reduce the risk of the event on airport operations;
- activating the UERG as needed;
- monitoring the situation; and
- unrolling any measures that were implemented during the event to recover operation after the event has been contained.

It is recommended that the airport operator promulgates information to airport users related to the local procedures and relevant contact information for reporting UA events. In some cases, airport operators might choose to launch information and prevention campaigns to raise awareness about the risks of unauthorized UA in the vicinity of the airport. An airport operator is also responsible for evacuation procedures if it is determined that the intent of the UA is malicious, and the target is the airport infrastructure.

Guidelines relating to Aerodrome Emergency Planning are included under Chapter 9 of ICAO Annex 14 to the Chicago Convention.

3. The Role of Aviation Security

In most cases, aviation security is a function under the responsibility of the airport operator. However, in some instances it is a separate authority that has full or shared responsibility for security at the airport. The role of aviation security is expected to evolve with the new threats caused by unauthorized UA. The extent of their involvement in an event involving an unauthorized UA will depend on local procedures. However, during an event of an unauthorized UA, it is important for aviation security officers to liaise with other stakeholders involved in the event, to respond to any UA related event according to the impact level.

4. The Role of the Air Navigation Service Provider (ANSP)

The ANSP provides information and advice when an unauthorized UA event occurs, in accordance with a state's aviation security/safety authority regulations. The ANSP also responds to an event by assigning personnel to manage the operational impact, share information with the local airport operator, and possibly other affected airports, and adjacent ANSPs. The ANSP may interface with the local authorities as required by the procedure.

ICAO Annex 11 to the Chicago Convention requires Air Traffic Services Authorities to develop and promulgate contingency plans for implementation in the event of disruption or potential disruption, of air traffic services and related supporting services in the airspace for which they are responsible for. Guidelines relating to contingency planning are included under Attachment C of Annex 11.

5. The Role of Air Traffic Controller (ATCO)

Air Traffic Controllers (ATCOs) must ensure the safe, orderly and expeditious management of flights. This includes the operation of aircraft in flight in the vicinity of the aerodrome and of aircraft operating on the ground on manoeuvring areas. The ATCO's role during an event involving an unauthorized UA may vary based on the local organization and procedures. However, in principle, the main responsibility of an ATCO is to observe or receive the initial information on a reported event, immediately provide the necessary traffic information to pilots to ensure safety of flight operations and to liaise with the relevant actors, primarily the airport operator. ATCOs are equally responsible for informing neighbouring sectors and affected areas about the UA event and coordinate the appropriate or requested responses to the event.

ATCOs can expect pilots requesting speed reduction, alternative routing and/or radar vector. The safe management of the airspace, during an unauthorized UA event, will consider possible delays, and diversion, especially if no precise information and trajectory of unauthorized UA are available.

The ATC operational supervisor at the affected ATSU may perform some of these tasks as well as initiate ATFM measures if and when required. .

6. The Role of the Pilot Operating Aircraft in the Vicinity of the Event

A pilot operating into an airport is responsible to see and avoid any collision hazards and will report any UA sighting to ATC. When encountering an unauthorized UA, the pilot will follow instructions from ATC to safely land or depart from that airport, unless a RA for that UA is generated. In that case and in accordance with Doc 8168, the pilot will follow the RA.

If capable, ATC may assist the pilot by providing traffic information on the unauthorized UA. The abilities for an aircraft pilot to positively identify the unauthorized UA may be limited. However, it is recommended that the pilot provide ATC with as much information as possible about the unauthorized UA. As with closely spaced parallel instrument approaches, an unauthorized UA within the approach path of the aircraft that is capable of communication and identified by ATC, will be provided with special guidance from ATC.

It is acknowledged that ability to sight and report sighting may be limited in cases where the pilot of an aircraft operating in the vicinity of the event is a remote pilot of an RPA.

7. The Role of the UAS Operator and UA Remote Pilot

A known UA operator or remote pilot may be authorized to operate in the vicinity of an airport, e.g. for infrastructure inspection. Such known and authorized operation of a UA is excluded from the scope of this guidance material. However, if an authorized UA is hacked and the UA operator or remote pilot is no longer in control of the UA then the operator or remote pilot must notify the authorities, airport operator, and ATC as soon as possible. Depending on local procedures, a direct number for reporting incidents may be available for UA operators or remote pilots.

An UA Operator or remote pilot who identifies an unauthorized UA via a detect and avoid system or other available surveillance methods is responsible for reporting the detection to the appropriate ATC facility.

8. The Role of UAS OEMS

It is recommended that UAS OEMs make design decisions that aid in the prevention of unintentional stray of a UA into unauthorized airspace. In addition to compliance with any electronic identification features mandated by a State, it is recommended that OEMs consider including geographically restrictive software within the flight control systems. Additionally, UAS OEMs can consider design and aircraft markings that can facilitate the UA being visually identified by individuals in other aircraft or on the ground.

9. The Role of the UTM Service Provider

If established, the Unmanned Traffic Management (UTM) service provider, will support the identification and tracking of UA to ensure the safety and efficient management of the airspace. A UTM provider will be able to identify registered and known UA and determine when a contingency situation is faced by a known operator or remote pilot. If available, a UTM provider will report unknown or unregistered UA.

10. The Role of Law Enforcement Authority

Law enforcement authorities may be involved in the detection and response phases of an event depending on the threat level and the local procedures. In addition, local law enforcement will play a critical role in carrying out the investigation of unauthorized UA events. If necessary, the law enforcement authority will pursue actions to stop unauthorized UA operations, in coordination with the other involved stakeholders. National or local legal frameworks and requirements will influence the extent of involvement of law enforcement authorities.

11. The Role of the Intelligence Agency and Other Security or National Security Committees

It is recommended that national intelligence agency, other national security committees, or public safety as applicable in each State, are informed of events classified as medium or high impact events, to make sure that the coordination between the agencies brings the best support for the most appropriate response over the event. Those agencies may play a significant role during the identification and the investigation phases. The network and intelligence gathered for different purposes may be an important source of information. Because of the sensitivity of some information, a liaison role and resource between the UAS Emergency Response Group (UERG) and the intelligence community needs to be established.

It is also worth noting that intelligence and security agencies may perform certain activities which fall under specific exemptions, according to the related security function it must perform. Additional guidelines are available for authorities such as the Global Counterterrorism Forum document titled “Berlin Memorandum on Good Practices for Countering Terrorist Use of Unmanned Aerial Systems”¹ and the ICAO “Aviation Security Global Risk Context Statement”².

¹ <https://www.thegctf.org/Portals/1/Documents/Framework%20Documents/2019/Berlin%20Memorandum%20EN.pdf?ver=2020-01-13-143548-187>

² ICAO Doc 10108 – Restricted, please contact ICAO or your national Appropriate Authority for Aviation Security

8 Unauthorized UA in the Vicinity of Airports

12. The Role of the Military

If a national strategy or plan is developed, the extent of involvement of military in the event of an unauthorized UA are expected to be clearly defined. In the case of a security related event military and local law enforcement may have a more prominent role.

Some States are working together with their military and law enforcement agencies to develop Counter-UAS solutions and define the authorities' roles, and associated responsibilities. There are concerns and challenges associated with Counter-UAS technologies, which are highlighted under Chapter 9.

13. The Role of Public Observers and Local Communities

If a UA is sighted by non-operational staff such as public observers or individuals in the local community, then the observers are recommended to inform ATC or the local authorities using available numbers and pass as much accurate information as possible about the UA sighting, including location, altitude, lateral and vertical separation, size, and other applicable details.

4.2 Involvement of Stakeholders

Actors involved in the response to an unauthorized UA event are expected to react in an appropriate manner depending on the impact of the event at or near an airport. Consideration is given to the possibility of malicious intent by an unauthorized UA operation in addition to careless UA operations or other low-level threat scenarios.

The tables under **Appendix 3** propose a Responsible-Accountable-Consulted-Informed (RACI) matrix which could be used and adapted to the unique conditions of each airport. It is recommended that airports, ANSPs, and regulators work together to identify the roles and responsibilities that fit for their local environment when dealing with unauthorized UA. The objective of the stakeholder RACI matrix is to create a baseline of thinking across a broad list of stakeholders that could be involved in an unauthorized event linked with a specific stage and process.

The columns contain the definition of roles for each phase from the initial assessment of an unauthorized UA event all the way through detection and identification, response, recovery and investigation.

The roles of different actors can be one of the following:

- **Responsible:** means an actor that is responsible to execute agreed steps or actions. There could be more than one responsible actor during any given phase.
- **Accountable:** is an actor who takes decisions and defines actions that are necessary in each phase. There could be one accountable actor per phase.
- **Consulted:** refers to an actor that provides input to all actions or decisions based on the impacts to their areas or their domain of expertise,
- **Informed:** is an actor who needs to be informed of the situation and how it is evolving.

5. Detection

5.1 Detection and Identification Responsibility

In some jurisdictions, governments and law enforcement have invested in UA detection and Counter-UAS technology. The UA detection and Counter-UAS technology is still developing and it may be beyond an airport's resources capability to invest in such technology. In addition, only relying on technology will not provide a comprehensive approach for detection and identification of unauthorized UA. If an airport considers using detection technology, then a safety risk assessment and a cost-benefit analysis will be needed before implementing any new technology.

Manufacturers of unmanned aircraft are investing in geofencing capabilities on board their aircraft. States may restrict certain areas which will be integrated into the geofencing capabilities. Nonetheless, there will still be a risk of an unauthorized UA operating in the vicinity of sensitive or safety-critical infrastructure, military and law enforcement activity areas, and airports. Therefore, relying on UA operators to know where they are not authorized to operate may not be enough.

The future evolution of Unmanned Traffic Management (UTM) is expected to enhance the ability to identify authorized and cooperative UA. Registration of UA will enable the NAA or regulator to identify the nationality of the aircraft, the operator and what person or machine is controlling the aircraft. Registration may also assist non-aviation-related agencies concerned with issues such as security, law enforcement and privacy. This is expected to reduce the frequency of events of unknown UA operating in non-authorized areas. However, the risks associated with reckless or malicious use of UA will continue to require monitoring, planning, and mitigation.

To ensure a harmonized approach and best results, it is recommended that detection and identification of unauthorized UA be a shared responsibility amongst the stakeholders involved. It is also recommended that local governments and law enforcement agencies work together with airport operators to ensure that there is an exchange of information related to identification and detection of unauthorized UA. Identifying an unauthorized UA (position, type, location) and determining the level of the threat enable an effective decision-making process and response by the stakeholders that are involved.

5.2 Detection and identification methods

Several detection/identification methods exist, ranging from visual sighting of unauthorized UA to sophisticated detection techniques relying on technology. This section is not intended to describe all of them but introduce the main 2 categories: visual detection and detection via technology.

5.2.1 Visual Sightings of Unauthorized UA

Visual sighting can be reported by pilots, ATC, airport personnel or public observers. The information provided by visual sighting may be limited but any sighting of an unauthorized UA in the vicinity of an airport or aircraft cannot be ignored. The first 10-15 minutes are critical for identification and response procedures. An initial assessment of a visual sighting of an unauthorized UA can enable a more effective way of agreeing on the most appropriate response for the initial threat level. The steps for carrying out an initial assessment are described under Chapter 6. An example of the initial assessment checklist is included in Appendix 2.

5.2.2 Detection and Identification by Technology

Some technological solutions can detect unauthorized UA and identify a particular model or even the aircraft or its operator's digital identification. Having situational awareness and the ability to deploy countermeasures is greatly enhanced if the exact location of the UA or its operator are known. Some equipment is expected to allow UA location tracking in real-time. Chapter 9 provides more details about available technologies for detection and counter UA measures.

If an unauthorized UA is detected by a system or technology, then such a detection will be immediately reported to ATC or the appropriate designated authority at the airport. Information and parameters received from detection systems can then be used to determine the threat level and initiate the applicable response.

6. Procedures

The following sub-sections provide recommended practices for procedures which can be scaled and adapted based on the local environment. It is important for all concerned actors to collaborate in the development of local procedures that will apply based on local specifications and regulations. In general, the procedure for responding to and managing a medium or high impact event involving an unauthorized UA event is expected to follow similar steps. However, the extent of involvement and the time of involvement of some stakeholders as well as the actions taken will vary depending on the impact level.

Figure 1 provides a quick reference for the main stages of the procedure cycle during an event of an unauthorized UA. The steps that are recommended to be taken during the different stages are further described in the following sub-sections. It is recommended that when developing local procedures, the local exceptions and limitations are considered, such as the role of security or local law enforcement agencies. In some jurisdictions, airport security functions may be conducted by local law enforcement, whereas, in others they may have standalone agencies or can be included in the airport operators' responsibilities.

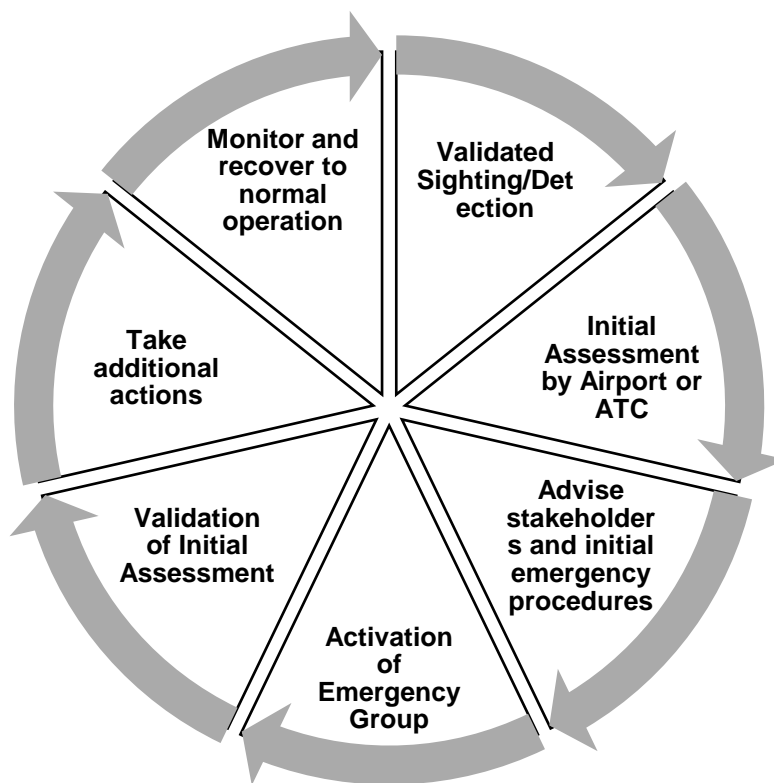


Figure 1: Procedures Cycle

If the airport operator does not have the authority to respond to events involving unauthorized UA, then it is recommended that the response plan and mechanism is adjusted to reflect the extent of involvement of law enforcement in the different phases. Once roles and responsibilities are defined, the Airport Security Plan and/or the Airport Operations Manual will be updated, particularly with regards to having a shared responsibility model.

6.1 Assessment of Impact Level

Any sighting or detection of an unauthorized UA in the vicinity of an airport or aircraft cannot be ignored. If an unauthorized UA is sighted or detected, it needs to be reported to the concerned regulator, law enforcement agency and local emergency response teams, as applicable. To make an initial determination of the impact level and consequently initiate procedures to follow, it is recommended that ATC and airport operator mutually agree on an **initial assessment** of the impact level. Part of this initial assessment is the identification if the operating UA is authorized or not, and then make an initial determination of the impact level.

It is recommended that the following is collected for the initial assessment of the event;

1. Location, including an estimate of the distance from airport, aircraft, or critical infrastructure.
2. Altitude and trajectory.
3. Moving or stationary.
4. Size, shape, appearance (e.g. small, quadcopter, camera underneath, colour, etc.).
5. Carrying payload or not.

A report of a UA operating in the vicinity of an airport or aircraft could be received from non-operational staff, e.g. the public. Such reports will also be taken into consideration.

6.1.1 Initial and Detailed Assessments of Impact Level

An example of an **initial assessment** checklist which can be used by ATC and/or the airport operator is included under **Appendix 2. Table 1** is provided as a quick reference with all parameters needed for the initial assessment to be conducted by ATC and/or the airport operator. An event may be categorized as low impact but could change to a medium or high impact event as more information is gathered. Therefore, ATC and the airport operator can continuously monitor a low impact event and share updates with the concerned stakeholders. If at any stage it is suspected that the intent of the unauthorized UA is malicious, then the event is considered high impact and the corresponding actions are initiated.

Whenever a medium or high impact event is identified, an emergency coordination group, the UAS Emergency Response Group (UERG) or a local equivalent, can be activated and additional response actions initiated. At this stage, it is recommended that another and a more comprehensive **collaborative assessment** of the risks is carried out to validate the initial assessment and agree on additional response measures. Recommendations for how to conduct a comprehensive risk assessment by the UERG or any other local stakeholder group are included under Appendix 1. It is recommended that such a collaborative approach to risk assessment and response involve stakeholders beyond ATC and the airport operator.

Parameter	Thresholds		
	Low	Medium	High
UA Size	Small	Medium	Large
Number of UA	One	Two	One or Several
Direction & Trajectory	Away from airport/aircraft	Towards airport/aircraft	Towards airport/aircraft
Altitude	Below 500ft	Between 500 and 1000ft	Over 1000ft
Flight Phase	Sighted/Detected outside traffic circuits	Sighted during final approach/initial climb	Sighted during Landing/Take-off
Proximity to airport, aerodrome, heliport, and critical infrastructure	Far from airport and/or critical infrastructure	Close to airport and/or critical infrastructure	Right over airport and/or critical infrastructure and causing visual obstruction
Proximity to aircraft	Far from aircraft	Close to aircraft	Right next to aircraft fuselage, engine, windshield

Trajectory	Stationary away from or moving away from risk areas and aircraft	stationary at or moving towards risk areas and aircraft	Stationary at or moving towards risk areas and aircraft
UA appears to be carrying a payload	No	Not Sure	Yes

Table 1: Initial Assessment of a Visual Sighting of an Unauthorized UA

6.2 Managing Air Traffic

Irrespective of the impact level or the response type, in the event of an unauthorized UA the pilot in command of aircraft operating in the vicinity of the aerodrome where the event occurred has the final authority over the safety of the flight. ATC will manage traffic in a way to ensure overall safety in the airspace. All ATC facilities need to be made aware of an unauthorized UA and be informed of its location. If contact with the remote pilot is possible, ATC will direct the UA to land or vacate the unauthorized area. If an unauthorized UA lands on an airfield, then the area needs to be cleared and local law enforcement needs to be notified.

Irrespective of the impact level of an unauthorized UA, ATC will make a radio broadcast informing aircraft of the situation, which can include the following;

- i. Location, altitude, and trajectory of the UA (exact or approximate)
- ii. Description of UA (color, size, lights, payload).
- iii. Nature of UA activity and/or interference with flight operations.

ATC and the airport operator will continue observing the UA throughout the event and provide updates to relevant parties.

Many UA flight times are approximately 20-30 minutes, at which point the UA will likely return to the operator or designated landing area for retrieval by the operator. It is important that officers track the UA during the return flight and direct unit(s) to the landing area to identify the operator. If it appears that the UA operator is located outside the airport jurisdictional boundary, the UERG can contact the law enforcement agency with jurisdiction over the location and request enforcement of applicable local municipal codes.

6.3 Activation of the UERG

To appropriately respond to an unauthorized UA, it is recommended that an airport has an emergency coordination group or cell or a similar functionality as a UERG. Alternatively, the role of the UERG can be integrated into existing local structures for response and recovery of emergencies at the local airport. If established, the UERG can consist of the following main actors:

- Local ANSP (ACC and Tower)
- Airport authority and operator
- Regulator
- Law enforcement / airport security
- UTM provider (if available)
- Airspace Users (this group would include both local airlines and foreign operators at the main hub)

The recommendations in this guidance material focus on the functionality of the UERG irrespective of the local organizational structure that is used to ensure such functionality exists.

6.4 General Response to an Unauthorized UA Event

Depending on the impact level, different steps can be carried out in response to an unauthorized UA event. The following table reflects the recommended steps to be taken depending on the type of event. When developing procedures, variations based on local legal frameworks need to be considered.

Impact Level	Response
<p style="text-align: center;">Low</p>	<ul style="list-style-type: none"> • Operating pilots, ATC and airport operator continue monitoring the situation for 60 additional minutes after the initial sighting • ATC to inform neighboring sectors and pilots already on and joining the frequency. • ATC or airport operator to inform the regulator, affected authorities and law enforcement. • ATC continue to inform pilots joining the frequency from the moment of initial report of sighting an unauthorized UA until the event is contained and poses no additional threat to operations • ATC and operating pilots to work together to ensure safe traffic movement • For operating traffic (either with the pilot on board, or piloted by a remote pilot), the pilots in command will have the discretion to take the necessary actions in their professional judgment to ensure the safe conclusion of the flight including deviating to an alternate airport • If no other report is received continue operations as normal • ATC to submit a post-event report to local regulator • In case the assessment of the event changes, upgrade the event to medium or high impact.
<p style="text-align: center;">Medium</p>	<ul style="list-style-type: none"> • UERG (or equivalent) is activated to conduct more thorough impact assessment and initiate the appropriate response • ATC to ensure the pilots of affected aircraft are notified of event and provided traffic information, as required (e.g. change runway, diverted). • ATC to inform neighboring sectors and pilots already on and joining the frequency. • The UERG or equivalent local emergency response group to inform the regulator, authorities and law enforcement and work with them to try and locate the operator • The UERG or equivalent local emergency response group to collaboratively decide on measures to be taken to minimize the risk of the event on airport operation • ATC to continue to inform pilots joining the frequency from the moment of initial report of sighting an unauthorized UA until the event is contained and poses no additional threat to operations • For operating traffic (either with the pilot on board, or piloted by a remote pilot), the pilots in command to have the discretion to take the necessary actions in their professional judgment to ensure the safe conclusion of the flight including deviating to an alternate airport • ATC and operating pilots to work together to ensure safe traffic movement • UERG to decide collaboratively regarding when the event is considered contained and when to scale back any imposed restrictions • UERG or equivalent local emergency response group to submit a post-event report to local regulator and applicable law enforcement authorities.
<p style="text-align: center;">High</p>	<ul style="list-style-type: none"> • UERG (or equivalent) is activated to conduct more thorough impact assessment and initiate the appropriate response including planning about restricting operations or airport closure • ATC to ensure the pilots of affected aircraft are notified of event and provided traffic information, as required (e.g. airspace closure). • ATC to inform neighboring sectors and pilots already on and joining the frequency. • The UERG or equivalent local emergency response group to inform the regulator, affected authorities and law enforcement and work with them to try and locate the operator • The UERG or equivalent local emergency response group to collaboratively decide on measures to be taken to minimize the risk of the event on airport operation • ATC to continue to inform pilots joining the frequency from the moment of initial report of sighting an unauthorized UA until the event is contained and poses no additional threat to operations • ATC and operating pilots to work together to ensure safe traffic movement • For operating traffic (either with the pilot on board, or piloted by a remote pilot), the pilots in command to have the discretion to take the necessary actions in their professional judgment to ensure the safe conclusion of the flight including deviating to an alternate airport. • UERG to decide collaboratively regarding when the event is considered contained and when to scale back any imposed restrictions • UERG or equivalent local emergency response group to submit a post-event report to local regulator and applicable law enforcement authorities.

Table 2: Impact Level and Associated Response Steps

6.5 Additional Considerations for Events Involving Malicious Intent and Security Threats

At global level, the ICAO Working Group on Threat and Risk stated in 2019 that “Developments in technology mean that weaponized RPAS are becoming more advanced, more accessible, and that terrorists are showing increased interest and demonstrated willingness to use this attack method in the civilian environment”. The ICAO Risk Context Statement takes into consideration the ICAO framework and not the measures that individual States and airports may have adopted. However, the increased global risk assessed for UA indicates that airport operators need to urgently engage with their appropriate authorities to identify appropriate mitigations. The first step is to carry out a thorough assessment of the security threats associated with unauthorized UA operations. It is recommended that the assessment considers the wide range of motivations for such operations including activism, espionage, negligence or carelessness, and terrorism. An airport risk assessment for security related threats helps identify response measures to severe threats to airport operations, such as:

- Use of UA to attack an aircraft in flight. Aircraft on either arrival or departure phase are the most vulnerable to attack using a UA. The two most notable scenarios associated with small UA flown deliberately into critical aircraft components (engine, windshield) are:
 - i. Use of UA’s mass to cause damage.
 - ii. Use of a UA with an explosive device (payload) attached.
- Use of UA as weapons to attack targets in the ground. This may include:
 - i. Delivery of a chemical, radiological or biological agent into a public area.
 - ii. Direct attack on an aircraft on the ground or airport with an explosive device.

Any act or attempted act which jeopardizes the safety of civil aviation is considered an “act of unlawful interference against civil aviation” by ICAO, and related procedures are outlined under Annex 17.

If a UA Operator suspects a cyber-attack inducing loss of control of the UA, then this is automatically considered a security event and the overtaken UA is regarded as having malicious intent. In such an event, necessary measures and precautions must be taken to secure a safe landing of the UA, or to shut it down. If the UA has a payload, the measures need to consider this element before deciding of the best course of action.

6.6 Response Procedures using Counter UAS Technology

If an airport has implemented any UA Detection technology, then the airport and law enforcement responsibilities may include the following:

- Detection of an unauthorized UA and identification of the type of device;
- Report of events to all stakeholders including the local civil aviation authority;
- Observation of the UA in flight;
- Locating the operator; and
- Ensuring UA lands outside the vicinity of the airport or is deterred from harming operating aircraft or airport facilities.

If an airport has implemented any Counter-UAS technology to mitigate unauthorized or malicious use of UA, or if the State’s local law enforcement has the capability and authority to use Counter-UAS technology, then in coordination with the UERG, the following steps may be followed after an unauthorised UA is detected;

- Disable, damage, or destroy the UA
- Log and secure the Counter-UAS equipment that is/has been used to contain the event.
- Conduct scene assessment and protect/secure the scene (shut down/disable any rotor, use Personal Protective Equipment, photograph the scene).
- Identify the UA operator if possible.

6.7 Recovery of Operations

Declarations regarding the containment of an emergency event and subsequent resumption of operations are some of the hardest decisions that key personnel have to make during an emergency. The UERG, or its local equivalent, can consider many factors when issuing “all clear” declarations and when resuming full or partial operations at the airport or facility. It is recommended that the resumption of full or partial operations is supported by a collaborative risk assessment to ensure that all relevant stakeholders participate and provide their full perspective of ongoing activity and impacts. Even though the authority to resume normal operations may rest with one individual, multiple individuals and organizations maintain the responsibility for recovery and therefore it is recommended that decision regarding resumption of operations is done collaboratively.

When conducting the assessment to resume operations, the UERG, or its local equivalent, may consider information, such as;

1. The status of the unauthorized UA (captured, disabled, disappeared, etc.) and when was the last sighting.
2. Which portions of the operation were affected and how that affects the resumption of operation.
3. Which facilities were impacted and how that affects the resumption of operation.
4. Which physical areas are being investigated and which will remain closed.
5. If all resources and equipment are available to support resumption of operation.
6. Whether additional personnel are needed to resume operations.

Particular attention needs to be given to situations where the unauthorized UA has not been sighted or detected for a period of time, but no information is available on the whereabouts of the UA or the pilot. There is a risk of a subsequent reappearance of the unauthorized UA. Therefore, following the assessment and decision to resume operations taken by the UERG, it is recommended that the following points are considered:

1. Notifications are made to all affected stakeholders that the airport is about to be declared safe, to ensure there are no concerns on the parts of impacted organizations or personnel.
2. Customer and passenger notifications and announcements can ensure controlled repopulation of facilities and awareness of potential ongoing impacts from the event.
3. Procedures are initiated for repopulation of public areas that need to be supported by airport staff to ensure orderly re-entry into the building and other facilities so that service and support organizations are not overwhelmed.
4. The necessary steps needed to communicate the containment of the event and resumption of activities to the relevant authorities, and if required, the public and media.
5. If the UA operator has still not been identified, the activation of local authorities to conduct a broader research
6. TA post-event assessment if the event occurred within the aerodrome area.

It is recommended that airport recovery protocols are standardized to define recovery and reopening practices with specific lines of authority (transnational, federal, local, airport operator). Such airport recovery protocols may have unique local characteristics that are specific to each individual airport.

6.7.1 Roles and responsibilities for unauthorized UA events outside the airport

It is recommended that airport operators, local law enforcement, and ATC agree on their respective roles regarding identification, reporting and mitigation of unauthorized UA when sighted outside the perimeter of the airport. In addition to local legislations and requirements, the following can be taken into consideration for the three main stakeholders:

1. Airport Operators: if the airport jurisdiction does not extend beyond the perimeter of the airport, the airport operator can ensure that appropriate arrangements have been made for responding to an unauthorized UA event outside the airport jurisdiction.

2. Local Law Enforcement: in coordination with airport and relevant authorities, local law enforcement can establish procedures to respond to non-cooperative and illegal UA outside the vicinity of an airport and take appropriate mitigating actions.
3. ATC: when an unauthorized UA is reported outside the vicinity of the airport, ATC can assess whether the actions proposed by local law enforcement to respond to the threat may affect air traffic and safe operations. ATC can also identify what additional arrangements are needed to ensure safety.

7. Reporting, Investigation and Trend Analysis

An event involving an unauthorised UA is considered a significant incident with safety and security implications and therefore needs to be reported to the regulator. It is recommended that local procedures establish the post-event reporting criteria and mechanism, with additional considerations if the UA is used intentionally to endanger aviation safety, which constitutes an act of unlawful interference. From a security perspective, ICAO Annex 17 – Security, requires that States have a mechanism for the reporting of security information from all sources and for the reporting of acts of unlawful interference. This is in addition to the safety reporting requirements under ICAO Annex 19.

7.1 Reporting Mechanism

Like other types of safety incidents, reporting of unauthorized UA events can include mandatory reporting, which is submitted to the regulator, as well as voluntary reporting. Mandatory reporting can be in a stepped approach with a safety incident report that is submitted to the regulator within 3 hours of the occurrence of an unauthorized UA event. Then once the event is contained; a final report can be submitted to the regulator. Such final report can support the investigation process.

The voluntary safety reporting systems within the airport and ANSP can enable the collection of safety data and safety information that is not captured by mandatory safety reporting systems. Information from voluntary and mandatory reporting can enable trend analysis and mitigation of future risks. This is critical for improving established procedures to respond to unauthorized UA.

7.2 Reporting Channels

Airport Operators: Guidance for reporting, utilising existing systems, can be provided to staff through the aerodrome operations manual. Consistency of reporting is critical to permit analysis of the data in line with ICAO Annex 19 and Annex 17. State bodies can be informed in order to carry out threat assessments. Dependent on the State this may be the police or other State security organisations.

Air Navigation Service Providers: In some cases, tactical measures and reporting in the case of unidentified or strayed aircraft, under the Procedures for Air Navigation Services – Air Traffic Management (PANS-ATM), have been expanded to cover unauthorised UA operations. A formal incident reporting system that includes unauthorised UA can be captured by the ANSP.

The general public may also report UA sightings. These reports may be to local authorities, but the reporter may also contact the airport to make the report. Airport websites are likely to be the first point of contact for the general public in relation to reporting unauthorized UA in the vicinity of an airport. Airport operators may consider placing advice on the web page to guide submission of information.

Manned Airspace Users: The reporting mechanisms under the safety management system can include reporting of encounters of unauthorized UA. To facilitate the analysis of the information, guidance can be provided by the operator to their operational staff in order to ensure consistency of reporting.

Cooperative/Known UA Operators: may also report the detection/sighting of an unauthorized UA, using DAA and therefore be able to file a report with the local authorities.

7.2.1 Recommended Taxonomy

Dependent on the circumstances an unauthorised UA may be classified as an AIRPROX, a strayed aircraft or maybe reported as being subject to unlawful interference. For example:

- *An Airprox is a situation in which, in the opinion of a pilot or air traffic services personnel, the distance between aircraft as well as their relative positions and speed have been such that the safety of the aircraft involved may have been compromised.*³

It is recommended that the occurrence type follow the taxonomy utilized by the State, the reporter's organization, or industry. The following taxonomy can be used to conduct safety trend analysis:

- i. Encounter with UA
 - Collision with UA
 - mid-air collisions
 - collisions on the ground between an aircraft and an UA

- ii. Near encounter with UA

In deciding whether the event is a 'Near encounter', consider:

- if the UA took avoiding action or would have if time had permitted.
- State/ANSP parameters for aircraft in critical proximity
- awareness of one aircraft to the other

Note: *If the pilot of an aircraft observes a UA while flying this would normally indicate the aircraft was in close proximity to the UA (due to the size of the UA).*

- iii. Sighting

Reported observation of UA within controlled airspace (or other airspace where permission is required), where the event is not classified as a near encounter.

7.2.2 Information Included in Security Incident Reports

States can utilise the common elements identified below to assist in security reporting. Information reported through safety mechanisms can also be utilised in the undertaking of security threat assessments.

To enable the analysis of the reported information it is recommended to have common elements contained in all reports. Different actors may have different perspectives of the scenario, but it is recommended that where possible all reports of security related events contain the following elements:

- Time of the observation/occurrence –provided in UTC to enable reports provided by different actors to be matched and amalgamated.
- Time the event ceased – this may not always be required if the event is a single sighting by a pilot but is tactically important when the unauthorised UA appears to be loitering in the area. Including this information in the post event report permits the investigator to confirm the number of UA based on expected battery life and may provide information on intent.
- Size and colour – In addition to the use of this information in the tactical assessment of risk, the size and colour of the unauthorized UA may be important in analysing the types of UA, calculating an underlying risk profile. The colour of the UA may appear different when seen from the ground than from the cockpit of the aircraft. Differences in colour reported by different actors does not necessarily indicate two separate occurrences.
- UA type – e.g. quadcopter, wing, etc.
- Number of reported/sighted UA if more than one.
- Position – using a common reference where possible, e.g. the airport, to base the multiple reports from. This can assist in matching and amalgamating the data. Reports in proximity to

³ UK Airprox Board 2015, accessed 15 July 2020, <https://www.airproxboard.org.uk/home/>

the airport may vary dependent on the actor, e.g. manned airspace user and air navigation service provider – right downwind for runway 16R, airport operator - south of the airport. Pilot reports that are not in proximity to the airport are more likely to indicate the locality being overflown at the time. Guidance can also be provided to actors to enable an accurate distance to be determined. Without vision assistance, to be visible a small quadcopter is likely to be within 660 meters⁴.

- Level – assessment of height is difficult from the ground. Actors can utilise cues to assist in determining the height of the UA but, where discrepancies in data exist, that of the manned airspace user can be taken as the most accurate unless ground based surveillance equipment is being utilised.
- Trajectory of flight / course / behaviour – This information is gathered during the actual response to permit the assessment of the threat. It can be replicated in the post event report so that security reviews can be undertaken, individual investigation by relevant authorities in attempt to determine those responsible, individual safety investigations for lessons learnt or analysis of trends.
- Cyber-attack – The attack vector, tactic and/or vulnerability and relative affected system, that was used to take-over the control of the UA or provoke loss of control, can be identified and shared by the OEM/Supplier, and a request for implementation of cyber security measures to limit the attack capacity can be proposed to the community. Training, education and awareness on cyber-attack and defence can be adjusted or developed accordingly.

7.2.3 Data Retention

Retention of safety data is covered under ICAO Annex 19 and ICAO Document 9859 – Safety Management Manual. It is up to the State to put these mechanisms in place and hence may vary across States. The retention of unauthorised UA activity can be included in and aligned with current safety data retention. If the unauthorised UA results in an aircraft accident then the provisions of ICAO Annex 13 – Aircraft Accident and Incident Investigation, as enacted by the State, apply.

Data being utilized in the judicial system for prosecution purposes can be required to be retained in accordance with State law and is not covered in this guidance material.

⁴ Aviassist RPAS, accessed 24 August 2020, Extending the line of sight for commercial drones, <https://www.aviassist.com.au/extending-line-sight-commercial-drones/>

7.3 Investigation

In line with Annex 13 of the ICAO Convention, any investigation of an accident or incident is solely to ensure the prevention of future accidents and incidents. It is not the purpose of this activity to apportion blame or liability. Using the same principle, an investigation of an event involving unauthorized UA can ensure the prevention of future events. In certain jurisdictions, some security aspects of events involving unauthorized UA might require investigation by local law enforcement.

Therefore, for the sake of this section of the guidance, the definition of an investigation carried out when an event involving an unauthorized UA occurs is:

A process conducted for the purpose of accident prevention which includes the gathering and analysis of information, the drawing of conclusions, including the determination of causes and/or contributing factors and, when appropriate, the making of safety recommendations.

It is recommended that every step of the investigation process is logged and properly recorded, including the chronological order and time stamp of all decisions that were taken throughout the event. This is particularly critical after the event is contained to assess the response and its effectiveness and be able to continually improve the response and recovery plans. Additionally, it is recommended that the different evidence/artefacts are secured or stored following a local custody process. The following figure illustrates the main steps that can be considered after an event is contained and operations has resumed.

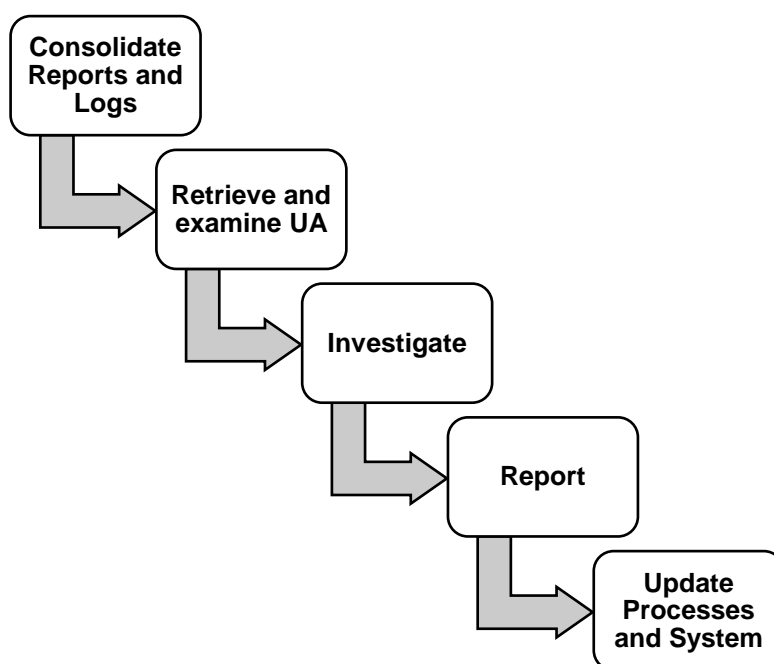


Figure 2: Actions Following an Event

Local authorities, law enforcement, and security agencies may have additional and more detailed steps to carry out their investigation of events involving unauthorized UA. For example, local legislation may fine or apply other legal penalties in relation to events of unlawful interference using an UA. In such a case, the actors who were involved in the event may be required to provide information to assist the local law enforcement in their investigation.

7.3.1 Investigation Steps

For the purpose of this section, it is assumed that geofencing interdiction methods have failed. The following proposes some possible actions and interventions. Investigation of events can include the following steps:

1. Secure UA and UA identification, including:
 - a. Identifying main device(s) and paired equipment, cellular, etc.
 - b. Log the state of the UA on site
2. Determine the nature of the event; cooperative, non-cooperative, weaponized.
3. Secure and identify witnesses and conduct interviews (at the scene and after recovery).
4. Download data from UA operator (if accessible).
5. Identify / Notify UA operator.
6. Log in an investigation casebook, all activities of the investigation including date/time/name/location/activity/event.
7. Report and present eyewitnesses' testimony, and investigation casebook.
8. Record and retain investigation outcome/report according to local legislations.

Specifically, in security related events, the local authorities may require a search and seizure, as required by local legislation. The extent of such search and seizure may cover:

1. The UA itself and its digital data. This includes:
 - a. Memory media storage
 - b. Copies of any downloadable data.
 - c. UA flight logs.
 - d. Cloud data/information.
 - e. Telemetry.
 - f. Data downlink from sensors.
 - g. Evidence of UA registry/certification.
 - h. Evidence of UA operator licensing.
 - i. Application/Server versions.
2. Counter-UAS identified signal recording and other logs.
3. Airport CCTV cameras to identify other sensitive locations, activities or events that may be linked

7.4 Analysis and trend monitoring

Analysis and trend monitoring fulfil requirements under ICAO Annexes 17 and 19. The analysis can be from a security or a safety perspective. ICAO Annex 13 investigations are undertaken with the objective of preventing future accidents or incidents.

7.4.1 Safety Analysis

Individual event: Analysis of an individual event can utilise the reported information to determine lessons learnt and methods to improve the response to future events. It is acknowledged that in most cases investigation is difficult.

Trend Analysis: General or targeted safety analysis can be used to determine and improve the understanding of the transport safety risk. Such an example was produced by the Australian Transport Safety Bureau in their publication: A safety analysis of remotely piloted aircraft systems 2012 to 2016:

A rapid growth and safety implications for traditional aviation.⁵ This report utilised not only submitted safety reports but UA certificate holders and industry trend information.

Analysis can also be undertaken on detected activity. UA surveillance equipment can be utilised, and the output analysed to determine the extent of unauthorised activity in close proximity to the airport and in relation to the flight paths. This information can be utilised to determine the level of risk in the system. However, this risk is applicable to unauthorised activity that is not malicious in nature. Refer to chapter 9 in relation to the use of such equipment. Such information can also be utilised to determine approximate regions from which the UA are being operated. Targeted education campaigns and signage in parks can then be utilised to reduce the number of occurrences.

7.4.2 Security Analysis

ICAO Annex 17 – Security, implies that States are to keep under constant review the level and nature of threat to civil aviation within its territory and airspace above it and conduct risk assessment for threats against aircraft. Such reviews and assessments can typically consider outcomes of vulnerability assessments and security reporting. These assessments can now include UA.

ICAO Doc 8973 – Aviation Security Manual now contains chapter 19 – protection of civil aviation infrastructure against unmanned aircraft. Given the sensitive nature of the material further guidance is not provided in this document.

7.5 Improvement of system and procedures for responding to unauthorized UA

It is important to learn from unauthorised UA events. The improvements may be minor in relation to check lists or communications between agencies or may be significant. Therefore, a State can conduct a vulnerability assessment or a post event risk assessment. Such an exercise involves analysis of past events and investigation reports to derive strategies that can lessen the impact of future risks.

Having a risk mitigation plan and implementation of mitigation measures can help ensure that an airport is prepared for the worst-case scenario. It is recommended that analysing risks and planning for future events is carried out as a collaborative effort between the airport, the regulator, the ANSP, local airlines, and law enforcement agencies.

7.5.1 Mitigation Planning and Implementation for Unauthorized UA Risks

A mitigation plan can be considered to lessen the impact of future unauthorized UA. Figure 3 illustrates the planning and implementation cycle of mitigation plans and measures.

⁵ <https://www.atsb.gov.au/publications/2017/ar-2017-016/>

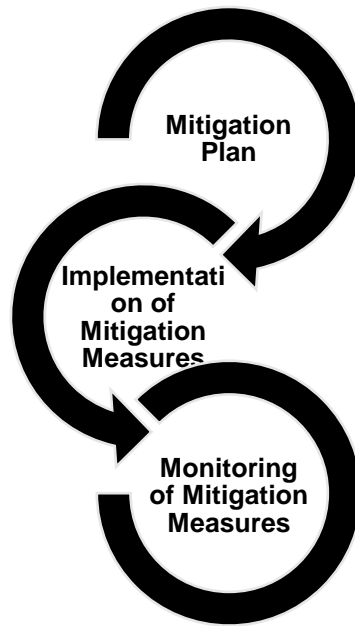


Figure 3: Mitigation Planning Cycle

A mitigation plan to reduce risks of future unauthorized UA events can be developed by the local airport in consultation with affected stakeholders such as the ANSP, local airline operators, and law enforcement and security agencies. Such a mitigation plan can be based on a review of current and emerging risks. Working with the different local stakeholders, an understanding of risks and their implications can help develop the right mitigation measures. An example of a risk assessment is shown in Table 3 and can be used to discuss and identify the right mitigation measures.

Event	Hazards	Consequence	Existing Controls	Rating	Ownership	New Controls	Rating
		(worst case scenario)					
				Tolerable or Intolerable			Tolerable or Intolerable

Table 3: Risk Assessment Matrix

Following the risk assessment, a mitigation plan can be developed with the following elements:

1. Mitigation measures to reduce the risk impact severity and/or probability of unauthorized UA
2. What actions need to be taken and when?
3. Who is responsible for the implementation of the mitigation measures and how will effective implementation be measured?

Once the mitigation plan is agreed, it can be used to drive local emergency procedures used by all actors. Emergency plans are used to appropriately respond to events when they occur, while the mitigation measures are on-going actions that can help reduce the impact of future events.

Once the mitigation measures are implemented the regulator and the airport operator can monitor the effectiveness of mitigation measures implementation. This includes evaluating current and new risks. A periodic revisit of the basic assumptions and premises of the risks can ensure that the mitigation measures and applied controls are effective.

8. Counter-UAS Technologies

8.1 Introduction

Counter-UAS technology and measures are a set of technological and operational tools that can be used, to monitor, detect, identify and counter UA incursions. Counter-UAS technology may include some countermeasures aimed to neutralize, or limit, potential risks posed by uncooperative UA. Counter-UAS technology also has the capability to record inappropriate or dangerous UA activities. Counter-UAS technology and measures can be both beneficial and harmful to aircraft and ATM operations. Therefore, the implementation of Counter-UAS measures needs to be preceded by an appropriate safety assessment that considers the potential impacts to all aviation stakeholders.

EUROCAE WG 115 and RTCA SC-238 are working together to develop standards applicable to Counter-UAS systems and technologies with a focus on Detection systems. Such standards can be taken into account when considering detection technologies.

8.2 Common UA Detection, Identification and Response Technologies

Currently, no ideal solution exists for defense against UA incursions at an airport. On-board UA capabilities and Counter-UAS technology are evolving rapidly. With limited ability to test Detection, Tracking and Identification (DTI) and Counter-UAS technology in airport-like environments, results from using DTI solutions are not overly conclusive. More testing and data collection are required. Responsible agencies can collaborate when evaluating DTI and Counter-UAS technology for use in commercial settings such as airports.

Currently in DTI and Counter-UAS marketplace, a wide variety of companies offer independent options for detection, identification, or mitigation, including those offering a combined layered approach with multiple tools for each area. Such comprehensive layered options often combine radar, radio frequency (RF), audio, acoustic, cameras, and artificial intelligence (AI) software integration programs for detection, tracking, and identification of UA, as well as a combination of electronic and kinetic options for interdiction. It is essential that the various technological modalities work together seamlessly to ensure layered approaches are accurate with their detection, identification, and tracking and can differentiate between approved and unapproved UA operations.

The following technical parameters, depending on the technologies, can be helpful in the selection of these type of Counter-UAS technology, depending on operational needs:

- a) Detection Range (m, km, miles)
- b) Scan Rate (Hz)
- c) Radio Frequencies or Frequency Bandwidth (Hz)
- d) Transmit Power (Watts)
- e) Direction Finding (degrees)
- f) Field of Regard/View (Vertical V and Horizontal H)
- g) Geolocation (Location Marker on digital support)
- h) Image Resolution (pixels)
- i) Classification (based on Counter-UAS Signature)

Recently, EUROCAE has produced the ED-280 “Guidelines for UAS safety analysis for the Specific category (low and medium levels of robustness), as part of their Specific Operations Risk Assessment SORA material. Additionally, IATA published a position on ‘Anti-UAS Technology’ which is available using this [link](#).

For technologies that are being considered, it is essential that each implementation undergo a thorough process demonstrating that it supports an agreed-upon safety benefit in a cost-effective manner. This requires appropriate investment decisions and implementation strategies through collaboration among all aviation stakeholders. The following section provides an executive summary of available Counter-UAS technologies for reference purposes. The subsequent sub-sections do not offer any endorsement nor support for any specific technological solution.

8.2.1 Detection Technology

8.2.1.1 Radar

Radar technology, with its all-weather, day/night capability can play an important role as a primary means of detecting UA-based threats. Radar detects UA of virtually any size by the radar signature generated when the aircraft encounters RF pulses emitted by the radar system. Radar can search, detect, and track multiple objects simultaneously, but to be successful, radar must quickly scan large areas with tremendous sensitivity, eliminate nuisance alarms from birds, and discern UA from ground targets.

To help distinguish between UA and other objects, algorithms, often enhanced with machine learning, are frequently employed. Radar can determine the exact position of an object and differentiate between stationary and moving targets; however, UA that only move vertically or extremely slowly sometimes pose a detection challenge.

8.2.1.2 Radio Frequency

Radio Frequency (RF) is usually considered a primary detection source for UA with all-weather, day/night performance capability. Scanners provide a solution for detecting, tracking, and identifying a UA often over an average detection range of 1–3 km. Detection uses algorithms to scan known frequencies to find and geolocate RF-emitting devices with an approximate location of a UA and its operator. Algorithms can also be employed to attempt to differentiate between authorized and unauthorized UA. RF systems can scan the electromagnetic spectrum and identify the specific transmissions from UA.

If the UA is transmitting a signal, the RF scanner will likely detect it, but an uncooperative UA will not emit RF signals. RF-based UA detection sensors can detect only a few airborne objects at a time, and their accuracy can be affected by numerous sources of potential interference, particularly line of sight obstacles that degrade detection performance. Overall, RF has a high probability of detection with a low false alarm rate.

8.2.1.3 Optical/Infrared Detection

Optical or infrared detection are not a typical detection source. Optical sensors can use infrared or thermal imaging as well as a standard daylight camera. Electro-optical sensors use a visual signature to detect UA, while infrared sensors use a heat signature. Optical sensors provide visuals on the UA and its potential payload and can record images as forensic evidence.

An optical system can be difficult to use for detection of a UA on its own because it is limited by weather and a narrow field of vision and range. It is often it is paired with radar and RF options as an additional tool for UA detection verification.

8.2.1.4 Acoustics

Acoustic sensor technology detects any object that produces noise (sound waves) and can detect sounds produced by UA motors. Acoustic sensors are generally combined with other detection tools. Algorithms and noise libraries can be employed to attempt to identify the type of UA and differentiate between authorized and unauthorized UA. The sensor must properly filter out ambient noise while still detecting small UA. Acoustic sensors have day/night performance but can be impacted by wind and other background noises. Sensors can detect multiple UA, and detection is possible even when the UA does not use RF communication.

8.2.1.5 Combined Sensors Technology

Combined sensors technology includes a combination of many systems that integrate a variety of different sensor types to provide a more robust detection, tracking, and identification capability.

8.2.2 Counter-UAS Technology

Any Counter-UAS system that transmits radio frequency (RF) energy must comply with the laws and regulations of their State. This regulatory structure typically involves a licensing process that is specific to each band of the RF Spectrum as so identified by the ITU and the State regulations. These regulations strictly control every aspect of the RF signal. This includes but is not limited to the type of modulation, channel width, power transmitted, out of band emissions, and the uses permitted in the specific band. The rules also specify the allowable interference created from transmitters and the amount of interference that receivers must be able to tolerate. Detection systems (e.g., Radar) that rely on active emitters must comply with these regulations.

Neutralization systems will also have to obtain permission to transmit from their State RF regulatory agency. This is often challenging as the regulations were not written to address RF emitters used to neutralize a UA. It is important that authorities, the local regulator, the ANSP, and airport work together to ensure that any deployed C-UAS technology does not have any potential conflict, particularly for spectrum, with regards to communication, navigation and surveillance infrastructure, aircraft equipage, and other technical systems supporting safe aviation systems. The use of any Counter-UAS technology is expected not to cause unintended safety or operational hazards to aircraft or aviation infrastructures. Therefore, the implementation of these technologies must be subject to a safety assessment and risk mitigation process to manage unintended risks.

8.2.2.1 Non-kinetic Counter-UAS Measures - Interruption of the WLAN

Interrupting the Wireless Local Area Network (WLAN) signal being used by some UA or broadcasting a set of radio-communication (RC) or computer commands to “take control” of the UA are possible. This technology needs however to be appropriately controlled to avoid instances of possible illegal sabotage or UA hijack. Moreover, careful and well-planned measures are expected to be deployed to avoid unpredictable / uncontrollable UA maneuvering following the WLAN interruption.

There are other examples of non-kinetic Counter-UAS measures. such as signal jamming, or GPS/GNSS spoofing that have a negative safety impact on manned aviation and therefore are not included.

8.2.2.2 Kinetic Interdiction

Kinetic interdiction refers to intercepting UA by physical means. Many types of kinetic options are being tested Kinetic techniques may not be a viable option for use in crowded areas due to the risk of a UA crashing or triggering the deployment of a payload. Local legal regulations need to be carefully reviewed when considering this type of Counter-UAS technology and measures. Safety impacts to other aircraft flying in the vicinity need to also be carefully evaluated. In some cases, a combination of interdiction elements to increase the likelihood of a successful interdiction.

Examples of kinetic interdiction measures include:

- Birds of Prey: Trained birds with protective gear used to attack and crash UA located in a restricted area.
- Nets: Hardened UA with attack nets capture and bring back targeted UA.
- Lasers/Microwaves: Directed energy to destroy the UA, causing it to crash to the ground.
- Live Fire: The use of conventional weapons, typically firearms, to target and shoot down UA.

8.3 Considerations for risk assessment of Counter-UAS technologies

The implementation of Counter-UAS measures will generally be within locations or airspace where there is a recognized safety and security risk to justify any infrastructure and operational costs for Counter-UAS measures. The areas of interest include the critical safety-sensitive areas around airports such as final approach, missed approach and departure corridors.

The use of Counter-UAS measures must not cause unintended safety or operational hazards to aircraft or aviation infrastructures. For example, the jamming or spoofing of GPS signals needs to be avoided as it may

harmfully impact aircraft navigation systems as well as air traffic management systems - both of which heavily rely on functional, uninterrupted GPS signals. Implementation of Counter-UAS measures must be subject to a safety assessment and risk mitigation process in order to manage unintended risks.

When deciding on the deployment of Counter-UAS measures, States, airports and aviation agencies are recommended to consider Counter-UAS measures that can:

- a) Support continuous monitoring of UA activities.
- b) Detect, identify and record UA activities in a timely manner and, where capable, geo-locate the operator of the UA.
- c) Perform effective countermeasures that can be safely and legally activated in time to prevent a UA from crossing the airport perimeter.

The use of any Counter-UAS technology must not:

- a) Create unintended safety hazards or increase unmitigated risks to other aircraft and aviation infrastructures;
- b) Hinder any local laws and regulations;
- c) Interfere with radio frequencies being used by aircraft, air traffic management (ATM) systems and other legally authorized applications; and
- d) Result in unpredictable UA maneuvering.
- e) Interfere with daily airport and airspace operations

Additional considerations for assessing the risks of any Counter-UAS technology include;

- a) Any limitations of the technology being considered;
- b) Analysis of previous reports indicating false positive or negative detection of a UA;
- c) Possible failure/modification of communication link or localization capabilities of the UA.

Prior to identifying the most suitable type of Counter-UAS technology, an evaluation of the environment of the C-UAS capabilities must be carried out, taking into consideration the following elements:

- a) The volume of airspace that the Counter-UAS is intended to protect and type of airspace users operating.
- b) Any existing airspace restrictions.
- c) The airspace requirements of the airports and applicable regulations.
- d) Existing and planned ATM safety and operational regulations and procedures
- e) Any security framework focusing on security policy, legislation and procedures to counter unlawful interference.
- f) Existing and planned Communication, Navigation and Surveillance systems.
- g) The airport type and layout design.
- h) Airport vicinity elements such as high-tension power lines, mobile phone antennas, wind farms, etc.
- i) The weather and light conditions.
- j) Local legal conditions including those related to aviation and frequency spectrum managements

8.3.1 Example of Technology Benchmarking

Airports and authorities can conduct their local risk assessment and technology comparison in consultation with airspace users, ANSPs, and other stakeholders. There are some examples of how to proceed with the risk assessment and technology comparison. One example is included in the table below which is used by the Homeland Security in the US. The table below considers several parameters including the sensor modalities where some require Direct or Visual Line of Sight (VLOS).⁶

⁶ Homeland Security – Science and Technology, Counter-Unmanned Aircraft Systems, Sept. 2019.

Modality	Active/Passive	Can Detect		Locate/Track		Identify/ Classify	Need LOS	Affected by Weather	Nighttime Operation
		UA	GCS	UA	GCS				
Radar	Active	Y	N	Y	Y	Limited	Y	N	Y
EO⁷	Passive	Y	N	Y	N	Limited	Y	Y	N
IR	Passive	Y	N	Y	N	Limited	Y	N	Y
RF	Passive	Y	Y	Y	Y	Y	Preferred	N	Y
Acoustics	Passive	Y	N	Y	N	Limited	Preferred	Y	Y

8.4 Cooperative UA

The future evolution of UTM will enhance the ability to identify authorized and cooperative UA, and by extension facilitate, by means of exclusion, the identification of unauthorized and uncooperative UA. In line with the ICAO UTM Framework, UTM is expected to have the ability to identify and track each unmanned aircraft in order to ensure safety and the efficient management of the airspace. Registration and remote identification (Remote ID) of UA are also expected to be part of future UTM system deployment.

Remote ID is expected to enable regulators, security and law enforcement authorities to identify UA operators flying in their jurisdictions. This is particularly important when it comes to UA operating in restricted airspace near aerodrome and other sensitive facilities.

8.4.1 Geofencing

Despite it not officially fitting into a counter UA mitigation, geofencing has mitigating qualities built into the UA itself. This technology can be regularly updated by manufacturers to include new and temporary restricted zones, evolving with risk-based data and information. Some manufacturers have gone so far as to expand the airport area restricted zones from two-dimensional circles to an enhanced safety zone, preventing UA from entering a three-dimensional bow-tie geofence to address approach and departure pathways. This can prevent unauthorized UA from flying near airplanes departing and landing at airports.

Risk-based solutions such as manufacturer-installed geofencing technology are essential advancements in mitigation and can become the industry standard, rather than the exception. Manufacturers can share the responsibility for helping to restrict access to sensitive flight locations, including airports, except for those authorized for approved UA missions. Geofencing can play a major role in ensuring that reckless use of UA do not interfere with airport operations. Reliable methods of ensuring that information on restricted zones utilized by the UA are up-to-date and routinely updated are also necessary.

⁷ EO is Electro Optical technology which uses cameras to track and detect UA

9. Training & Awareness

9.1 Training and Awareness for Individual Operators

The concept of a user-friendly test for new UA operators can help ensure a basic understanding of flight safety and airmanship, especially regarding recreational or personal use of small UA. Some manufacturers have begun requiring new operators to pass a short “knowledge quiz” before operating a new UA. Additional resources and recommendations exist through ICAO, IATA, ACI and IFALPA.

Some States require UA operators to undergo not only a training but a licensing and qualification process. Requirements for obtaining a license or permit to operate a UA, even for personal use, are available on States websites under their published regulations. Current State regulations can be accessed on the ICAO UAS Toolkit (<https://www.icao.int/safety/UA/UASToolkit/Pages/default.aspx>).

9.2 Awareness for Individual Actors

The different actors involved in the detection and response phases of an unauthorized UA can have their own internal training to ensure that their staff are aware of the local regulations and requirements and the developed contingency and response plans. It is recommended that the training follow an established training programme, that would include initial training and recurrent training. The training can include both theory and practical exercises. For example, airport operators can regularly conduct tabletop exercises and drills to test procedures and ensure that their staff as well as the stakeholders they deal with are familiar with the steps that can be taken for different types of events. Such a training would be recorded and kept up to date into the individual actor’s personal training file. Any agreed response procedures and framework for assessing risks can also be communicated to the operational teams of the main actors.

9.3 Tabletop exercises

In addition to training for individual actors, tabletop exercises can be conducted involving all actors. If available and established, the UREG can be tested during the tabletop exercises. A subset of the UREG may be engaged in the planning and preparation of the exercise. The airport operator may organize these tabletop exercises and involve the different actors. Such tabletop exercises may be integrated into the regular testing of the Airport Emergency Plan. A draft template for such an exercise and the scenarios that could be used for simulating events are included under Appendix 5.

9.4 Public Awareness

In order to better educate the public about the impacts of unauthorized UA operation near or at airports and to make information accessible to UA operators and remote pilots, regulators can work with airport authorities to make available such information to the public. Different channels can be used, such as dedicating a webpage for the “dos” and “Don’ts”. Flyers and mobile applications can also be used. An example is the Before You Fly campaign and B4UFLY mobile application that shows recreational UA operators where they can and cannot fly with interactive maps.

Appendix 1 - Risk Assessment Matrix

The following tables provide a reference for how to conduct a detailed assessment of risks associated with unauthorized UA events. Different actors involved in the detection and response of unauthorized UA may have their own internet risk assessment processes. Whenever the intent is identified as malicious, then the event can be considered high impact, irrespective of the other parameters.

Using the threshold tables under this appendix, the impact level is confirmed. In most cases an event can be characterized by a threshold for each parameter and therefore the assessment and determination of the impact level can consider the different weights of the thresholds. Using the weighted values of the different thresholds, the UERG can identify a total weight for the impact assessment. The level of exposure can be determined using parameters such as traffic volume. Combining the weight of the impact and the level of exposure the UERG can determine the level of response. The roles and responsibilities of the different stakeholders in the event on an unauthorized UA can also be determined based on the level of risk.

The risk assessment model included below can also be used to evaluate the event once it is contained and make recommendations for improvements to local procedures. When doing an assessment of historic events to better prepare for future risks and hazards, the following questions can be considered:

- What were the direct and indirect impacts/damage of a previous event related to unauthorized UA on:
 - Facility infrastructure
 - Facility operations
 - Flight Operations
 - Flying public
- How long did it take to return to normal operation?
- What data or information was maintained on damages or disruption? Were problem areas fixed or upgraded after the last event?

Step 1: Information collection about the event

Parameter	Thresholds		
	Low	Medium	High
Intent of Operation	Known / cooperative UA	Unknown / Uncooperative UA	Malicious Intent (unknown/uncooperative UA)
UA Weight / Size	250 g to 25 kg	25 kg to 150 kg	150 kg and above
Direction & Trajectory of the UA	Away from aerodrome/aircraft	Towards aerodrome/aircraft	Right over the aerodrome or next to aircraft
Proximity to aerodrome / aircraft	More than 5 km away	Between 1 and 5 km	Within 1 km radius
Altitude	Below 400ft	Between 400 and 1000 ft	Over 1000 ft
Number of Unique UA Sightings	One	Two	Several
UA Carrying Payload	No	Not Sure	Yes

Step 2: Assign weights to thresholds & identifying impact levels

A weight is given to make an assessment and determine the consequence and impact level. The following tables can be used. Using pre-identified thresholds, the impact level is determined. In most cases an event includes varying threshold levels and therefore the assessment and determination of the impact level can consider the different weights and then calculate a total weight for the impact assessment.

Parameter	Weights of Threshold		
	Low	Medium	High
Intent of Operation	1	2	3
UA Weight / Size	1	2	3
Trajectory of the UA	1	2	3
Proximity to aerodrome / aircraft	1	2	3
Altitude	1	2	3
Number of Unique UA Sightings	1	2	3
UA Carrying Payload	1	2	3

Threshold Weight Range	Impact Level
$X \leq 7$	Low
$7 < X < 10$	Medium – Not Critical
$10 < X < 15$	Medium - Critical
$X > 15$	High

Appendix 2 - Initial Assessment Checklist

Item	Recorded Response
How Many UA were reported?	
What is the source of the report? (pilot, staff, public, etc.)	
Does the UA appear to be carrying something (payload)?	<input type="checkbox"/> Yes <input type="checkbox"/> No Specify:.....
Is there an official approval/authorization for a UA to operate in that airport/airspace?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Not sure
What time was the UA sighting/detection reported (UTC)?	
Was the report of UA sighting/detection repeated?	<input type="checkbox"/> Yes <input type="checkbox"/> No
Is an accurate position/location/trajectory of the UA provided/available?	<input type="checkbox"/> Yes <input type="checkbox"/> No Specify:.....

Was the UA stationary or moving?	
Flight trajectory and speed (e.g. towards/away from runway, fast/slow)	
Was the type of the UA and/or its operator identified?	
Additional details of physical characteristics of UA reported (size, colour, lights, markings, fixed wing/multicopter, number of rotors, etc.)	
Does the UA appear to be deliberately attempting to interfere with traffic?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Not sure
List all the other units to which information was transferred. 1..... 2.....	
Is there a VIP flight conducting operation at the airport or terminal?	<input type="checkbox"/> Yes <input type="checkbox"/> No <input type="checkbox"/> Not sure
What immediate measures were taken?	
Other measures that were taken and when?	
How much time has elapsed since the report was received?	
Any other info?	

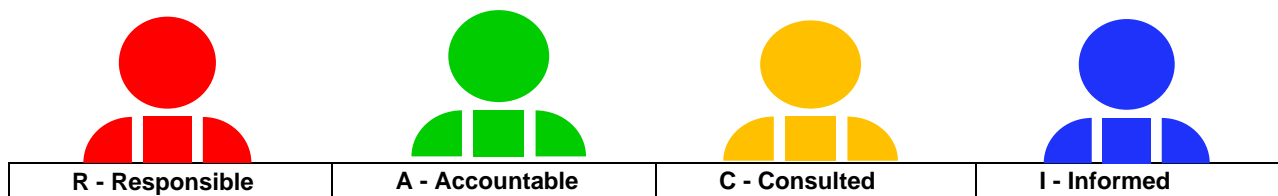
Appendix 3 - Stakeholder Matrix

Stakeholder Matrix for Low Impact events

Stakeholders	Initial Assessment	Detection & Identification	Response	Recovery	Investigation
Regulator	I*	R	R	I/C	A
Airport Operator	A**	R	A	A	R
Airport / Aviation Security	I	I	I	I	C
Air Traffic Controller	R	I	R	R	I
ANSP	R	I	R	R	R
Law enforcement authorities & Security Agencies	I	A	I	I/C	C
UTM (where there is a nearby provider)	I	I	R/I	R / I	C
Military	I	R	I	I	C
Pilot Operating in the Vicinity	R	I	R	R	I
UA Operator and UA Remote Pilot	I	C	I	I	C
UERG (or Equivalent Emergency Cell)	I	I	I	I	C

*Note: could also be R (responsible) in some cases

**Note: Could be the ANSP depending on who received the report

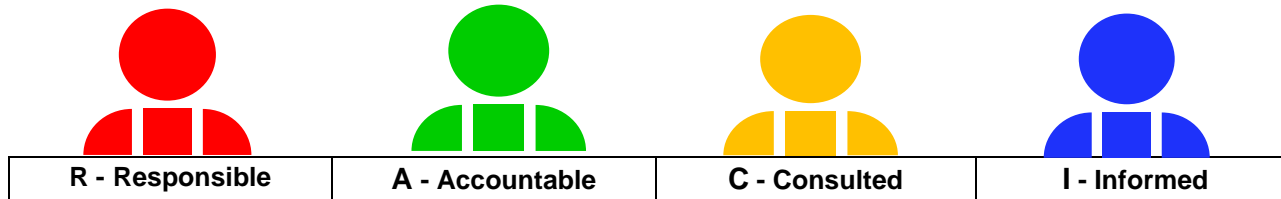


Stakeholder Matrix for Medium & High Impact events

Stakeholders	Initial Assessment	Detection & Identification	Response	Recovery	Investigation
Regulator	I*	R	R	I/C	A
Airport Operator	A*	R	R	R	I
Airport / Aviation Security	I/R	I/R	I/R	I/R	C/R
Air Traffic Controller	R	I	R	R	I
ANSP	R	I	R	R	I
Law enforcement authorities & Security Agencies	R	A	R	I/C	C
UTM (where there is a nearby provider)	I	I	R/I	R / I	C
Military	I	R	I/R	I	C
Pilot Operating in the Vicinity	R	I	R	R	I
UA Operator and UA Remote Pilot	I	C	I	I	C
UERG (or Equivalent Emergency Cell)	R	I	A	A	I

*Note: could also be R (responsible) in some cases

**Note: Could be the ANSP depending on who received the report



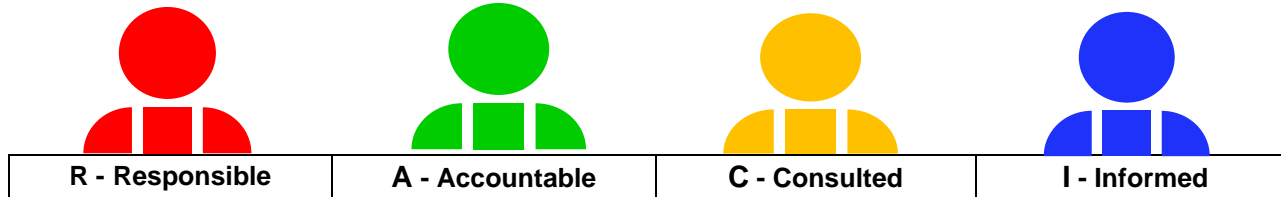
Stakeholder Matrix Specific for Security Related Events

Stakeholders	Initial Assessment	Detection & Identification	Response	Recovery	Investigation
Regulator	I*	R	R	I/C	I
Airport Operator	A**	I	I	I	I
Airport / Aviation Security	R	R	R	R	R
Air Traffic Controller	I	I	I	I	I
ANSP	I	I	I	I	I
Law enforcement authorities & Security Agencies	R	A***	A***	A***	A***
UTM (where there is a nearby provider)	I	I	I	I	C
Military	R	R	R	R	R
Pilot Operating in the Vicinity	I	I	R	R	I
UA Operator and UA Remote Pilot	I	C	I	I	C
UERG (or Equivalent Emergency Cell)	R	I	I	R	I

*Note: could also be R (responsible) in some cases

**Note: Could be the ANSP depending on who received the report

***Note: Depending on the country, the accountability may rest with the regulator or aviation security



Appendix 4 - Case Studies

Examples of events involving of unauthorized UA and simulated table-top exercises are included here for reference and to help build on lessons learned when developing local procedures.

There are resources available for worldwide events involving unauthorized UA, such as DEDrone: <https://www.dedrone.com/resources/incidents/all>.

Case Study 1: UAE

The UAE has experienced an increase in incidents of unauthorised intrusions of controlled airspace by UA which led the UAE GCAA to adopt a robust risk assessment process to determine the most appropriate actions to be taken.

Location	Date	Local Time	Length of delay
Abu Dhabi	16 Dec 2015	1616	5 minutes
Abu Dhabi	05 Dec 2015	1645	65 minutes
Abu Dhabi	26 Nov 2015	1645	65 minutes
Dubai	11 Jun 2016	1120	80 minutes
Dubai	28 Sep 2016	0805	45 minutes
Dubai/ Sharjah	29 Oct 2016	1945	80 minutes
Dubai/ Sharjah	18 Nov 2016	1325	-
Abu Dhabi/ Bateen	18 Nov 2016	0800	-

The UAE GCAA moved from complete closure of airspace to adopting a mechanism for determining the action on the day using a tactical risk assessment process to be conducted in-situ by supervisors and other stakeholders. The GCAA reviewed the existing Safety Alert 04/2016 with the aim of providing more guidance and support for decision makers in assessing the operational risk according to each circumstance. A tactical risk assessment process was determined to be the most appropriate mechanism and is a key part of the updated material.

The GCAA determined that the elevation of the material from a Safety Alert to a Safety Decision would provide more support for decision makers and emphasise the importance of the process. The Safety Decision is designed to work as per the following order:

- a) Report of an intruder
- b) Attempt to identify
- c) Advise aircraft in the area
- d) Advise the police
- e) Gather more information
- f) Determine hazardous area
- g) Analyse the risk to aircraft
- h) Take appropriate actions
- i) Monitor the situation
- j) Scale-back any restrictions
- k) Continue traffic information
- l) Resume normality

An unauthorised UA is considered a significant incident with safety and security implications. The GCAA requires Air Traffic Service Units (ATSUs) to establish and implement a procedure to ensure:

- prompt notification to the GCAA Duty Investigator, and;
- a Reporting of Safety Incident (ROSI) is submitted within 3 hours from the time of the occurrence.

Case Study 2: Riga, Latvia

On 2 May 2020, an unmanned aircraft became uncontrolled because the control system was switched off during a controlled test flight. The operator lost communications with the UA and lost track of its location. Emergency procedure was followed by UA operator to inform ANSP about missing an uncontrolled UA. This led to a restriction of IFR and night VFR flights in Riga FIR and expanded searching operation for 3 days.

Facts:

- UA operation initially was conducted in reserved airspace for UA operator activities.
- Take-off weight of fixed wing UA was 26kg and the expected duration of flight was up to 90 hours.
- Initial flight operation plan: endurance test within VLOS.

Institutions involved:

- Civil Aviation Agency;
- Air Navigation Service Provider (Latvijas gaisa satiksme (LGS));
- Latvian National Armed Forces;
- Aeronautical Search and Rescue Coordination Centre – (ARCC);
- State Police;
- State boarder guard;
- State Fire and Rescue Service.

Media was involved to receive information from the company about the location of the missing UA. It caused both positive and negative consequences. During uncontrolled flight, the UA entered Class C airspace approaching the Riga International Airport runway threshold points of less than 4NM at the approximate altitude of 120m (AMSL). Missing UA was found on 15th May 2020, about 77 km away from the place off take off.



Case Study 3: Transport Canada National Exercise (RPAS Shield II)

On 20 Nov 2019, Transport Canada (TC) led a tabletop exercise (TTX) to engage and guide stakeholders through response actions to an unauthorized UA incursion at Vancouver International Airport (YVR). The main objectives of the exercise were to:

1. Test response protocols for use in an event of a UA incident at YVR.
2. Identify detection and interdiction capabilities.
3. Examine appropriate time for resumption of airport operations.

The exercise was co-hosted by TC and the Vancouver Airport Authority (VAA) and involved participants from VAA, TC, NAV CANADA, Royal Canadian Mounted Police, the Department of National Defense, and other federal and industry partners. The participating stakeholders in the exercise were divided into:

- **Players:** Respond to situation presented based on current plans, policies, and procedures.
- **Observers:** Do not participate in moderated discussion but may support players in developing responses.
- **Facilitators:** Provide situation updates and moderate discussions.
- **Evaluators:** Observe and document player discussions.

The exercise considered a hypothetical scenario during which multiple unauthorized UA are sighted in and around YVR airspace and consequently led to the disruption of operations at YVR. By injecting different variables, the players were given the opportunity to simulate their respective response actions to the unauthorized UA, with the aim to mitigate the UA threat, locate the operator, and ultimately resume YVR operations.

The scenario and injects invoked discussion and collaboration by all participants. The TTX objectives were achieved and through this exercise, TC was able:

- validate the response protocols included in the *Industry Guidance: Developing Integrated Response Plans for RPAS Incident at an Airport*;
- verify roles and responsibilities of key stakeholders;
- verify legal authorities of key stakeholders;
- discuss and practice coordination of response actions of key stakeholders;
- discuss counter-UA technology capabilities (detection and interdiction); and,
- verify protocol for resumption of airport operations.

This exercise further identified the importance of using tabletops to highlight gaps, practice protocols and refine techniques that may not be regularly used, while also allowing unauthorized UA incident management to be integrated into regular incident management systems. Overall, the Vancouver TTX was well received and provided an opportunity for key stakeholders to engage with each other offering participants an educational forum on the topic of unauthorized drones.

Appendix 5 – Template for Tabletop Exercises

SCENARIO 1 – An unauthorized UA is sighted in vicinity of xxxxx Airport, followed by multiple incursions into controlled airspace			
Serial	SITUATION	QUESTIONS / EXPECTED ACTIONS	TARGET AUDIENCE
1	<p>Today is XX/XX/ 202x and the time is 0800 hours (EST). xxxxx Airport is fully operational. The weather is fine, winds are from the north at 10 knots.</p> <p>No operational difficulties are being experienced.</p> <p>There is considerable media interest in Air operations due to the recent protests over aircraft noise and pollution.</p> <p>Police have been monitoring the activities of a protest group known as 'Save the Planet' who have been using social media to call for protests against the airport and the impact of air travel on the climate change.</p>	<p>What is your organisation currently dealing with?</p> <p>What resources do you have available?</p>	All participants
2	<p>Approximately 08:30 UA activity is occurring in areas between 5km and 10km west and south of the airport.</p> <p>Several UA are flying in excess of 400ft</p>	<p>Is this information of interest to any agency?</p> <p>How might you become aware of this information?</p> <p>How would you monitor?</p> <p>Who would you notify?</p> <p>How is this recorded?</p> <p>Does anyone have authority, responsibility or capability to proactively search for an UA?</p> <p>What detection capabilities are available? Who has the capabilities?</p> <p>Is a threat/risk assessment being conducted at this time? Who is leading it?</p> <p>How is the information communicated to the appropriate agencies?</p> <p>Would this information make its way to the law enforcement?</p> <p>What actions are being taken at this time by each agency?</p>	<p>ANSP</p> <p>AIRPORT</p> <p>Law enforcement / airport security</p> <p>UTM provider (if established)</p> <p>Regulator</p>

SCENARIO 1 – An unauthorized UA is sighted in vicinity of xxxxx Airport, followed by multiple incursions into controlled airspace			
Serial	SITUATION	QUESTIONS / EXPECTED ACTIONS	TARGET AUDIENCE
3	Approximately 09:00 UA activity is reported to be occurring in area 2km to 5km of the airport. Most activity is occurring west and south of the airport.	<p>Is this information of interest to any agency?</p> <p>How might you become aware of this information?</p> <p>How would you monitor?</p> <p>Who would you notify?</p> <p>Is this recorded?</p> <p>Does anyone have authority, responsibility or capability to proactively search for an UA?</p> <p>What detection capabilities are available? Who has the capabilities?</p> <p>Is a threat/risk assessment being conducted at this time? Who is leading it?</p> <p>How is the information communicated to the appropriate agencies?</p> <p>Would this information make its way to the law enforcement?</p> <p>What actions are being taken at this time by each agency?</p>	<p>ANSP</p> <p>AIRPORT</p> <p>Law enforcement / airport security</p> <p>UTM provider (if established)</p> <p>Regulator</p>

<p>4</p>	<p><i>At 09:30 a UA appears on the western boundary of airport. It then travels north and remains adjacent to the northern end of Runway X. It climbs to a height of 300 ft and hovers just outside the airport boundary.</i></p> <p><i>An approaching xxxxx aircraft, sights the UA and reports its location to ATC.</i></p> <p><i>The UA hovers for a further ten minutes and then travels in a westerly direction disappearing from sight.</i></p>	<p><i>Is the UA assessed as a threat by any agency?</i></p> <p><i>Is there a formal Threat/Risk assessment to follow?</i></p> <p><i>Who is notified? How are they notified?</i></p> <p><i>What action is taken?</i></p> <p><i>Who is in control?</i></p> <p><i>Have any offences been committed?</i></p> <p><i>Who is investigating?</i></p> <p><i>What is the impact on air operations?</i></p> <p><i>Does anyone have authority, responsibility or capability to proactively search for an UA?</i></p> <p><i>What detection capabilities are available? Who has the capabilities?</i></p> <p><i>Is a threat/risk assessment being conducted at this time? Who is leading it?</i></p> <p><i>How is the information communicated to the appropriate agencies?</i></p> <p><i>Would this information make its way to the law enforcement?</i></p> <p><i>What actions are being taken at this time by each agency?</i></p> <p><i>How does this impact the threat/risk assessment? Does it need to be repeated?</i></p> <p><i>How does this impact the actions of each agency? Any further actions being taken?</i></p> <p><i>How are the key partners coordinating the response?</i></p> <p><i>What effect does this have on airlines?</i></p>	<p><i>ANSP</i></p> <p><i>AIRPORT</i></p> <p><i>Law enforcement / airport security</i></p> <p><i>UTM provider (if established)</i></p> <p><i>Regulator</i></p> <p><i>Airspace Users</i></p>
----------	---	---	--

SCENARIO 1 – An unauthorized UA is sighted in vicinity of xxxxx Airport, followed by multiple incursions into controlled airspace			
Serial	SITUATION	QUESTIONS / EXPECTED ACTIONS	TARGET AUDIENCE
		Are interdiction capabilities available? Who has the capabilities? What are the technical challenges and requirements?	

5	<p>At 10:00 a UA is seen approaching south of Runway X from a westerly direction at an undetermined height. It crosses the path of a xxxx Aircraft which is in the process of landing, it is reported by the pilot as a near miss.</p> <p>The UA then continues to hover at a height of 600 feet south of Runway X, for a period of approximately fifteen minutes. It then travels in a westerly direction before disappearing from sight?</p>	<p>Is the UA assessed as a threat by any agency?</p> <p>What is the possible impact of a UA strike on a commercial aircraft?</p> <p>Who is notified? How are they notified?</p> <p>What action is taken?</p> <p>Is any action taken regarding Airport operations?</p> <p>Is the incident regarded as an attack on an aircraft?</p> <p>Does any agency have the capacity to disable the UA if incursions continue?</p> <p>What means do agencies have to detect UA incursions into controlled airspace?</p> <p>Is anyone collecting evidence?</p> <p>Who responds to media?</p> <p>Who is in control of this situation?</p> <p>Have any offences been committed?</p> <p>Who is collecting evidence?</p> <p>Who is investigating?</p> <p>How do agencies and organisations work together?</p> <p>Does anyone have authority, responsibility or capability to proactively search for an UA?</p> <p>What detection capabilities are available? Who has the capabilities?</p> <p>Is a threat/risk assessment being conducted at this time? Who is leading it?</p> <p>How is the information communicated to the appropriate agencies?</p>	<p>ANSP</p> <p>AIRPORT</p> <p>Law enforcement / airport security</p> <p>UTM provider (if established)</p> <p>Regulator</p> <p>Airspace Users</p>
---	---	--	--

SCENARIO 1 – An unauthorized UA is sighted in vicinity of xxxxx Airport, followed by multiple incursions into controlled airspace			
Serial	SITUATION	QUESTIONS / EXPECTED ACTIONS	TARGET AUDIENCE
		<p><i>Would this information make its way to the law enforcement?</i></p> <p><i>What actions are being taken at this time by each agency?</i></p> <p><i>How does this impact the threat/risk assessment? Does it need to be repeated?</i></p> <p><i>How does this impact the actions of each agency? Any further actions being taken?</i></p> <p><i>How are the key partners coordinating the response?</i></p> <p><i>What effect does this have on airlines?</i></p> <p><i>Are interdiction capabilities available? Who has the capabilities?</i></p> <p><i>What are the technical challenges and requirements?</i></p>	
6	<p><i>At 10:30 information is received by Police that a person has been seen operating a UA from a vessel located in waters immediately north of the airport</i></p> <p><i>(suspect vessel is unable to be located?)</i></p>	<p><i>Who responds to this report?</i></p> <p><i>What is the estimated response time?</i></p>	Law enforcement
8	<p><i>At 1100 a UA travelling from the east crosses the airport boundary and flies above Runway A for a period of fifteen minutes. It then travels east, disappearing from sight.</i></p> <p><i>Vision of the UA flying above the runway is broadcast by the media, who are reporting that the airport is closed?</i></p>	<p><i>What is the impact on Air operations?</i></p> <p><i>How do agencies and organisations work together?</i></p> <p><i>What technology is deployed?</i></p> <p><i>What Plans and procedures are activated?</i></p> <p><i>Are there existing procedures to follow?</i></p> <p><i>Who is dealing with the media?</i></p>	<p>ANSP</p> <p>AIRPORT</p> <p>Law enforcement / airport security</p> <p>UTM provider (if established)</p> <p>Regulator</p> <p>Airspace Users</p>

SCENARIO 1 – An unauthorized UA is sighted in vicinity of xxxxx Airport, followed by multiple incursions into controlled airspace			
Serial	SITUATION	QUESTIONS / EXPECTED ACTIONS	TARGET AUDIENCE
9	Numerous calls are received by police from members of the public regarding persons operating UA in the vicinity of the Airport?	Who responds to this information? Is there a way to identify legitimate and approved UA use as opposed to the offending UA?	Law enforcement ANSP
10	At 11:20 calls are received by police which report a person has been seen operating a UA from a white van parked at various locations outside of the airport precinct.	Who responds to this? Is this information shared?	Law Enforcement

<p>11</p>	<p>At 1200 a UA appears on the western boundary of the airport flying at 300ft. It flies above Runway X and appears to be deliberately interfering with Airport Operations. It flies for about fifteen minutes at various heights along the length of the runway. It then disappears west.</p> <p>At 1245 a UA appears from the Eastern boundary, flies at low level into the airport and lands on the Joint User Hydrant Installation (fuel farm). It remains in situ. Witnesses report that the UA appeared to have a package hanging from its undercarriage.</p> <p>Emergency Services (ARFF) respond. The UA is located on the roof of a fuel storage tank. It is noted to be carrying a package which appears to be an IED.</p>	<p>Who is in charge of responding to this incident?</p> <p>What is the impact on Air operations?</p> <p>Do evacuations occur?</p> <p>Is the EOC/UERG in a safe location?</p> <p>Who is in charge of making the area safe?</p> <p>Who has carriage of investigations?</p> <p>Is this regarded as a terrorist incident?</p> <p>Would an application for Military assistance be made?</p> <p>Does anyone have authority, responsibility or capability to proactively search for an UA?</p> <p>What detection capabilities are available? Who has the capabilities?</p> <p>Is a threat/risk assessment being conducted at this time? Who is leading it?</p> <p>How is the information communicated to the appropriate agencies?</p> <p>Would this information make its way to the law enforcement?</p> <p>What actions are being taken at this time by each agency?</p> <p>How does this impact the threat/risk assessment? Does it need to be repeated?</p> <p>How does this impact the actions of each agency? Any further actions being taken?</p> <p>How are the key partners coordinating the response?</p> <p>What effect does this have on airlines?</p>	<p>AIRPORT</p> <p>Law Enforcement</p>
-----------	--	---	---------------------------------------

SCENARIO 1 – An unauthorized UA is sighted in vicinity of xxxxx Airport, followed by multiple incursions into controlled airspace			
Serial	SITUATION	QUESTIONS / EXPECTED ACTIONS	TARGET AUDIENCE
		<p>Are interdiction capabilities available? Who has the capabilities?</p> <p>What are the technical challenges and requirements?</p> <p>Are airport operations suspended at this? Is airspace closure being considered? Who has authority to do so?</p> <p>Is assistance from additional agencies being requested at this time? How would this be done?</p>	
12	<p>At 1300 Information is received from the public that a UA was observed taking off and landing near the xxxx address.</p> <p>Police attend and find a white van parked in an area to north of the service centre near the lagoon. No person is located.</p>	<p>Who responds to this information?</p> <p>What action is taken?</p>	Law Enforcement
13	<p>At 1330 the occupant of the vehicle, returns from the service centre, he admits being a recreational UA user and flying a UA at low level around the area. He denies flying in the vicinity of the airport?</p>	<p>Has an offence been committed?</p> <p>Who prosecutes this offence?</p> <p>What action is taken?</p> <p>Is this person taken into custody?</p> <p>Were his vehicle and premises searched?</p> <p>Is this information shared</p>	Law Enforcement

SCENARIO 1 – An unauthorized UA is sighted in vicinity of xxxxx Airport, followed by multiple incursions into controlled airspace			
Serial	SITUATION	QUESTIONS / EXPECTED ACTIONS	TARGET AUDIENCE
14	<p>It is now 17:30 the UA and IED have now been rendered safe and removed from the Joint User Hydrant Installation (fuel farm).</p> <p>There has been no further UA activity since the last incident.</p>	<p>What is the impact on Air operations?</p> <p>How are Air operations restored?</p> <p>What information is considered?</p> <p>Who makes the decision?</p> <p>What has been the impact to Airlines?</p> <p>Who is dealing with media?</p> <p>Is this now regarded as an act of Terrorism?</p>	<p>ANSP</p> <p>AIRPORT</p> <p>Law Enforcement</p>
16	<p>It is now 08.00 on (following day)</p> <p>Update status on Person Of Interest (POI). No charges laid for airport incident. However, no further UA flights since arrest.</p> <p>No other POI's or suspects have been identified by Police.</p>	<p>What is the status of Air operations?</p> <p>What has been learned from yesterday?</p> <p>What resources are now on hand to deal with further UA activity?</p> <p>What is the implication of sustained closure?</p> <p>How is the information shared with key partners that the threat has been neutralized?</p> <p>Is the threat/risk assessment repeated at this time?</p> <p>At what point will airport operations resume and how is that decision made?</p> <p>If airspace was closed, at what point is airspace reopened? How is that decision made?</p>	<p>All agencies</p>
19	<p>Would the situation have been different if a threat to airport had been received in the days preceding this incident?</p>		
20	<p>Would the situation have been different if a high-level dignitary was due to land on the day?</p>		
21	<p>Would the situation be different if occurring in the hours of darkness?</p>		

SCENARIO 1 – An unauthorized UA is sighted in vicinity of xxxxx Airport, followed by multiple incursions into controlled airspace			
Serial	SITUATION	QUESTIONS / EXPECTED ACTIONS	TARGET AUDIENCE
22	Conduct Hot Debrief	<p><i>What are the key issues that have come out of that discussion that need further consideration/exploration?</i></p> <p><i>Is there a technical solution available?</i></p> <p><i>Are there legislative impediments?</i></p> <p><i>What needs to be improved?</i></p> <p><i>What worked well?</i></p>	All participants