Countering Threats from Uncrewed Aerial Systems

Assessing The Threat And Vulnerability

Published: **June 2023**
Classification: **Official**

National Protective Security Authority

Contents

Executive Summary

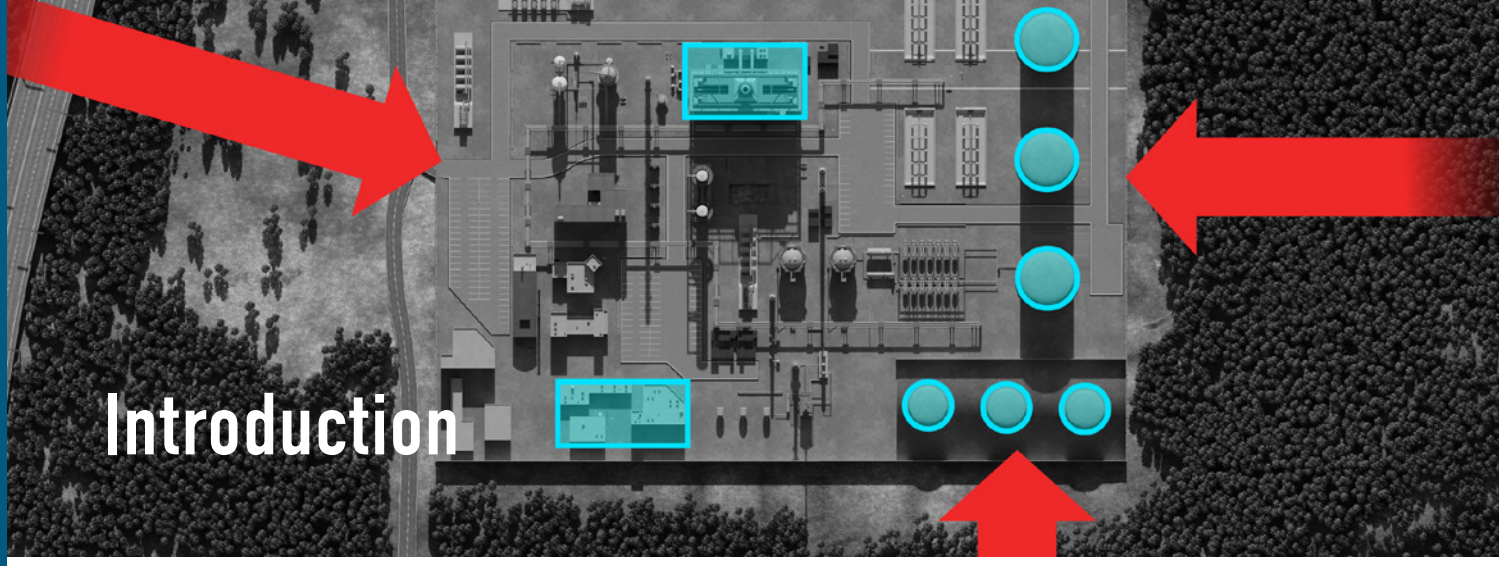
Guidance on the completion of a site specific Counter-Uncrewed Aerial System (C-UAS) Vulnerability Assessment (VA).

This document provides information as to how to assess the vulnerability of a site to the threat of Uncrewed Aerial Systems (UAS). Detailed guidance is provided as to the four tasks that should be undertaken to complete the VA.

TASK 1	Identify stakeholders and establish roles and responsibilities
TASK 2	Identify potential threats posed and critical assets
TASK 3	Identify the most likely Launch Sites (LS)
TASK 4	Consolidate the information gathered to identify the overall vulnerability

The information gathered can be used to inform:

- The understanding of the threat, vulnerability and risk from UAS to a site.
- The development of mitigation measures that could reduce the vulnerability and risk.



Introduction

Scope

A significant part of developing a strategy and plan to counter the threats of Uncrewed Aerial Systems (UAS) is undertaking a comprehensive assessment of how a site is vulnerable to the risks posed by UAS. This guidance document is intended to assist those responsible for the protection of National Infrastructure (NI) sites, sensitive sites, and crowded places that may have a risk or threat posed by UAS to complete a Counter-UAS (C-UAS) Vulnerability Assessment (VA) that will identify:

- The critical assets vulnerable from a UAS.
- The UAS threat actors and scenarios considered relevant to the site.
- The potential Launch Sites (LS) and flight paths.

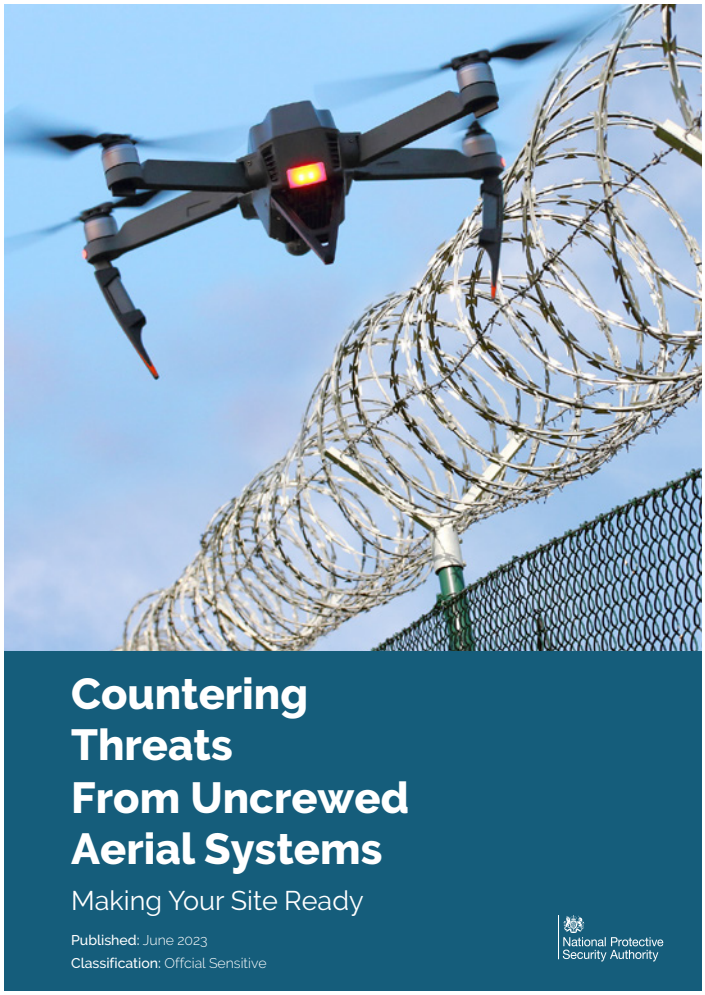
The information gathered can be used to inform:

- The understanding of the threat, vulnerability and risk from UAS to a site.
- The development of mitigation measures that could reduce the vulnerability and risk.

It should be read by:

- Site Security Managers.
- Physical Security Managers.
- Those responsible for site security risk assessments.
- Those in the security team and police delivering or supporting the site VA process

The guidance provided will integrate with the overarching document, Countering Threats From Uncrewed Aerial Systems – Making Your Site Ready, and other supplementary guidance documents, as described in the document titled – Countering Threats From Uncrewed Aerial Systems – an overview of guidance documents.



The focus of this guidance is on security-related risks. However, the principles provided can also be applied to safety-related risks. Those responsible for managing safety and security related risks must work together to identify and mitigate risk.

Many flights around sites may be flown by pilots who are either unaware of the risk that their UAV may be causing or being flown lawfully. Nonetheless these flights may still pose a risk to the site. Legislation to control the flying of UAS is being regularly updated in response to the developing threat and developments in UAS technology. Therefore, it is important to understand how the latest legislation may influence the flights around your sites. [1]

It is essential to have a common understanding of the terms used in completing the VA and the subsequent risk assessment. Many of these are common to all vulnerability and risk assessments and others specific to UAS VAs. Therefore, a glossary is provided on page 21 of the most frequently used terms.

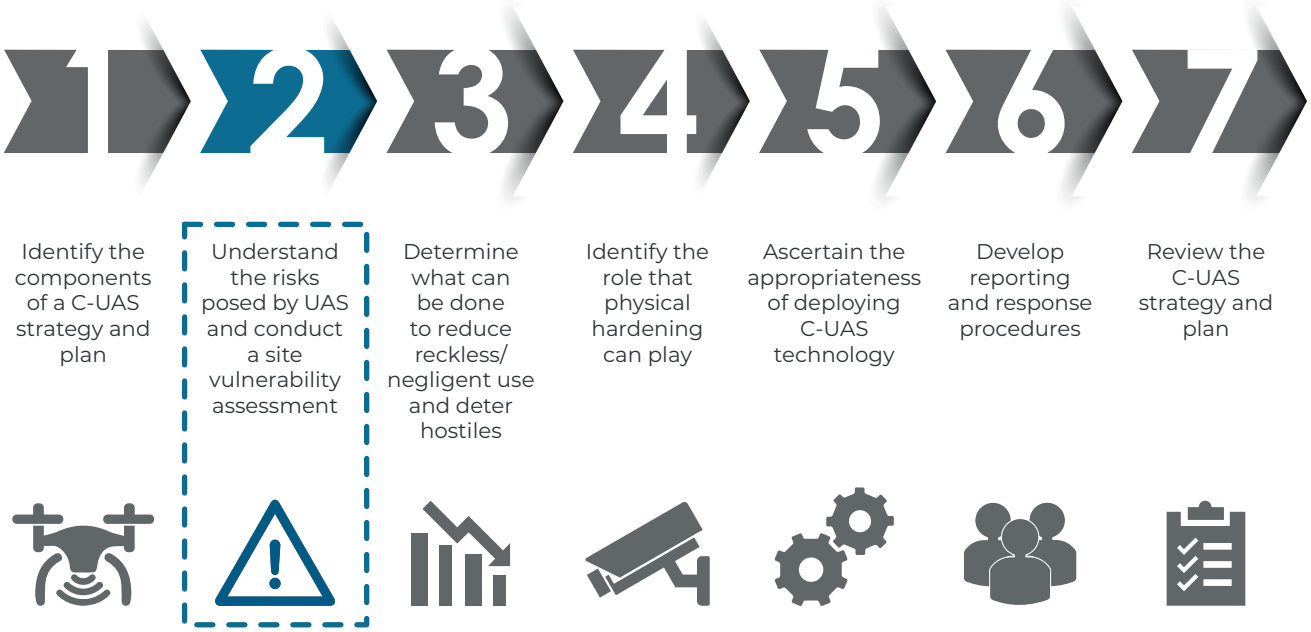
Out of scope

This guidance will **not** provide information concerning a particular methodology for scoring the risk. The information gathered through the VA process should be used to assess the UAS risk within a site's existing risk assessment processes. The VA process is intended to integrate with the NPSA Protective Security Risk Management process[2] , which provides guidance on the end to end risk assessment process.

[1] For the latest UK C-UAS legislation and regulation go to: https://register-drones.caa.co.uk/drone-code/where-you-can-fly [2] https://www.npsa.gov.uk/protective-security-risk-management-psrm-0

High level Vulnerability Assessment (VA) process

Developing a Counter-Uncrewed Aerial Systems (C-UAS) strategy and plan is a complex task involving the seven steps, illustrated in the diagram below. These steps are set out in Countering Threats From Uncrewed Aerial Systems – Making Your Site Ready. The assessment of threat and vulnerability are the second step within this overall process.



The VA is a key step in developing the C-UAS strategy and the plan to manage the risk of UAS incidents. Information will need to be collected before the start of this process. This will include understanding the overall site security strategy and how the development of the VA will inform the C-UAS strategy and plan. It will be important to understand the level of protective security that is already in place at the site. This will include the physical, operational and technical measures in place to mitigate the risk of security incidents generally and UAS risks specifically.

Examples of this may be:

- Assets that are covered from view, e.g. assets hidden by a tree line.
- Assets that are concealed/disguised, e.g. assets disguised by netting.
- Assets that are protected by the design or construction or where the asset is located, e.g. assets that are designed and constructed to be able to withstand the blast of an IED.
- Where information security measures are in place to protect sensitive information.
- Where physical and operational security measures are in place that reduce the vulnerability of assets (CCTV, lighting, netting, patrol, etc.).

This information is likely to be held within the overall site security risk assessment and will be developed further as the vulnerability assessment is completed.

Completing a VA will enable those responsible for sites to gather the information required to assess the risk and identify the measures that need to be taken to mitigate that risk.

This guidance breaks down the VA process into four tasks, illustrated in figure 1. These tasks are described in the following sections. The tasks vary considerably in complexity and, for the benefit of this guidance, are described sequentially. However, as each task is completed, additional information will come to light that may concern the tasks already completed.

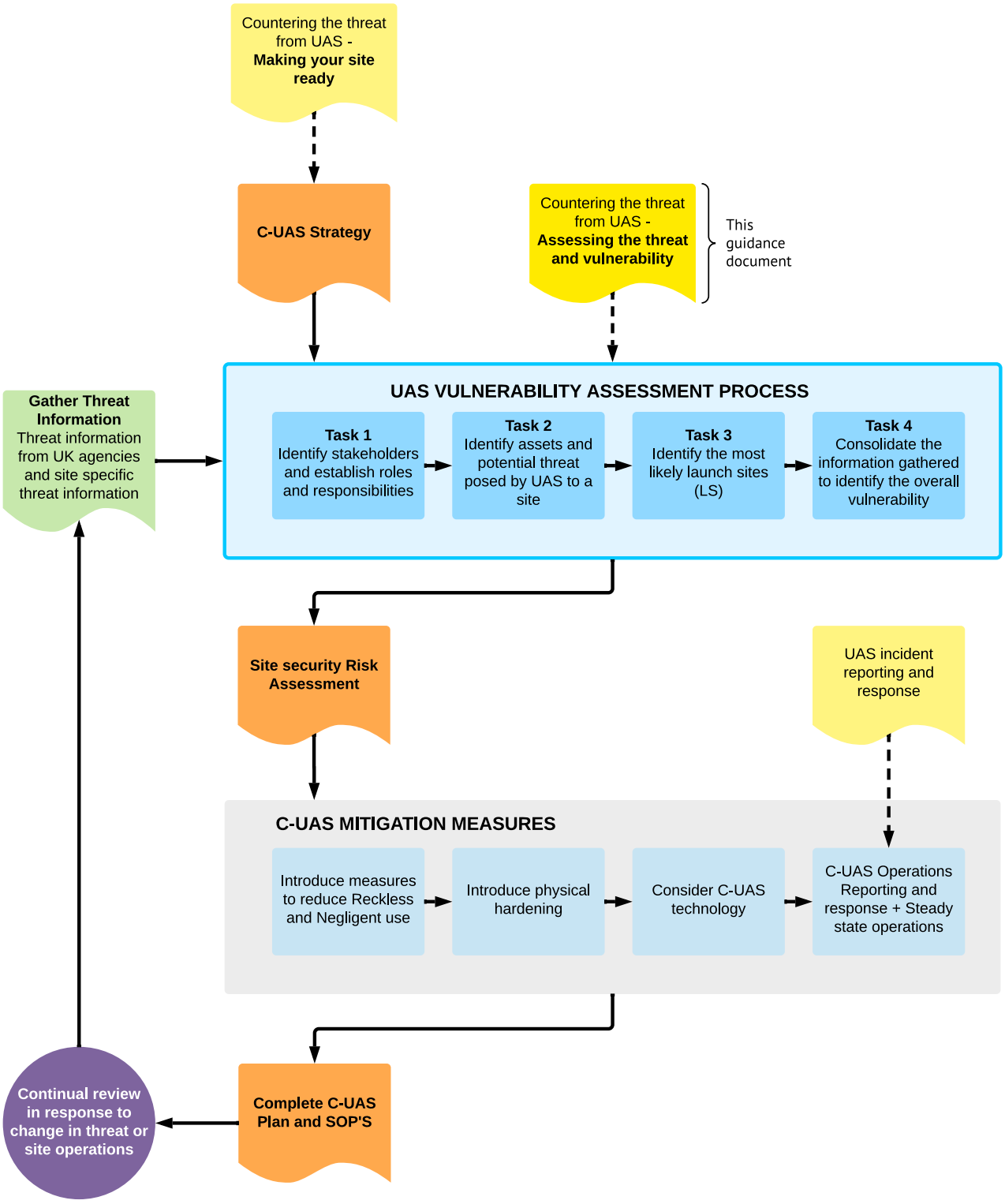


Figure 1 - Vulnerability Assessment Process

As the VA process is worked through, it will generate detailed information that will be used to inform the content of the C-UAS plan and the assessment of the UAS risk.

TASK 1: Identify Stakeholders And Establish Roles And Responsibilities

Time should be spent identifying the key internal and external stakeholders and determining the roles and responsibilities of each.

Consideration should be given as to who owns the risks associated with an unauthorised UAS incident. The ownership of risk may vary depending on the risk scenario and where the risk is manifested. The risk owner should be provided with sufficient resources and information to sufficiently understand and manage the risk.

Internal stakeholders

The internal stakeholders that need to be involved will vary at each site. These are likely to include those responsible for the site's assets, health and safety, site operations and senior decision makers. As a site's key assets are identified and assessed it is important to engage and involve the individuals who are able to identify how each asset works, describe exactly how they are likely to be vulnerable to UAS threats and help develop effective mitigations.

External stakeholders

Whilst the ownership of the risk to the site may remain with the senior risk owner, it is vital to understand the role other organisations may play in both adding to and mitigating the risk. Time should be spent identifying other external stakeholders. These may include:

- The police.
- Local authorities that may need to be involved in the process as a result of either their ownership of adjacent land, management of the transport infrastructure or as the planning authority.
- Those responsible for local public transport, such as rail and bus operators.
- Neighbouring businesses and other organisations.
- Other local land owners whose land the pilot may choose to launch an UAV from.
- Local flying clubs who may be operating nearby.

The Police

The police will have a very important part to play. The role they already play in patrolling, responding to incidents and conducting criminal investigations must be understood.

The police may be able to provide intelligence in relation to local, national and international threat reporting. This information can be used to help identify the most relevant threat scenarios to each site. Depending on the nature of your site they may be able to support you in the identification of the most likely Launch Sites (LS). Once the VA is complete the police may be able to continue to help inform the likelihood of a threat scenario taking place at a site and identify new and developing threats that should be added to the process. For detailed information contact your local police force Counter Terrorism Security Advisor. They can then decide how they can support your request.

Your local police force may also operate their own UAS in the vicinity of your site and it will be important to have a way to deconflict this activity against any reported sightings.

TASK 2: Identify Potential Threats Posed And Critical Assets

This section will progress through five steps, figure 2. The first three collectively create the threat picture relevant to the site (**who**, **how** and with **what**), whilst the fourth step identifies the assets likely to be targeted (**where**) within the site that the threat may be focused. These outputs are a critical element in understanding the overall UAS risk and providing the tools to go forward in accurately planning how to mitigate it. The threat scenarios in task 2. 5 summarise this for future work.

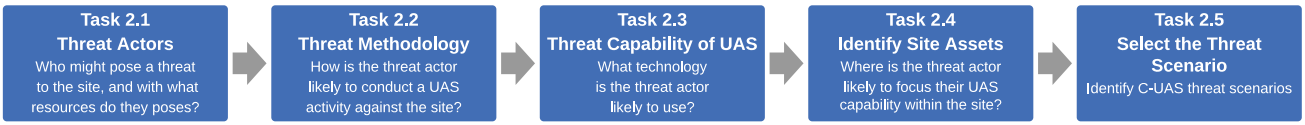


Figure 2 - Five steps of Task 2

The information gathered during this process will be used to help assess the vulnerability and risk, illustrated in figure 3.

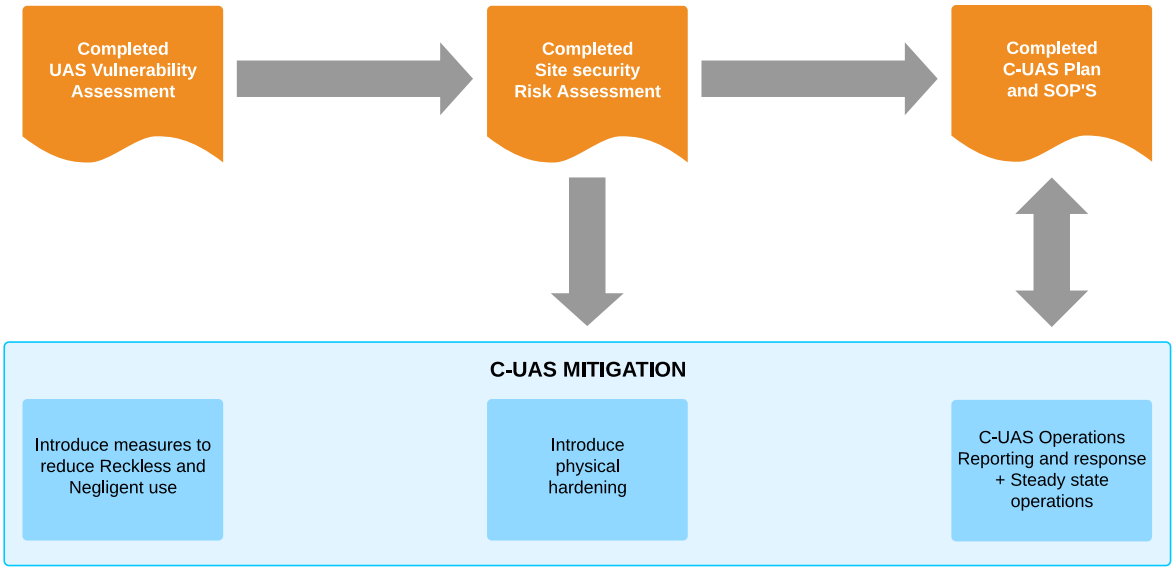


Figure 3 - Vulnerability and Risk assessment

The information collected concerning the capability of both the threat actor and the UAS used to deliver any threat will play a crucial part in identifying the most likely threat scenario and the resulting requirement for any C-UAS mitigations.

Task 2.1 Identify the Threat Actors

A number of different threat actors could use a UAS to deliver a security threat of concern but their approaches, methods and equipment may vary significantly. It is necessary to consider what type of threat actor may try to deliver a threat at a site. Examples of threat actors include:

- Reckless or negligent users
- Journalists and others conducting unauthorised surveillance
- Unlawful protesters
- Serious and Organised Criminals (SOC) / Criminals
- Terrorists
- Hostile State Actors (HSA)

The capability of the threat actor should be considered. A reckless or negligent user will likely have limited skill or knowledge of how they can maximise the performance of a UAS. However, HSA are likely to be highly skilled, operate UAS to their full potential, and have an enhanced awareness of security measures protecting sites. Accordingly, an assumption will be made about the capability of the operator when identifying LS.

Site operations and trends in UAS use

An assessment of the UAS threat should include:

- Obtaining threat information concerning local, national and international hostile and reckless UAS activity from your local police contacts, NPSA adviser and other partner agencies.
- Understanding the overall security threat to the site from all security threats and considering how a UAS could deliver those threats. Using a UAS to deliver the attacks may distance the attacker from existing security measures.
- Gathering historic information about suspected hostile, reckless or negligent and legitimate UAS activity in and around the site.
- Analysing information from any Detect, Track and Identify (DTI) capability that has been installed at the site. The information gathered may only provide a partial picture of UAS activity.

It is essential to recognise that the threat presented to a site from a UAS may emanate from a person who has no intention to cause harm or damage at the time of the flight, they are simply reckless or negligent in their actions. These flights can impact safety or security as much as a flight flown by a pilot with malicious intent. Recent examples of such flights have occurred adjacent to several international airports or major event sites.

Task 2.2 Identify Threat Methodology

UAS have been seen to be used by threat actors to deliver a number of different threat methodologies. They have been increasingly used by terrorists in conflict zones and extensively used by criminals to smuggle drugs and other prohibited items into UK prisons. Their use in protest has been limited to date. There are also a number of notable occasions (Gatwick Airport incursion 2018) when it has not been possible to identify the pilot or their intention even after a thorough investigation.

Some examples of the methods of how UAS can be used are set out below. However, it should be noted that this is not a definitive list and should only be used as a guide. Some incidents can be seen to fit within several different methods, as set out in table 1. It is also reasonable to assume that as UAS use continues to grow, the threats they are used to deliver will also develop.

UAS provide threat actors with some key capabilities over other more traditional methodologies. These will include the ability to:

- Fly across perimeter security measures into otherwise secure areas.
- Remotely deliver a range of threats with low likelihood of being detected by traditional security measures.

The threat methodologies that should now be considered are as follows:

DISRUPTION – Flying over or near the site and preventing site operations from continuing as normal. For the purposes of protest or nuisance. This may include a prolonged disruption caused by an extended flying time.

SURVEILLANCE – Flying over or stationary (perch and stare) near the site to gather information, either obtaining images or data. This may involve the use of a camera, microphone or other electronic means.

DELIVERY OF A PAYLOAD – Delivering or removing an item. Delivering restricted, illegal or illicit items into a controlled area or removing property from a secure site.

USING A UAV AS A KINETIC WEAPON -The UAV can either be unmodified or modified (I.e. addition of a payload) to enhance the weapon's effect.

CYBER-ATTACKS – Cyber related threats involve the use of a UAS to deliver malicious attempts to damage or disrupt services and networks, including IP theft.

In order to select which methodologies may be most likely to occur at a site it is necessary to consider what activities are taking place at or adjacent to the site and why they could make the site a target for unauthorised UAS activity. The following key questions must be answered within this process:

- Why would an attacker prefer to use a UAS to undertake an attack rather than use any other attack methodology?
- How and why is the site more vulnerable to a UAS attack than any other attack methodology?

Location	Date	Threat Methodology	Actor	Threat actor / Scenario	Type of attack
Coast of Oman	07/2021	UAV as a weapon	HSA	Mercer Steet oil tanker strike	State sponsored FW UAVs used for kamikaze explosive strike
Jammu Kashmir India	06/2021	Delivery of a payload	Terrorist	Terrorist organisation operating in Pakistan, reported to have used UAVs to attack an airport in Jammu Kashmir. Previously, they used UAVs to smuggle weapons and explosives across the border into India.	Large RW UAVs used to smuggle weapons deliver explosive attacks.
Newmarket England	05/2021	Surveillance	Criminal	Male charged with breaching flight regulations having flown a UAV at Newmarket Racecourse. Believed the intention was to gain an advantage when placing bets.	COTS medium RW flown in breach of CAA regulations
Edinburgh Scotland	01/2021	Delivery of a payload	Criminal	Criminal activity. Male convicted of attempting to fly a mobile phone into a maximum security prison using a UAV	COTS small RW UAV used to carry payload.
Saudi Arabia	09/2019	UAV as a weapon	HSA	UAVs were used to attack oil processing facilities at Abqaiq	State sponsored FW UAVs used for kamikaze explosive strike
Heathrow London	09/2019	Disruption	Protestors	Extinction Rebellion Protestors planned to fly UAVs into Heathrow Airport as part of a protest.	COTS small RW UAV flown into controlled area.
Christchurch New Zealand	03/2019	Surveillance (HR)	Terrorist	Far right extremist shot dead 51 people after conducting an MTA at 2 mosques. During the trial, it was revealed attacker used a UAV to conduct reconnaissance two months before the attack.	COTS RW UAV used for reconnaissance to maximise impact of MTA.
UK	12/2018	Disruption	Unknown	Hundreds of flights were cancelled at Gatwick Airport near London, England, following reports of drone sightings close to the runway	Intent of pilot never established. However, believed to be to cause disruption. Details of UAS not known.
Venezuela	08/2018	UAV as a weapon	Unknown	Two UAVs allegedly laden with explosives flew towards Venezuela's president, in a reported assassination attempt while he was speaking at a military parade.	Large RW UAVs with IEDs used in a reported assassination attempt.
Tabqa Syria	08/2014	Surveillance (HR, Coordination of Attacks, Propaganda)	Terrorist	Islamic State used UAVs for attack planning or propaganda purposes. For example, IS militants used UAV footage to survey the Tabqa military airfield, a key Syrian air base that the group later captured.	COTS RW UAVs used for surveillance and reconnaissance to support attack planning.

Table 1 - Examples of previous UAS incidents

Task 2.3 Threat Capabilities of UAS

Having gained an understanding of the level of ability of the actor (from Step 1) and the threat methodology they may use in (Step 2), an estimate can now be made of the type of UAS that will be used to deliver that threat. They are either described as rotary wing (RW) or fixed wing (FW) as illustrated in figure 4. The capability of the multiple different models of UAS that are readily available to purchase will vary considerably. This will include:

- The payload they can carry.
- The speed they can travel.
- The amount of flying time their battery enables.
- The range they can operate up to.
- The operating environment. (UAS operating in open rural areas may perform closer to the manufacturers claimed specifications when compared to complex and or urban environments where performance may be reduced).

ROTARY WING

- ➕ Easy to control and manoeuvre
- ➕ Can hover, perch and stare
- ➕ Can fly vertically and horizontally
- ➕ More compact size
- ➕ Small area required to launch
- ➖ Limited endurance
- ➖ Less stability in the wind
- ➖ Lower flight speeds

FIXED WING

- ➖ Higher skill to operate
- ➖ Unable to maintain fixed position
- ➖ Can only fly horizontally
- ➖ Less compact size
- ➖ Larger area required to launch
- ➕ Longer endurance
- ➕ Greater stability in the wind
- ➕ Greater flight speeds

Figure 4 - Types of UAS

Task 2.4 Identification of the site assets

A fundamental part of the VA process is to identify the assets that are critical to the operation of a site and assess how vulnerable they are to a UAS threat. A critical asset is anything an organisation deems critical to its success or continued operation and may include:

- Physical items, such as buildings, equipment and products created or held on the site.
- Information, data stored or transmitted in any format (hard or electronic copy)
- Individuals with unique knowledge and/or skills for which there is limited supply and organisational reliance.
- Services provided from a site.
- Large groups of people creating crowded places.

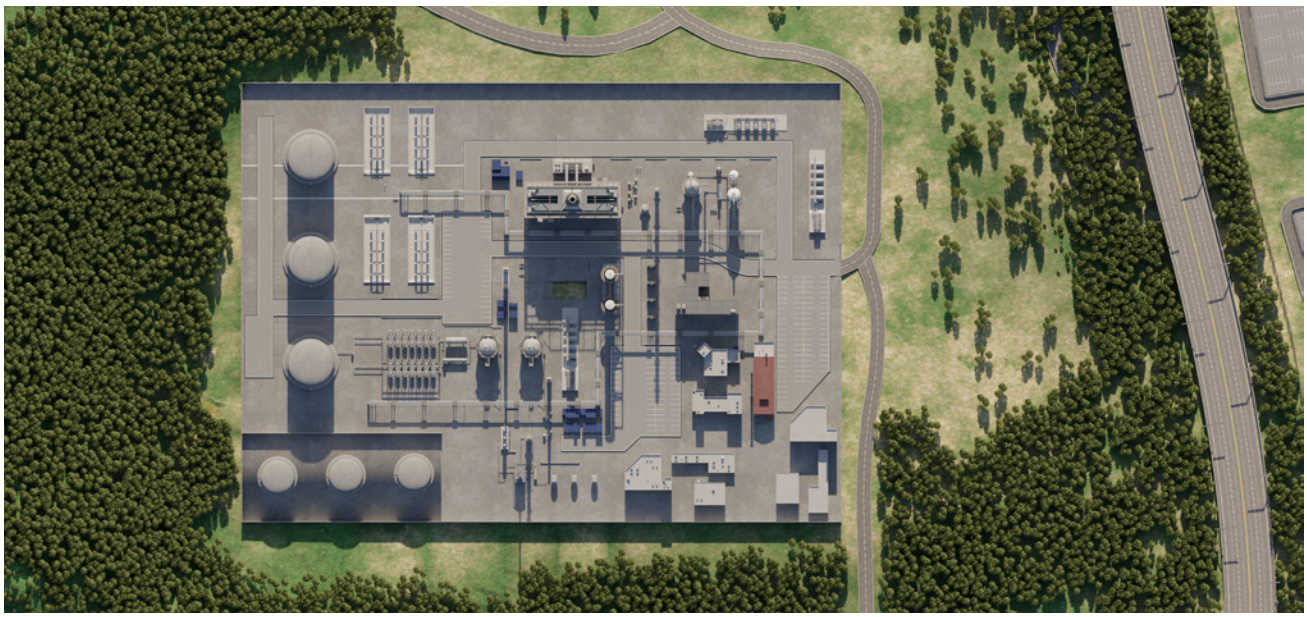
Each site is likely to have multiple assets. It is therefore important to focus this process on the assets, that if compromised, would have a significantly detrimental impact on the operation of the site. These are identified as critical assets.

The assets may be located either inside or outside of the perimeter of the site.

Once assets have all been identified, the information collected should be collated, and the location plotted on a map.

Task 2.5 Select the threat scenarios suitable to the site

As a summary of the threat picture, threat scenarios provide an effective planning tool for subsequent risk assessment and mitigation work. Having developed an understanding of the UAS threats that are relevant to the site and identified the critical assets, consideration should be given as to how the threats identified are likely to impact against each of the critical assets.



TASK 3: Identify the most likely Launch Sites (LS)

One of the most useful outputs of the VA process is the identification of likely Launch Sites (LS), as these can directly drive practical steps to reduce the risk to a site and effectively focus mitigation methods. This task is split into the three tasks as shown in figure 5.

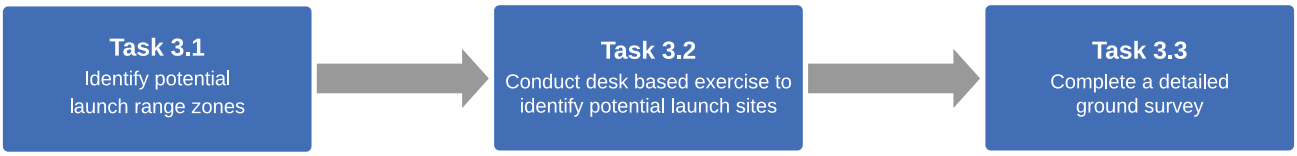


Figure 5 - Three Steps of Task 3

There are mapping software tools that are available to support the Launch Site Survey (LSS). Under certain circumstance your local police contacts may be able to support you in completing the survey. The involvement of the police in this stage of the process will be of benefit in enabling them to inform their response to any UAS incident at the site.

Task 3.1 Identify potential launch range zones

Each threat scenario should now have likely LS parameters associated with it. These can now be used to Identify potential launch range zones for each scenario. This effectively reduces the amount of space around the site that is assessed as likely to be used for UAS launch. These will define:

- If the pilot is likely to need to operate with a clear Line of Sight (LoS) from the LS to the asset or the LS to the UAV.
- If the pilot is likely to operate overtly, obscured or covertly from view.
- The launch range zone, the distance from the asset they are likely to fly from.

The area surrounding the asset from within which a UAV is most likely to be launched is defined as the Launch Range Zone (LRZ).

The LRZs may be broken down into several likely Launch Sites (LSs) where it is assessed that the UAV will most likely be launched. The selection of LS is explained in section 3.

Task 3.2 Conduct desk based exercise to identify potential launch sites

Once the likely launch range zones have been identified, a desk based exercise should be conducted to identify the likely LSs. The potential LS will be identified using a map marked with the LRZs and the local knowledge of the stakeholders involved, as illustrated in image 1. This exercise aims to identify as many LS as possible in advance and save time when out on the ground conducting the ground survey.

As this exercise and the subsequent ground survey are completed, it should be noted that this is not a definitive solution. For example, if a launch range zone is plotted and a suitable LS is identified that sits just outside a range zone, then that site should still be included within the assessment.

In addition, there is a risk that a pilot may launch from beyond the 500m, 1000m, or 1500m zones selected. This may involve a pilot with a higher level of skill and competency flying a more sophisticated UAS.

Some sites in rural areas may have a large area from which a UAV could be launched from multiple sites. Others in urban areas may have a minimal number of potential launch sites. Conducting the VA will help sites identify the most vulnerable LSs close to the perimeter of the site. These sites will afford the least amount of detection and reaction time.

Image 1 - Potential launch sites identified

Task 3.3 Conduct ground survey to confirm most likely LSs

A detailed ground survey should now be conducted of likely launch sites. Each site should be visited and a search made for additional sites which have not previously been identified.

Consideration should always be given to the ownership of the land on which potential LSs sit and permission should be sought from the land owner before visits are made onto private property.

A record should be made as to why each LS may be suitable and the measures that are in place to prevent UAVs being launched and landed. This will enable the identification of the LS identified as being the most likely to be used.

TASK 4: Consolidate The Information Gathered To Identify Overall Vulnerability

A considerable amount of information will be gathered as the steps are completed.

The information gathered will include:

- The key assets vulnerable from a UAS.
- The UAS threat actors and scenarios considered relevant to the site.
- The potential Launch Sites (LS) and flight paths.

In addition the detailed information gathered during the VA can now be used to inform the development of the C-UAS plan and the assessment of the UAS risk.

This information can be incorporated into mapping systems used to support the command and control of UAS incidents. This will enable sites to readily visualise the critical assets and likely launch sites and share key information with the police and other partners.

- **Understanding the threat and risk from UAS incidents to a site.**
  The information gathered will enable an assessment to be made of which specific threats present the greatest risk to the site. The site security risk assessment process will introduce an assessment of:
  - The impact of an asset being attacked and
  - The likelihood of that threat event occurring.

  The site security risk assessment process will produce a risk score which will then allow decisions to be made as to whether the risk identified is acceptable. It will enable a comparison to be made between all UAS risks and other security risks that have been identified for the site. This will ensure that any UAS mitigations introduced are proportionate to the overall level of security presented at the site.
- **The measures required to reduce reckless and negligent UAS activity.**
  A baselevel of C-UAS measures should be in place that will reduce the risk of reckless and negligent flights taking place. This process will identify weaknesses and where additional measures may be required to bolster the base level of mitigations. The process will focus the introduction of additional measures towards either the launch sites that are most likely to be used or the assets that are most vulnerable.

- **The requirements for C-UAS technology.**
  Only once the threat and risk to the site is understood and non-technical measures have been optimised should C-UAS technology be considered.
- **The response procedures triggered in the event of a UAS incident.**
  The VA will enable the response procedures to be informed by the identified threat scenarios. This should enable a rapid and carefully considered incident response. The LSs that have been identified should be used to inform the response to suspected UAS sightings.

Ongoing review

Once this process is completed for the first time the information should be reviewed regularly.

It should be reviewed and updated as:

- Mitigations are delivered to show the level of risk that now remains.
- New threats materialise across the world.
- The use of the site changes.
- Part of the post-incident review process.
- UAS capability develops.
- UAS incidents occur on the site, similar sites across the UK and CNI sites around the world.
- Other non-UAS specific security measures are changed.

Completing the VA is an important task, and depending on the nature of the site being assessed, it may take a considerable time to complete. Further guidance may be obtained from your NPSA adviser and local police force.

Glossary of Terms

Beyond Visual Line Of Sight (BVLOS)	Pilot is unable to see the UAV.
Catalogue of Security Equipment (CSE)	Provides a range of products that have been evaluated against specific NPSA security standards and the performance rating achieved.
Counter-Uncrewed Aerial System (C-UAS)	Measures taken to mitigate the threat of unauthorised UAS activity.
Critical Asset	An asset can be a person or group of people (crowded place), the premises they occupy, the products and services they supply and the information and intellectual property they have. Assets can be physical and digital and be vulnerable in multiple different ways. A critical asset is anything an organisation deems critical to its success or continued operation.
Detect Track and Identify (DTI)	Detect is the ability to sense and classify the presence of a UAS. Track is the ability to determine the UAS position and movement over time. Identify is the ability to determine the size and type (fixed wing, multirotor) of a UAS.
First Person View (FPV)	First Person View flying is the ability to control a UAV from a “pilot’s eye” perspective through the use of an on-board camera and ground-based receiving and viewing equipment. The viewing equipment is normally a set of video goggles or video screen.
Flight path	A single path depicting where an aircraft intends to fly.
Geo-fencing	Geo-fencing is a virtual barrier around predefined areas of airspace. It is manufacturer specific and therefore has no effect against UAVs manufactured by someone else.
Ground Control Station (GCS)	Allows the pilot to remotely control and or monitor the operation of the UAV.
Global Navigation Satellite System (GNSS)	A satellite system that is used to pinpoint the geographic location of a user’s receiver anywhere in the world.
Launch Range Zones (LRZ)	The general zone from the asset that a UAV is likely to be launched within. Shown by a concentric shape marked at 500m, 1000m, and 1500m from the asset.
Launch sites (LS)	A specific space within the LRZ from which a UAS is likely to be launched as a result of the particular geographic location in relation to a set of known criteria.
Line of Sight (LoS)	A straight line along which an observer has unobstructed vision.

Reckless or negligent	Disruption caused by users who are simply unaware of the regulations and fly their UAS in a negligent or reckless manner that may unintentionally cause danger or disruption.
Radio Frequency (RF)	The commonly used communications bands that a UAS uses to communicate between the GCS and the UAV.
Risk	Risks are identified threats, aligned to assets and their vulnerabilities, that have been assessed for likelihood (of the threat event occurring) and impact (to the organisation and/or third parties) should the threat transpire.
Risk appetite	The level of risk that an organisation will tolerate. In some cases, a temporary loss of service or capability may be acceptable; in others, a service may be deemed business critical and cannot be allowed to fail.
Steady State Operations	The period of time when a site is operating under normal conditions and there is no live threat identified. Operational and technical capabilities are running to detect and deter attacks.
Threat	An intention to cause harm. Consider threats from across the full spectrum of threat actors, and also how these threats might overlap or evolve over time.
Uncrewed Aerial System (UAS)	UAS is used interchangeably with; drone, uncrewed aircraft (UA) or Remotely Piloted Aircraft System (RPAS). The UAS is comprised of the UAV, GCS and a bi-directional link between the UAV and the GCS that provides control, status and imagery information.
Uncrewed Aerial Vehicle (UAV)	Aerial Vehicle that can operate without a pilot being on board.
Vulnerability	How inherently prone an asset is to the threat. Any weakness that can be exploited by an adversary to gain access and damage or steal an asset or disrupt its critical function.
Visual Line of Sight (VLOS)	Pilot is able to see either the asset or the UAV from the launch site.