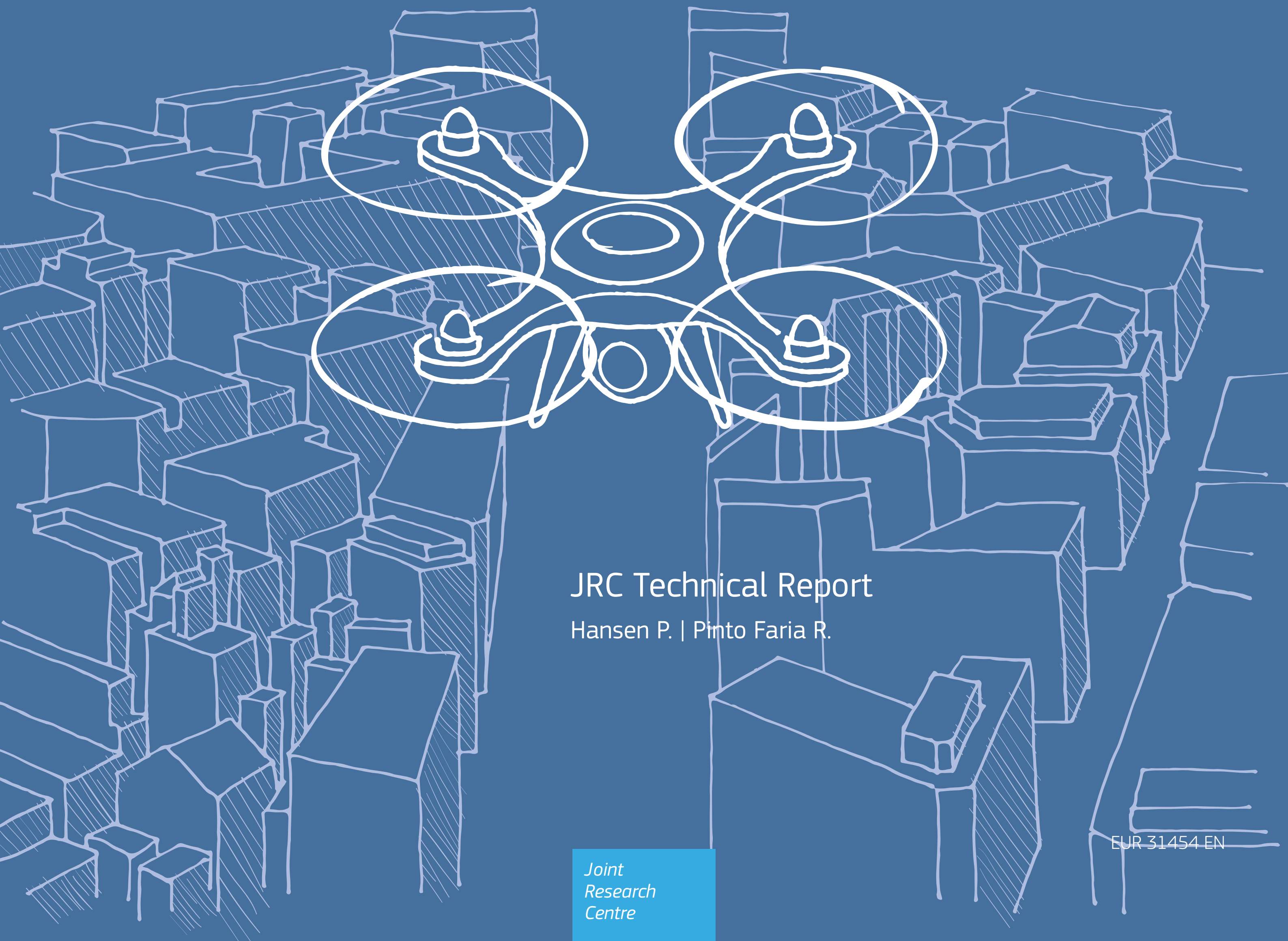
ISSN 1831-9424

European Commission

Protection against Unmanned Aircraft Systems

Handbook on UAS protection of Critical Infrastructure and Public Space: A five Phase approach for C-UAS stakeholders



JRC Technical Report

Hansen P. | Pinto Faria R.

EUR 31454 EN

Joint Research Centre

This publication is a technical report by the Joint Research Centre (JRC), the European Commission's science and knowledge service. It aims to provide evidence-based scientific support to the European policymaking process. The contents of this publication do not necessarily reflect the position or opinion of the European Commission. Neither the Commission nor any person acting on its behalf is responsible for the use that might be made of this publication. For information on the methodology and quality underlying the data used in this publication for which the source is neither Eurostat nor other Commission services, users should contact the referenced source. The designations employed and the presentation of material on the maps do not imply the expression of any opinion whatsoever on the part of the European Union concerning the legal status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries.

Contact information

Name : HANSEN Paul (JRC-GEEL)
Address : European Commission
Joint Research Centre
Retieseweg 111
2440 Geel
BELGIQUE/BELGIË

Tel.: +32 (0)14 571 485
Email: JRC-DRONE@ec.europa.eu

EU Science Hub

https://joint-research-centre.ec.europa.eu

JRC132714
EUR 31454 EN

Print	ISBN 978-92-68-06614-0	ISSN 1018-5593	doi:10.2760/747997	KJ-NA-31-454-EN-C
PDF	ISBN 978-92-68-01253-6	ISSN 1831-9424	doi:10.2760/18569	KJ-NA-31-454-EN-N

Luxembourg: Publications Office of the European Union, 2023

How to cite this report: Hansen, P., Pinto Faria, R., Handbook on UAS protection of Critical Infrastructure and Public Space: A five Phase approach for C-UAS stakeholders, Joint Research Centre, Publications Office of the European Union, Luxembourg, 2023, doi:10.2760/18569, JRC132714.

Protection against Unmanned Aircraft Systems

Handbook on UAS protection of Critical Infrastructure and Public Space: A five Phase approach for C-UAS stakeholders

JRC Technical Report

Hansen P. | Pinto Faria R.

Contents

Abstract

An effective counter unmanned aircraft systems (C-UAS) solution needs collaboration from many stakeholders to agree on processes and procedures. This handbook was developed by the European Commission's Joint Research Centre (JRC) and is based on the experience gained in its DRONE project [1]. The recommendations were developed through a collaboration project. The recommendations in this handbook are supported by targeted consultations and workshops with key stakeholders such as law enforcement agencies (LEAs), authorities, regulators and technology companies.

The handbook provides advice on how to protect against malicious UAS and provides guidelines, references, approaches and considerations. It covers detection, tracking, identification and neutralisation through the processes of risk analysis, solution design, implementation and operation of a solution. It explains the importance of combining systems and processes with the involvement of stakeholders to create a complete solution.

This handbook is a key component of the Commission's C-UAS package, announced as a flagship action under the Commission communication 'A drone strategy 2.0 for a smart and sustainable unmanned aircraft eco-system in Europe' [2]. This package includes a dedicated C-UAS communication, outlining the main ideas for the EU's future policy on how to address the potential threats posed by UAS. As part of the drive to provide continuous practical support to EU Member States and stakeholders, the JRC has produced two handbooks; the first is this five-phased approach to developing a C-UAS solution, while the second contains a series of recommendations for assessing the risks stemming from the malicious use of UAS, complemented with advice regarding the physical hardening of non-military infrastructures against such threats.

[1] EU Science Hub, https://joint-research-centre.ec.europa.eu/scientific-activities-z/drones-counter-drones-and-autonomous-systems_en.

[2] Commission communication – A drone strategy 2.0 for a smart and sustainable unmanned aircraft eco-system in Europe, COM(2022) 652 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022DC0652.

Introduction

In Europe, and the rest of the world, the use of UAS (commonly referred to as drones) is increasing. Common services [3] for UAS have been defined to increase use across sectors such as agriculture, transport, survey and surveillance, see figure 1. The EU's safety framework for operating and setting the technical requirements of unmanned aircraft harmonises the European UAS market and should increase applications, development and services linked to UAS.

While UAS can offer valuable opportunities for commercial applications, there is also potential for misuse. UAS can be used to breach privacy rules, for espionage by using camera technologies, to hijack telecommunication signals and, in combination with biological or chemicals agents, explosives or other weapons, they can harm persons, disrupt services and damage infrastructure.

Although most non-cooperative use of UAS would probably fall under the category of non-intentional (careless or clueless), it should not be excluded that criminals and terrorists might increasingly misuse UAS to target public spaces, individuals and critical infrastructure (CI). This trend has already been seen across the world where UAS were used in terrorist attacks. The *modi operandi* and the targets of UAS incidents are so different that countermeasures must include both active and passive elements.

While EU regulations have made it safer to use UAS and at the same time more difficult to misuse certain types of UAS, the rapid pace of innovation and easy access to UAS mean that incidents are likely to increase even more. With the frequency and impact of these incidents increasing [4], the need for preventive countermeasures and preparedness is particularly important for CI owners and managers of public spaces.

Many UAS and components that can be modified for a specific malicious purpose are available on the market. There is, therefore, a need for countermeasures to control non-collaborative or malicious use of UAS.

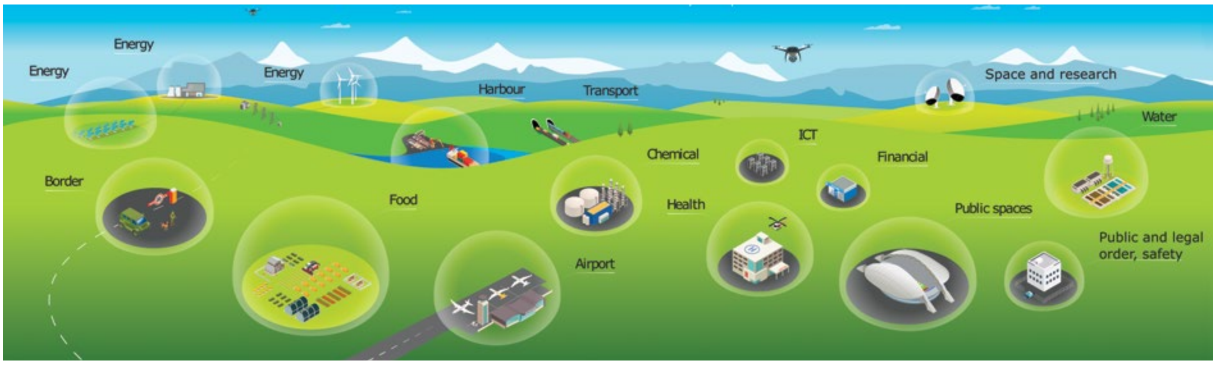
[3] https://www.sesarju.eu/U-space.

[4] https://transport.ec.europa.eu/system/files/2022-11/SWD_2022_366_drone_strategy_2.0.pdf

Scope and objective of this handbook

This is the first edition of what can be considered a living document covering a fast-evolving area. The Commission will closely follow the relevant regulatory, procedural and technological developments and update the handbook, when necessary, in the years to come.

Figure 1: A selection of critical infrastructure types for which this handbook provides recommendations



This handbook does not contain an extensive overview of available C-UAS techniques and technologies. Instead, it provides a methodology and advice to evaluate the needs of a C-UAS solution and how to design and implement this. It provides guidance on how to determine the most appropriate solution and offers an approach to implement and operate such a solution.

While there are lots of similarities between solutions, it is also clear that no ‘silver bullet’ C-UAS solution exists and probably no solutions will be identical. The recommendations are generic enough to represent a sound basis for developing further solutions that currently do not exist.

The getting started, design and installation phases were tested and verified in the project as part of the proof of concept in the JRC DRONE project, which includes a living lab on the JRC Geel site. The recommendations regarding the installation and operation phases are based on common project and solution-implementation principles. The handbook recommendations are the foundation of the C-UAS living lab, which will be open to stakeholders to identify regulation needs, organise processes and procedures and to optimise C-UAS solutions.

Five-phased approach to a C-UAS solution

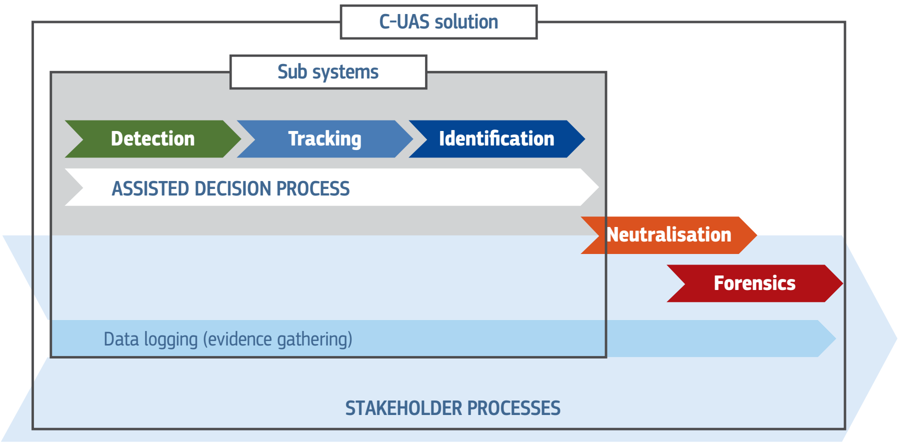
It is clear that C-UAS is a challenging task and that no 'silver bullet' implementation is available, meaning there will most likely be no standard implementation or identical solutions. Each solution will need to be adapted to the needs of a particular site and its environment. There are, however, elements that are common and all implementations will benefit from the recommendations described in this document.

Where commonly C-UAS covers detection, tracking, identification and some neutralisation, the methodology described here advises that event logging also be included and, very importantly, the processes linking this to the stakeholders be involved at all levels. Event logging is often overlooked, but it is essential for forensics and post-event analysis.

A complete solution should cover the complete C-UAS value chain, see Figure 2. Many implementations need a system or systems to be combined with processes and procedures of the stakeholders involved. This handbook guides readers to understand each aspect and guides them through five phases to achieve a solution. Each phase contains recommendations and elements that need to be done before, during and after the phase.

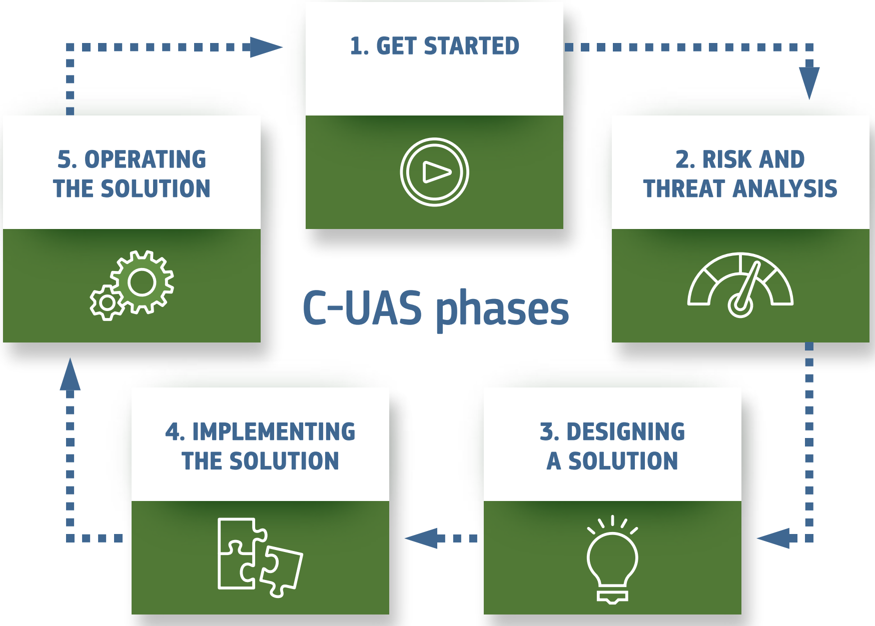
This section covers the difference between a C-UAS solution and a C-UAS system and why one should implement a solution. Figure 2 shows the complete value chain used in this handbook.

Figure 2: C-UAS solution value chain



The following section describes the recommended phases for the implementation of a solution. Each of the phases begins with a list of elements that is needed to complete the recommendations of the specific phase. These are to be complemented with site-specific information. At the end of each section, there is a summary of what was addressed and what is needed to move to the next phase. It is recommended that these phases are taken in consecutive order. The recommended process to obtain a solution is shown in Figure 3.

Figure 3: The five phases in the C-UAS solution development process


1. GET STARTED
2. RISK AND THREAT ANALYSIS
3. DESIGNING A SOLUTION
4. IMPLEMENTING THE SOLUTION
5. OPERATING THE SOLUTION
C-UAS phases

The reader will see what elements to complete and which stakeholder should be involved to complete these actions. These actions will be needed later in the processes or phases.

Clearly no solution can be considered static, and it should evolve with changes to needs, sites, threats and stakeholders. As changes can be temporary or permanent and occur at any time, the solutions must be closely monitored, and each step repeated when needed. Following this methodology will make changes more structured.

An overview of the five phases is given below.

1. Get started with C-UAS phase. This phase describes the first recommended actions when investigating the need for a C-UAS solution and sets the principles, goals and requirements for the rest of the project. In many cases, there is a need to complement internal competences with consultancy.

    - The business case and need to get started.
    - The mandate to be followed.
    - Where, who and what to protect against.
    - Identify the stakeholders and define roles and responsibilities.
    - Identify the legal base to start an implementation.
    - Collection of site-specific information. Determine what authority is there to enforce, who are the airspace managers, maps, plans, insurance, etc.
    - Allocation of the budgetary framework for starting the process.

2. The risk and threat analysis phase investigates, analyses and documents the site's UAS risks and threats to establish a threat-response plan. This plan serves as a key input to the countermeasure selection process.

   - Identifying whom to protect against.
   - Understanding the risks and investigating how these can be integrated into current risk plans.
   - Defining the UAS risk in scenarios.
   - Identifying the site's critical assets that are vulnerable to UAS.
   - Site survey.
   - Regional factors. Are there activities close to the CI, close to borders, development of UAS services in the area?
   - What are the macro risks the CI is trying to protect against?
   - Choosing the appropriate mitigation level to the risk and objective of the solution.
   - Creation of a site threat-response plan.

3. The solution design phase matches the threat-response plan to the use of technologies and stakeholders processes to effectively counter the UAS risk. The site-specific information and needs will be incorporated in the design. The design will be matched with test and verification processes. This will include solution and technology test plans.

   - Merge the site specifics with needs, risk and threats.
   - Define clear roles and responsibilities of all the stakeholders.
   - Define how to test the solution and train stakeholders.
   - Implementation of the foundational minimum services.
   - Selection technology components that will enable the mitigation needed.
   - Detail the design into an architecture.

4. The solution implementation phase provides guidance on how the solution to be implemented will look at different considerations during implementation. This phase describes how to use the design and provides guidance on what will help implement the solution in collaboration with stakeholders.

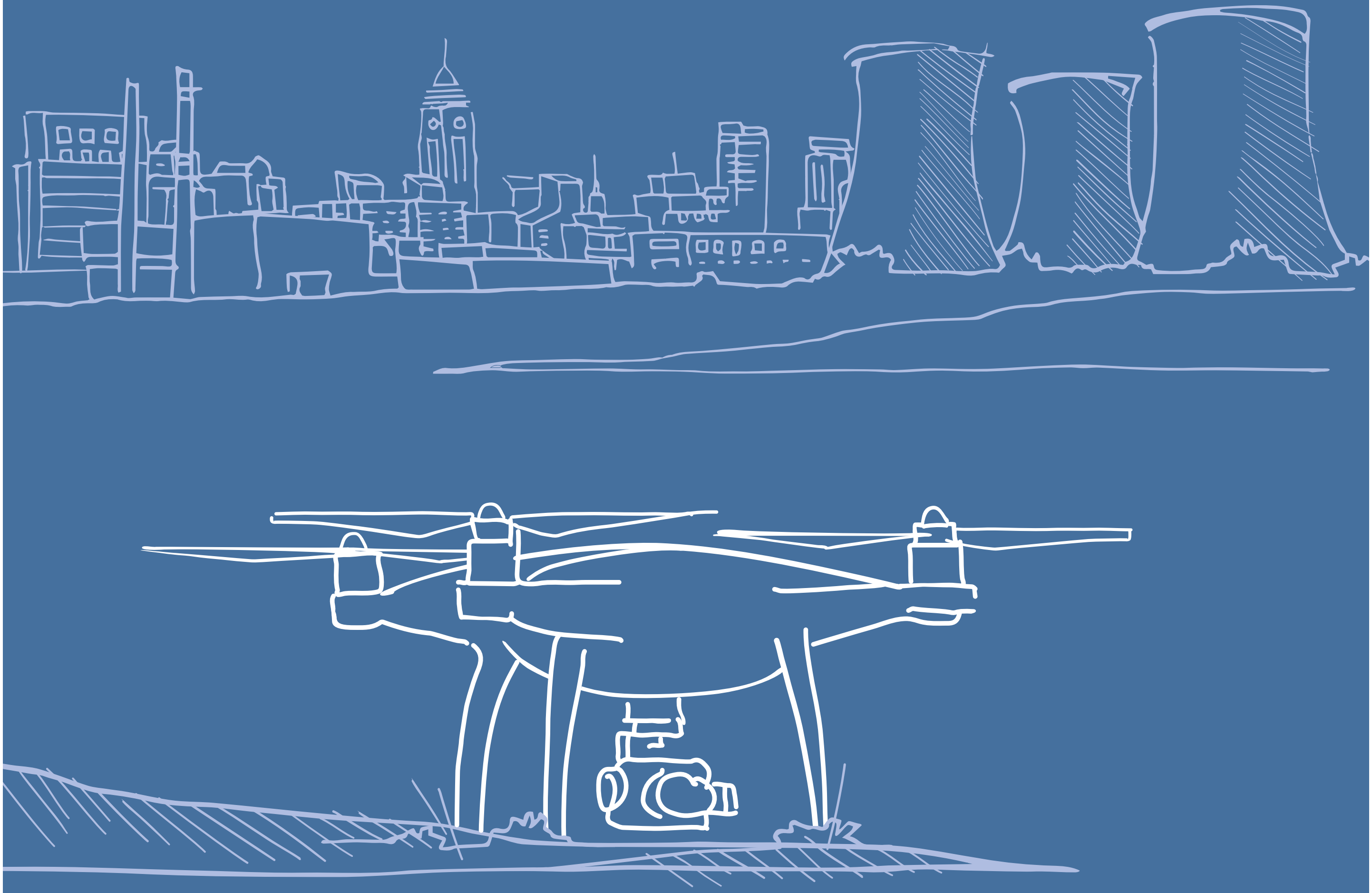
   - Installation of the solution.
   - Penetration tests.
   - Equipment calibration and testing.
   - Set-up of post-implementation operation plans and solution acceptance criteria.
   - Solution acceptance criteria and testing.
   - Operation manuals and transition to service mode.

5. The operation phase addresses how the solution is kept operational and remains aligned with the site threats over the long term. The solution requires maintenance and updates over its lifetime and may evolve depending on changes such as new risks, site changes or specific events (e.g. visit of a very important person (VIP)). The details of this phase depend on the solution's countermeasure configuration.

   - Operation of the solution.
   - Communications and keeping stakeholders informed.
   - Keeping the solution up to date.

1

Phase one / Getting started with C-UAS



The 'getting started' phase is the first step that is taken towards securing a site against non-cooperative UAS. It involves investigating the need for a C-UAS solution and sets the site's principles, goals and first requirements for the C-UAS threat and risk analysis, solution selection process and its implementation. Prior to starting up a C-UAS project, it is important to understand that awareness, regulatory domains and procedures can increase and support passive countermeasures (deterrence) without any major pre-investment from the site itself.

The intent to protect against UAS is the very first phase in developing a C-UAS solution and serves as the trigger to further investigate the C-UAS possibilities. This intent can arise from any source, for example, an identified uptick in UAS traffic around the site, a tip from the Member State's intelligence services, installation of new at-risk facilities on the site or a change in the regulatory framework. This intent sits within a broader organisational context and is influenced by political, economic, societal, technological, environmental or legal factors. Clear identification of the business trigger is fundamental for justifying any initiatives related to C-UAS. Examples of triggers might be an incident with a UAS at another site, or new legislation mandating the need for a C-UAS solution.

BOX 1: PHASE ONE – GETTING STARTED

Information needed for this phase:

- threat understanding (high level);
- legislative understanding;
- high-level requirements;
- site and environment information.

At the end of this phase, you should have the following:

- Business case and clear mandate descriptions.
- An understanding of what needs to be protected against what and where.
- Constraints for use of technologies in the counter solution.
- Clarified the needs for a C-UAS solution with defined business needs and project governance. This should include a clear scope, objectives and deliverables.
- Site information and environment information that could influence the C-UAS solution.
- Stakeholder analysis (high level).
- Understanding on the fundamental minimum services that allow you to prepare an implementation.

In this first phase, it is recommended to gather high-level C-UAS requirements for further refinement throughout the project. These requirements include:

- site-specific needs and constraints that the project and solution should take into account;
- information on the environment;
- use of technologies (e.g. permission to use radar technology, ICT systems and data to remain on-site on dedicated servers);
- intelligence (e.g. informing authorities in the event of a C-UAS incident);
- legal and regulatory boundaries;
- any other areas relevant to a C-UAS solution.

In this phase, it is also important to start a high-level identification of stakeholders and begin conversations with them.

DEFINITION

Counter UAS is to lawfully and safely detect, track, identify and mitigate the risks of unmanned aircraft systems.

C-UAS system is a component of a solution designed to perform C-UAS.

C-UAS Solution is a collection of C-UAS systems, stakeholders and processes involved in operating them.

1.1 BUSINESS CASE AND CLEAR MANDATE

For a successful project, it is essential to have a clear definition and mandate to start implementing a C-UAS solution. Documenting this intent to protect a site or infrastructure is highly recommended and will make it easier to get buy-in from decision-makers and stakeholders.

The business case will serve as a guide to the project manager, as well as the stakeholders, and will include a description of the C-UAS objective, scope, estimated timeline and budget, roles and responsibilities, and approach to stakeholder communication.

The business case should do the following:

- Specify the clear mandate and justification to start the protection project. This should come from the highest hierarchical and authorities level possible.
- Define the objective, scope and outcome of the C-UAS solution.
- Define the level of mitigation that is required for the site (e.g. is the objective to monitor, do soft intervention or hard intervention).
- Document the solution's alignment with the site's security needs.
- Document the strategic short-term and long-term objectives.
- Provide a justification for the investment and define the budgetary framework.
- Describe the legal basis for a C-UAS solution.
- Define the first stakeholders that need to be involved and define the roles and responsibilities of each.

The format of such a business case may be aligned with the site's own project management methodology.

1.2 THINK SOLUTION INSTEAD OF SYSTEM

It is important to have a clear picture early in the process of what is needed to mitigate all the risks identified. An understanding of the difference between a C-UAS system and a solution is of crucial importance. C-UAS systems mostly consist of several technology components that are combined and linked. Typically these include detection, tracking and identification components, some form of operator to help categorise UAS and threats, some system logging and, in some cases, neutralisation, see Figure 2.

Although in many cases this can help to mitigate the risk, it is advised to approach C-UAS as a complete solution. A solution can include several systems and additional services and processes. While this will complicate the implementation, it will surely contribute to a better protection. A well-implemented solution will also make it easier to evolve alongside changes (temporary or fixed) in the threat landscape.

In addition to the C-UAS system elements, a C-UAS solution, see Figure 2 also considers the business and stakeholders processes, organisation and external factors, such as regional regulations. The solution might also include neutralisation and logging of information that is needed for forensics analysis of events and for future improvements.

The solution should be integrated into current stakeholder processes and be able to exchange information between stakeholders.

Figure 2 shows the C-UAS solution value chain and the list below describes some of the important elements that are included in all solutions.

- Detection technologies, tracking and identification systems. These could be from different suppliers and combine output through sensor fusion.
- Assisted decision processes and automated processes with interlinked systems. This will assist the operators in making optimal use of the solution.
- Data logging that includes both the events from systems and from stakeholder processes. All events should be consolidated and include observations, events reported via other ways (phone or manual), U-Space [5] and unmanned aircraft systems traffic management (UTM) events, other geographical zones and neighbours, public services, law enforcement agencies (LEAs), etc.
- There are many stakeholder processes to be included and a continuous evaluation should be part of the solution. The processes should include the following.
    - » Notification to authorities in the event of an incident.
    - » Interaction and agreements with LEAs. This will include what and who to contact in the event of an incident, who does what and when.
    - » Agreements with airspace service providers (UTM, U-Space).
    - » Interaction with authorities and neighbours.
    - » Computer-aided dispatch.
    - » Neutralisation permission request to the stakeholder that has the authority to decide this.
    - » Forensics data exchange.
    - » Communication to stakeholders that are affected or influenced by the solution.

[5] https://www.sesarju.eu/U-space.

1.3 INTEROPERABILITY AND DESIGN PRINCIPLES

Any C-UAS solution is an interoperability exercise on legal, organisational, semantic and technical levels. It is advised that stakeholders use the design principles described in this section and that every phase in the handbook is checked against the European interoperability framework [6], see Figure 4.

Figure 4: European interoperability framework

LEGAL INTEROPERABILITY
ORGANISATIONAL INTEROPERABILITY
SEMANTIC INTEROPERABILITY
TECHNICAL INTEROPERABILITY

Source: European interoperability framework (adapted).

- **Legal interoperability** enables organisations operating under different national legal frameworks, policies and strategies to work together. National laws and policies could block cooperation, there is therefore a need to establish clear agreements about how to deal with differences in legislation across stakeholder groups.
- **Organisational interoperability** refers to the way in which public administrations (i.e. government agencies and organisations) align their business processes, responsibilities and expectations to achieve commonly agreed goals. In practice, organisational interoperability means documenting and integrating or aligning business processes and relevant information exchanged.
- **Semantic interoperability** ensures that the precise format and meaning of exchanged data and information is preserved and understood: 'what is sent is understood'. This includes syntactic aspects, such as the terminology used to describe concepts and describing the exact format of the information.
- **Technical interoperability** covers the linking systems and services of applications and infrastructures. Aspects include interface and services specifications, and data and metadata standards and formats.

[6] https://joinup.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/european-interoperability-framework-detail.

When implementing a solution, it is recommended to have these principles in mind during all phases.

On top of interoperability, all solutions should be:

- **relevant** – the solution should be relevant to the needs of the CI or public space where it is implemented and should mitigate the risk identified;
- **effective** – so the solution will mitigate the risks and incidents when they occur;
- **efficient** – to efficiently mitigate risks and incidents (for this the solution needs to be well implemented and operating properly);
- **coherent** – coherent solutions are aligned with measures taken on similar CI or public spaces and implementations in surroundings;
- **impactful** – the impact of the solutions should be measured based on how they mitigate or reduce the effects of the incidents;
- **sustainable** – sustainable solutions will evolve with the changes of the environment, threats and CI.

The use of a project management methodology [7] will enable project managers to deliver solutions and benefits to their organisations by effectively managing the entire life cycle of their projects. It will make it easier to standardise, structure and organise needs and the solution implementation.

It is highly recommended to use open communication standards and protocols when designing a solution. A supplier might have a proprietary protocol that is used and working well, but when connecting to other systems and integrating the system into a bigger solution this often becomes cumbersome and difficult, needing additional resources and time.

1.4 WHAT TO PROTECT AGAINST WHOM AND WHERE?

An essential step early in the solution-definition process is to define and describe the first high-level needs of the C-UAS solution. At this stage, there is probably no clear understanding, definition or description on what to protect against. It is essential that before starting to design a solution and choosing technology systems, these definitions are described. In many cases, it can be very difficult to get a clear answer and risk assessments are needed to clarify the approach. When starting to investigate UAS protection, it is important to already know what to protect, the legal outline, CI business needs, the level of integration with airspace management, national and regional borders, who is allowed to do what and considerations on integration with the stakeholders.

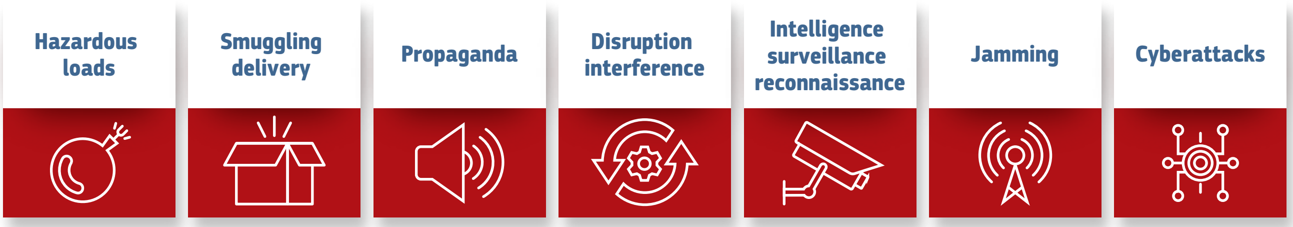
The better the description is elaborated, the easier the choices will be later in the process. All the parameters are very much linked and should be recorded, resulting in a high-level description needed for the next phases of risk assessments and solution design.

[7] See PM^2 project management methodology.

What to protect against?

Effective countermeasures depend on the type of the target (e.g. people, VIPs, data, infrastructure), its vulnerabilities and the intent of the perpetrator. It is also very important to document in this phase the type of UAS that could be used in an attack.

Figure 5: Key UAS threat types to critical infrastructure



Possible threat categories that have been identified in recent years in a civil context include the following.

- **Transfer of hazardous loads.** The payload capacity of UAS has increased over the last years due to more efficient engines and batteries, meaning they can be used for transferring an improvised explosive device, grenades or chemical, biological, radiological and nuclear substances within a secured perimeter. Modern UAS are able to carry substantial loads at great distances, with increased accuracy through the use of cameras and devices. The load may be placed at a point of interest, like a building roof, be released through a specially designed mechanism or triggered while in mid-air or even be deliberately piloted against an exposed facility in a kamikaze attack. Potential targets include specific individuals, CI, public spaces and information technology systems and services (e.g. energy production plant, financial institution, public administration, defence infrastructure).

- **Smuggling / delivery.** The use of UAS for delivering equipment at specific locations has already been observed in a number of cases across Europe, since they can easily bypass traditional control points and secure areas. The delivered equipment (e.g. a firearm) may be used by an aggressor who has already entered the secure area through the normal control procedure. For instance, a variety of different payloads (e.g. mobile phones, drugs, illicit goods, weapons) have already been delivered in prisons or smuggled across international borders.

- **Propaganda.** UAS may also be used by protesters and terrorist groups to record their actions, spread leaflets or other material in public spaces to reinforce their propaganda efforts. Footage may be broadcast online to attract sympathisers and encourage the recruitment of new terrorists or protesters, as it projects an image of a successful organisation with determined members.

- **Disruption and interference.** Even the presence of a UAS may be enough to interfere with the normal operations of an asset due to the safety issues that are raised from such an action (e.g. interference with civil aviation, flying over the audience during a music performance). Various types of mass events in urban areas may also be disrupted, initiating panic reactions from the attending public that could lead to injuries/victims or create favourable conditions for a secondary attack (e.g. channel people into specific locations).

- **Intelligence, surveillance and reconnaissance.** UAS may also be used to collect information and observe activities, mainly through the use of cameras, including cameras with night vision or thermal sensors. This enables perpetrators to gather information about the vulnerabilities of a potential target from a safe distance and exploit them during an attack, or even provide real-time information while the attack is taking place. Lately, powerful microphones have also been developed, which allow eavesdropping of private/confidential conversations to take place. Moreover, private images captured by a UAS invading the privacy of individuals may be used for criminal purposes, such as fraud or blackmail.

- **Jamming.** A UAS mounted with appropriate electronic equipment may be used as a local jammer to interfere with perimeter security systems, GPS systems or mobile phone signals. This tactic can create additional vulnerabilities that can be exploited by a perpetrator, or even have a significant effect on the operations of the asset (e.g. airport).

- **Cyberattacks.** A UAS can pose a cybersecurity threat by targeting local wireless networks and disrupting communications, delivering malware, hijacking and/or manipulating sensitive data. This can be done with specific equipment that gain access to the wireless system. Moreover, a UAS may be the target of a cyberattack (i.e. UAS hacking), as perpetrators may gain control and alter its route, gain access to its data or destroy it (e.g. denial of service).

With the increased commercial, professional and recreational use of UAS and as many technologies associated with UAS use are still evolving, the threat categories, which are summarised in Figure 5, are certain to evolve in the future. Improved batteries and engines will permit longer flight times with increased payloads while faster mobile networks (5G) will allow for long-distance communication, and artificial intelligence applications can be used to enhance cooperation between UAS so they can form swarms.

Whom to protect against?

Commonly, incident actors are grouped into the following categories: compliant/careful, clueless, careless and criminal/terrorist. At the time of an incident, it might not be possible to tell which 'C' it is, and the classification will probably only be possible during the post-incident analysis. Whatever the reason, if a UAS is detected in a place where it should not be, it needs to be countered accordingly. A correct classification can be used to update the threat picture for future updates and the evolution of the solution.

The compliant, clueless, careless and criminal categorisation, see Figure 6, can be used in the threat assessment to classify the intent or motivation of the pilot.

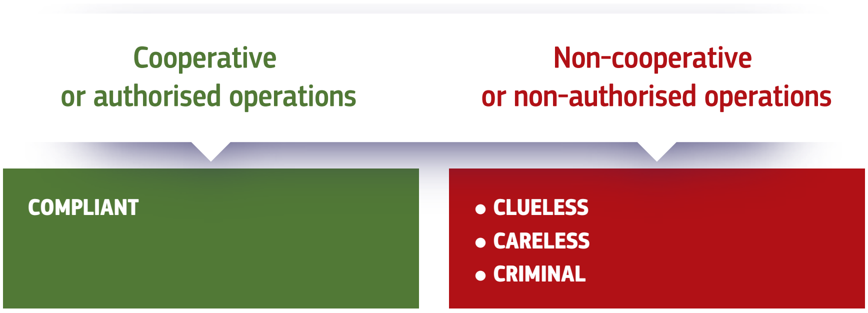
- **Compliant/careful** pilots follow the rules and regulations but might suffer from technical or operational circumstances that may cause the unmanned aircraft to enter into a restricted zone and become non-authorised unmanned aircraft (e.g. due to loss of control, wind or technical malfunction).

- **Clueless** individuals do not know or understand the applicable regulations and restrictions. As a result, they operate in a zone that is restricted. Typically they have no intent to do harm.

- **Careless** individuals know the applicable regulations and restrictions but breach them through either fault or negligence. As a result, they fly their unmanned aircraft in restricted zones.

- **Criminal/terrorist** are individuals who, regardless of whether they know the applicable regulations and restrictions, actively seek to use UAS maliciously to interfere with the safety and security inside the restricted zones of CI or public spaces.

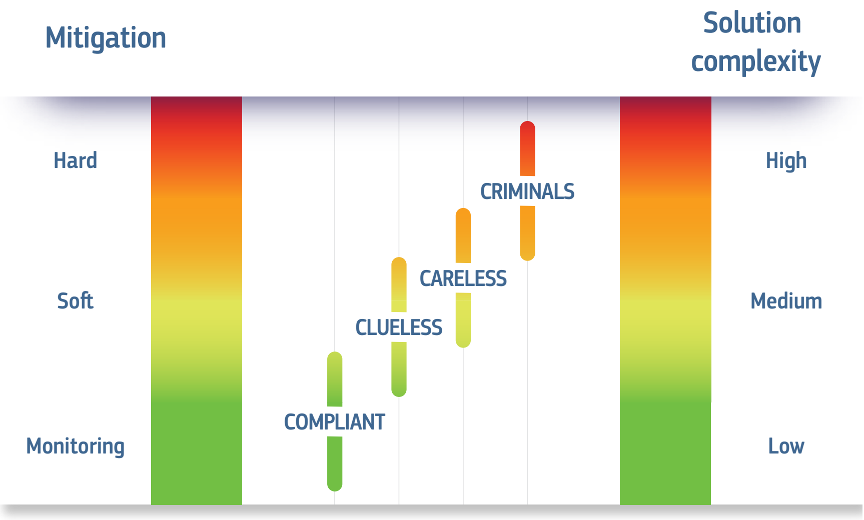
Figure 6: UAS flight categories



It is clear that the solution needed is completely different based on what and who you are protecting against. It can be assumed that criminals will exercise sophisticated and deliberate attacks. They could use modified UAS and have, for example, modified UAS communication signals so they can avoid detection, tracking or identification.

When protecting against criminals, the solution will often need 'hard' mitigation, and these are therefore the most complex and challenging threats to protect against, see Figure 7.

Figure 7: Mitigation and complexity of countermeasures for different categories of UAS users



Often, a distinction should be made between cooperative and non-cooperative UAS.

- **The cooperative UAS** pilot will comply with the legal requirements and will have the required permissions to fly in the airspace. This is comparable to the abovementioned compliant individual. However, due to external factors, the flight could nevertheless transform into a threat that needs to be mitigated.

- **The non-cooperative UAS** pilot covers the clueless, careless and criminals. This user will fly where they like, could have malicious intentions or could be a threat by coincidence or malfunction.

Whatever categorisation is used, it is of course important to remember that the real category may never be known.

Where to protect?

When deciding what to protect it is advisable to breakdown the elements of the site. Are some parts more important and need more protection? Where are the most import elements located? Are these away or close to boundaries of site or borders that could be important? Environmental factors like rural or urban surroundings should be documented.

TIP

If an unmanned aircraft is in an airspace where it should not be, in violation of the rules and regulations, then it could be a risk and should be mitigated with the measures decided.

1.5 STAKEHOLDER MANAGEMENT

Stakeholders should be involved in the early stages of the C-UAS solution implementation process. When the agreements with the internal business entities are approved and the decision to start the solution development has been taken, it is time to look at internal and external stakeholders. As can be seen in Figure 2, the process of involving stakeholders is very important and is cross cutting between all systems. Any project management methodology will have some stakeholder element included. Stakeholder identification and analysis can be time-consuming and comprehensive. It should be revisited regularly to ensure that it is up to date and complete. Start with the known stakeholders and build upon these.

The involvement of stakeholders in developing a C-UAS solution is essential. Some of the benefits are the following.

- **Ensuring project success.** Stakeholders can provide valuable input throughout the project life cycle, from the initial planning stages to implementation and evaluation. Their involvement ensures that the project is aligned with their expectations, needs and objectives, which increases the likelihood of success.

- **Identifying risks.** Stakeholders can identify potential risks that may impact the project's success. This allows project managers to mitigate or avoid these risks before they become significant issues.

- **Gaining support.** By involving stakeholders in the project, you can gain their support and buy-in, which can help overcome resistance to change or any potential obstacles that may arise during the project.

- **Managing expectations.** Involving stakeholders can help manage their expectations and prevent misunderstandings. This helps ensure that everyone involved has a clear understanding of what is expected of them, and what the project aims to achieve.

- **Improving communication.** Engaging stakeholders helps to establish clear lines of communication between project managers, stakeholders and team members. This promotes transparency, reduces conflicts and allows for a better understanding of the project's progress and outcomes.

Because of the diversity of the stakeholders involved, it is recommended and important to make a first stakeholder map as early as possible.

The mapping should at least specify the actors affected by the solution and those involved in the operation of or exchanging information with the solution. In the beginning, these external stakeholders can be limited to the warning zone and UAS geographical zone perimeters.

As C-UAS solutions in the neighbourhood and surroundings will be an important source of information, and to avoid technology interferences, stakeholders from these should also be included.

LEAs (local, regional and federal) are important stakeholders for event monitoring and neutralisation. The responsibilities for different LEA levels will vary and it is important to map responsibilities.

The following is a list of priority stakeholders to be consulted in any project:

- end users of the solution;
- similar CI sites;
- authorities and regulators for the site you need to protect;
- authorities with risk and threat assessment competencies;
- regulatory authorities for the infrastructure and location of the solution;
- management of the site to be protected;
- security and safety;
- authorities regulating the site to be protected;
- LEAs (local, regional and federal);
- authorities involved in mitigating risks (that have permission to do so);
- intelligence and security agencies;
- airspace managers and UTM / U-Space stakeholders around the site to be protected;
- neighbours around the site to be protected;
- regulation bodies that allow the use of technologies (e.g. frequencies for radar and possible jamming);
- system integrators.

Naturally, the stakeholders differ depending on the specific implementation. Many stakeholders and actors are linked to the understanding of the threat and corresponding risks. A good stakeholder management is therefore important in all phases of the solution development and implementation process.

Figure 8 is an example of a RASCI (responsible, accountable, supportive, consulted, informed) table [8] that could be used to map stakeholder involvement. Such a table should be complemented with the special stakeholders identified and linked to the site to be protected. The phase follows the C-UAS design process roadmap, as shown in Figure 14.

TIP

It must be clear that the involved stakeholders vary from solution to solution. The higher the protection, the more complicated the stakeholder management is.

In the design phase, the stakeholder involvement will be further elaborated.

Figure 8: Example of a RASCI matrix with stakeholders involved during the C-UAS solution development process (to be complemented with specific needs)

Stakeholder category	Stakeholders	Phase one Getting started with C-UAS	Phase two Identification of UAS risks to add to an existing risk assessment	Phase three C-UAS solution design	Phase four Solution implementation	Phase five Solution implementation
Site	CI business owner	A	A	A	A	A
	Local security	R	R	R	R	R
	Local community and neighbours	I	I, C	I, C	I	I
	Similar CI sites	C	S	C	S	
	Organisation regulator	S	C	C	I	S
Authorities	Law enforcement	C	C	I	I	S
	Authorities allowed to use mitigation	C	C	C	R	R
	Authorities regulating use of technologies	C	I	C	I	I
Government entities	Authorities with risk and threat assessment competencies	C	C	I	I	C
	Regulatory authorities	C	C	S	C	I
Private entities	Telecommunications operators	C	C		S	
	C-UAS solution suppliers	S	C	C	C	C
Airspace	UTM services	C	C	C	R	R
	U-Space service provider	C	I, C	I	C	I

R = responsible | A = accountable | S = supporting | C = consulted | I = informed

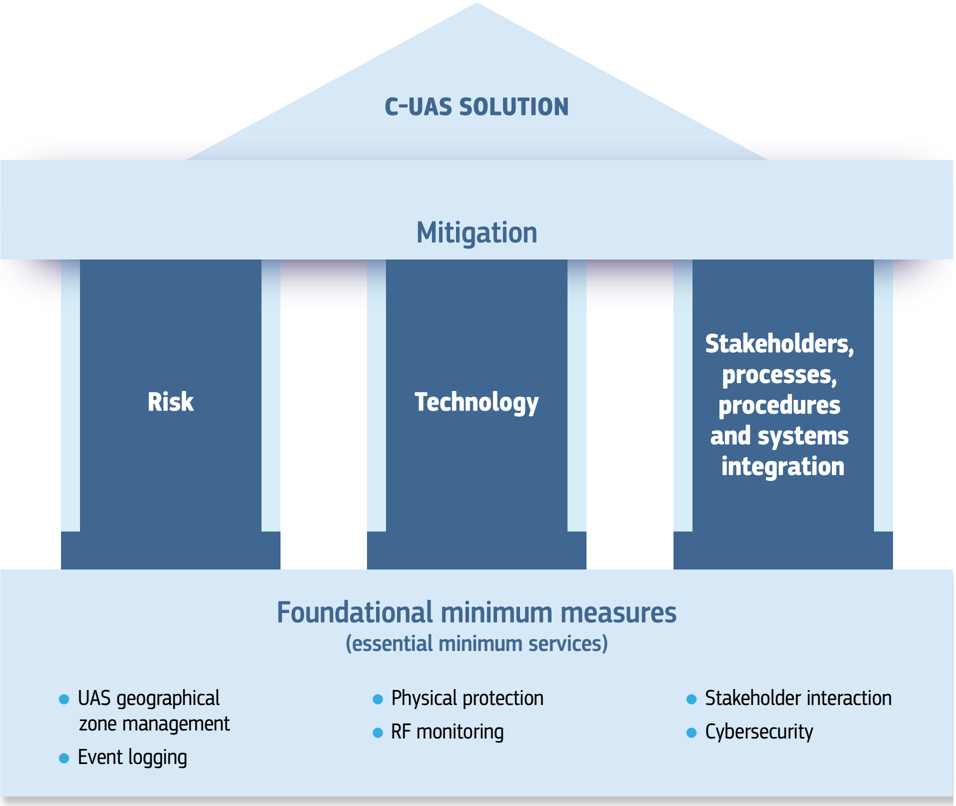
[8] See PM² project management methodology

1.6 FOUNDATIONAL MINIMUM MEASURES

The foundational measures are essential and common to all solutions and must be considered and included in most solutions. The implementation of these measures will enable the solution to evolve with risk-level changes, when technologies are updated or changed, when processes change and prepares for data exchange with stakeholders.

These are services which are always needed and should be implemented at an early stage. See Section 3.1 for more details on how to design these services.

Figure 9: Foundational minimum measures supporting the other pillars of a C-UAS solution


C-UAS SOLUTION
Mitigation
Risk
Technology
Stakeholders, processes, procedures and systems integration
Foundational minimum measures
(essential minimum services)
UAS geographical zone management
Event logging
Physical protection
RF monitoring
Stakeholder interaction
Cybersecurity

The foundational minimum measures are the following.

- **UAS geographical zone management** refers to the management of airspace established by the competent authority that facilitates, restricts or excludes UAS operations in order to address risks pertaining to safety, privacy, protection of personal data, security or the environment, arising from UAS operations[9]. This includes the permissions to operate UAS, use C-UAS technologies and test the UAS solution. An investigation on the use of tools to manage airspace, such as the use of UTM and links to U-Space services, should begin as soon as possible, as it is important to integrate the tools into other solutions implemented around the area to be protected. It also includes the management of stakeholders in the zones around the site.

[9] Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R0947.

- **Event logging** aims at understanding what is happening in your airspace by logging all activities of UAS use and observations in and around the site to be protected. The logging should cover all data sources and observation measures. The logging should be as complete as possible, so it can be used for future analysis of risks and for potential forensics.

- **Physical protection** is an important element to start with in the early stages, by considering the risks posed to buildings and physical infrastructure and whether any structures need upgrades or changes. These initiatives depend on which types of UAS are to be countered. In the later phases, this needs to be re-evaluated when the risks have been clarified. For more details, see the JRC handbook on physical protection against UAS[10].

- **RF monitoring** for UAS is the minimum detection that all protected airspaces should start with. The aim is to detect as many UAS as possible, but it is also clear that it is not possible to detect them all. This method detects and reads the communication emitted by the UAS and the communication between the UAS and its base station. The remote ID UAS emit includes important parameters that can be used to manage the airspace. Intercepting the communication between the ground station / pilot and the UAS adds additional information. These sources complement each other and, together with location detection, give a very good basic airspace overview. It must be noted that this will not detect dark UAS[11], which are programmed to fly without communication with the base control station. Neither will it detect UAS that have been modified to not emit these signals or to use non-standard frequencies. For maximum coverage, it is advised to monitor the frequencies and range around those normally used by UAS, and to avoid vendor-specific systems that only detect their UAS.

- **Stakeholder interaction** is one of the key processes in a solution, yet it is often neglected and underestimated. All systems can be installed and working to specs, but without the involvement and integration of the stakeholders needed to mitigate the threat within the time available these systems can be useless. As seen in Figure 2 the processes involving stakeholders are relevant for all systems and elements of the value chain.

- **Cybersecurity** is an important issue for any solution that has ICT systems connected to the internet, or where information is exchanged with other systems. The C-UAS solutions should be designed using available cyber-protection measures. All elements of the design should be able to operate without internet connection. Where risks are identified as high, there should be redundant systems and sensors when possible.

BOX 3: GETTING STARTED PHASE SUMMARY

At the end of this phase you should have a better understanding of:

- Business case and clear mandate descriptions.
- What needs to be protected against what and where.
- Constraints for use of technologies in the counter solution.
- The needs for a C-UAS solution with defined business needs and project governance. This should include a clear scope, objectives and deliverables.
- Site information and environment information that could influence the C-UAS solution.
- Stakeholder analysis (high level).
- The fundamental minimum services that allow you to prepare an implementation

[10] Protection against Unmanned Aircraft Systems - Handbook on unmanned aerial systems risk assessment and principles for physical hardening of buildings and sites

[11] Dark UAS or invisible UAS are unmanned aircraft in automatic flight mode without transmitting RF signals from both the remote control and the drone.

Phase two / Risk and threat analysis

This phase analyses the UAS threats of the site to be protected. The approach presented in the handbook to assess the risks related to UAS-driven attacks is based on the International Organization for Standardization (ISO) 31000:2018[12] standard's generic definition of risk assessment: 'Risk assessment is the overall process of risk identification, risk analysis and risk evaluation'. Such a description aims to incorporate both natural and human-induced hazards in the risk process, even if there are major challenges when it comes to estimating the likelihood of rare events and quantifying the consequences in the human/social domain. It is advised to assess the UAS risks using the risk assessment methodology already used by the site and to update the risks list with the UAS risks identified. Using the methodology already in place will minimise doubling and avoid incompatibility between two different risk assessment methods. If a new risk assessment process needs to be established, the JRC risk assessment for CI[13] is a good guide on how to apply the security-by-design approach from the JRC[14]. The risk assessment in phase two is therefore a summary from the JRC handbook on physical protection against UAS.

In all cases, the risk assessments should help stakeholders understand the site-specific UAS risks, so they can design a C-UAS solution that mitigates the risks identified.

BOX 4: PHASE TWO – RISK AND THREAT

The following are items that need to be collected before starting this phase:

- site risk register (from previous and other related risk assessments);
- legislative understanding of both local and EU[15] [16] rules and regulations covering the CI or public space you need to protect;
- high-level requirements as defined in phase one 'getting started';
- site and environment information.

At the end of this phase you should have:

- threat identification
- site survey
- risk and threat analysis
- a threat-response plan.

The malicious use of UAS that is analysed is one of the means that may be employed by a perpetrator targeting an individual, public space or infrastructure. Different attack tactics may be distinguished that take advantage of the UAS capabilities. To facilitate the evaluation process, the development of scenarios is proposed depending on the vulnerabilities of the examined CI. Figure 10 shows the risk assessment process.

[12] International Organization for Standardization, ISO 31000:2018, Risk management – Guidelines, 2018.

[13] JRC risk assessment for critical infrastructure, https://joint-research-centre.ec.europa.eu/scientific-activities-z/critical-infrastructure-protection_en.

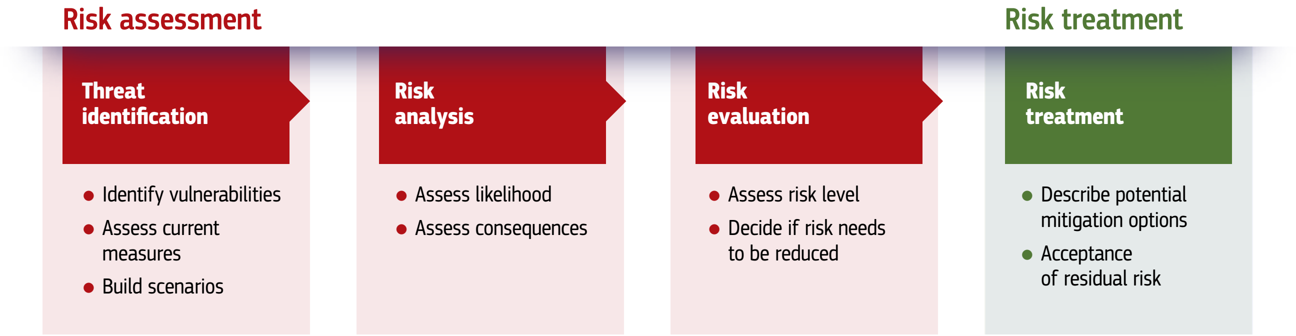
[14] https://home-affairs.ec.europa.eu/news/security-design-protection-public-spaces-terrorist-attacks-2022-12-14_en.

[15] Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R0945;

[16] Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R0947.

- **The threat identification** process is identifying potential means and methods of attack, including the identification of vulnerabilities in the examined asset against the considered UAS attack tactic, the assessment of current (if any) protective measures and the production of scenarios.
- **Risk analysis** is assessing the likelihood and impact of each threat, combined with identifying any vulnerabilities or weaknesses that could be exploited. Risk analysis can be conducted through a variety of techniques, including brainstorming, scenario analysis or using mathematical models. The purpose of risk analysis is to provide a comprehensive understanding of the risks that are present and to identify the most significant risks that need to be addressed.
- **Risk evaluation** is assigning a risk score or rating to each threat, based on its likelihood and potential impact. The purpose of risk evaluation is to prioritise risks and determine which ones require immediate attention. Risks that have a high likelihood and high impact are typically considered the most critical, while risks with a low likelihood and low impact may be considered less important.
- **Risk treatment** is identifying and implementing appropriate risk control measures, such as implementing security protocols, improving disaster recovery plans or purchasing insurance. The goal of risk treatment is to reduce the likelihood and impact of potential threats, and to minimise the overall risk to the organisation. The specific risk treatment measures chosen will depend on the nature of the risks involved, the available resources and the risk tolerance of the organisation.

Figure 10: Risk management stages



The result of the risk assessment may differ substantially depending on the background of the expert who is performing the assessment. If there is not sufficient data to evaluate the scenario likelihood, then it may be useful to adopt qualitative methodologies and use judgement to assess the risk. To reduce bias, assessors should meet certain requirements, such as prior expertise in conducting terrorism risk assessments, no conflicts of interest and impartiality.

The risk assessment will need to be documented, with instructions for their precise interpretation, to the owners/operators of the examined asset who are responsible for establishing the acceptable risk level limits and deciding if risk treatment is required.

Performing a thorough threat and risk analysis is a cornerstone in a C-UAS solution development process, as it defines basic requirements to both the future system and the broader solution. The scenarios defined during the threat and risk analysis are a key input for testing during the implementation phase, and for regular testing while operating a C-UAS solution. It should be clear that all solutions and the threat picture will evolve and that this should be repeated at regular intervals. The analysis should clearly define the potential harm that a non-corporative UAS can cause to the CI or public space (threat) and the likelihood that this takes place (risk).

In most cases, the UAS itself does not pose an isolated risk, but it is part of a broader risk (called a 'macro risk'). It is therefore recommended to address the UAS risk as part of the site's broader risk management programme and not as a separated UAS risk assessment.

2.1 RISK IDENTIFICATION

The first step in the risk assessment process is the identification of the UAS threats that are relevant to the asset under evaluation. Threat identification focuses on pinpointing tactics that aggressors may use and on formulating possible scenarios. Identifying man-made threats and their likelihood is a challenging task, since, contrary to natural hazards, available data are scarce and therefore a large degree of subjectivity is usually involved when trying to link a specific threat to a potential target. Data relating to current and emerging threats, the intent of an attack, and other related sensitive information may be requested from intelligence services and LEAs. More information on available data sources that can facilitate the identification of threats may be found in Security by Design: Protection of public spaces from terrorist attacks [17].

2.2 RISK ANALYSIS

Threats to a specific CI can vary considerably. Characteristics of the site (environment, size, neighbouring implementation, buildings, etc.) influence the threat picture. Furthermore, each site will have different concerns when it comes to UAS. For example, a prison owner might be more concerned about UAS flying in contraband, while the organisers of a public event will focus more on UAS threats that might threaten public security. The most common threat categories are shown in Figure 5.

It is important to identify the elements of a site that could be affected by a non-cooperative UAS attack. Examples include (but are not limited to) persons, buildings, assets, safety-critical services, core CI operations and controlled materials.

[17] Coaffee, J. et al., *Security by Design: Protection of public spaces from terrorist attacks*, Joint Research Centre, Publications Office of the European Union, Luxembourg, 2022.

For completeness, it is recommended to perform a site survey that includes:

- **site specifics,** including critical asset locations and site access points;
- **environment,** including three-dimensional site positions, topography, land use (urban/rural/forest) and human terrain (urban areas, structures, transport routes);
- **virtual terrain,** including airspace restrictions, electromagnetic or RF spectrum usage, potential blind spots in detect, and track and identify coverage (e.g. trees obstructing radar signals);
- **potential UAS launch sites and approach routes** referring to the environment of the individual facility, including its geography, procedures and capabilities, which will dictate the methodology used to describe situational awareness;
- **physical vulnerabilities,** such as building structures and windows.

Once the site survey has been done, it should be used to understand the threats and potential vulnerabilities that will most likely be targeted in order to define the scenarios. It is recommended to define each scenario (defining capability, intent, site survey vulnerabilities) and then describe each one individually in more detail (typically answering: who, what, where, when, why, how, consequence, etc.).

To quantify this relative likelihood, the threat level in the area surrounding the examined potential target needs to be assessed. This is a challenging task since usually relevant data are scarce and often unavailable due to their sensitive nature.

Some indicators to use are the following.

- **Threat history.** Gives information regarding previously reported, failed or prevented attacks/threats with each specific tactic used to target the building or its users, or in similar facilities. The threat history considers public statements made from terrorist groups against civil targets and their motivations, especially if preference is exhibited on the examined scenario.
- **Attack complexity/capability.** Estimates the practical/technical expertise the aggressor would require to perform the UAS-driven attack (e.g. creating an improvised explosive device or chemical, biological, radiological and nuclear substances) and the difficulty in obtaining the UAS (e.g. depending on its size), the weapon or the components for its creation. It examines the financial resources required for acquiring the materials and other essential elements that might be needed (e.g. supporting infrastructure, communications network and supply chain).
- **Attractiveness / motivation**. Depends on the attractiveness of the target (e.g. cultural/religious/symbolic significance, people attendance) related to the potential attack tactic. It investigates if a certain modus operandi seems more attractive to the attacker because it could have a greater impact due to the asset's functions (e.g. interdependencies with other facilities, collateral consequences for the state and society, public and/or sensitive data presence).

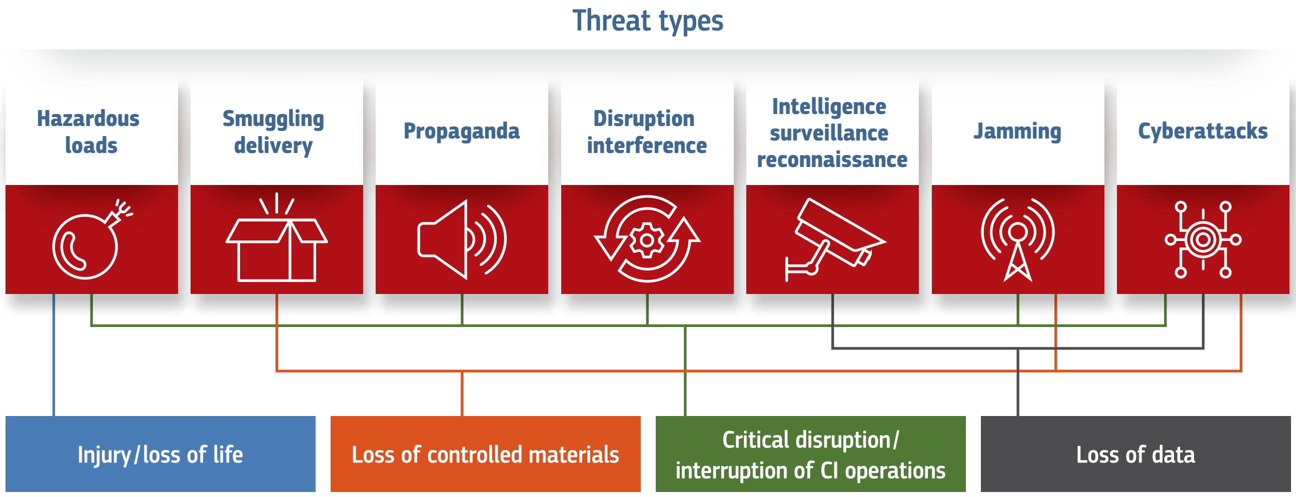
With the UAS threat integrated into scenarios, these can then be mapped with the macro risks. Examples of macro risks featuring UAS would be (but are not limited to) the following.

- **Injury / loss of life.** Including the use of UAS as weapons in a physical attack.
- **Loss of controlled materials.** The use of UAS to support criminal activities (e.g. intellectual property, business-critical information or theft of controlled substances).
- **Critical disruption/interruption of CI operations.** The use of UAS for sabotage, either directly against the CI facility or indirectly against a dependent facility, with a weaponised and/or support function (e.g. intelligence gathering / cyberattack).
- **Loss of data.** Including the use of UAS as an intelligence platform to support hostile planning activities, espionage and unlawful information gathering.

How these macro risks map to the identified UAS threat types will differ for each CI site. It is up to the business owners to assess how the macro risks relate to the UAS threat types for their site. It is certain that all macro risks will be linked differently in all implementations.

For instance, the UAS threat type 'physical attack' could contribute to the 'loss of life' risk. Risk managers can use the UAS risk register to examine the scenarios. It is important to note that the risk matrix should be adapted to the specific context of the CI site. This is illustrated by the example in Figure 11

Figure 11: An example of UAS threat types that map into macro risks



Likelihood and consequences assessment of UAS incidents

The risk-level assessment of malicious UAS combines an evaluation of the likelihood of occurrence of each identified scenario and the potential consequences if this scenario materialises. Such a process uses the results of the threat and vulnerability assessment. This can be illustrated in a risk matrix as shown in Figure 12.

Figure 12: Example of risk matrix

Impact		Score					
Critical	5	🟨	🟧	🟥	🟥	🟥	🟥
Severe	4	🟩	🟨	🟧	🟥	🟥	🟥
Substantial	3	🟩	🟩	🟨	🟧	🟥	🟥
Moderate	2	🟩	🟩	🟩	🟨	🟧	🟥
Low	1	🟩	🟩	🟩	🟩	🟨	🟧
Ineffective	0	🟩	🟩	🟩	🟩	🟩	🟨
Likelihood		0	1	2	3	4	5
		Not possible	Unlikely	Possible	Probable	Likely	Highly likely

Very high	High	Moderate	Low
🟥	🟧	🟨	🟩

With UAS risks identified in the UAS risk register, a baseline risk score could be established as part of the UAS risk analysis. Factors to consider during risk analysis are the following.

- **Threat actors.** Likely threat actors should be identified from the threat analysis. This step is important for building likely scenarios, against which risk control measures should be taken.
- **Likelihood.** A qualitative, relative scoring based on threat actor motivation and capability. The scoring typically goes from 0 to 5 (5 being the most critical threat) or from improbable, moderately probable, highly probable, probable to almost certain.
- **Impact.** A score based on the effect of the threat on the relevant risks in the CI macro risk register. Qualitative assessment is recommended, with a suitable methodology and scoring system agreed by individual CI business owners[18].

[18] One example might be values linked to the business continuity plan (e.g. recovery point objective, recovery time objectives or work recovery time).

- **Risk score.** The risk score is calculated by multiplying likelihood and impact, with a possible weight factor based on the CI site's risk acceptance levels. The risk score can be non-linearly weighted if the impact of an event can be disproportionate to the likelihood (low likelihood events can be sufficiently catastrophic as to require appropriate risk mitigation). While this handbook shares one possibility of calculating risk, the reader is free to choose the methodology and/or follow what their site already has in place.

Consequences of an attack are linked to the type of asset and the conditions at the time of the incident. Past incidents have demonstrated that the direct, immediate repercussions of an attack range from effects on human life (e.g. injuries or fatalities) to major economic losses (e.g. repair costs and disruption of services) and environmental disasters (e.g. water contamination). Indirect, long-term consequences are more difficult to assess, as they include political/social aspects such as the effects on the population's psychology and indirect economic costs (e.g. impact on the tourism industry). To facilitate this evaluation, the assessor has to respond to a number of questions, including the following.

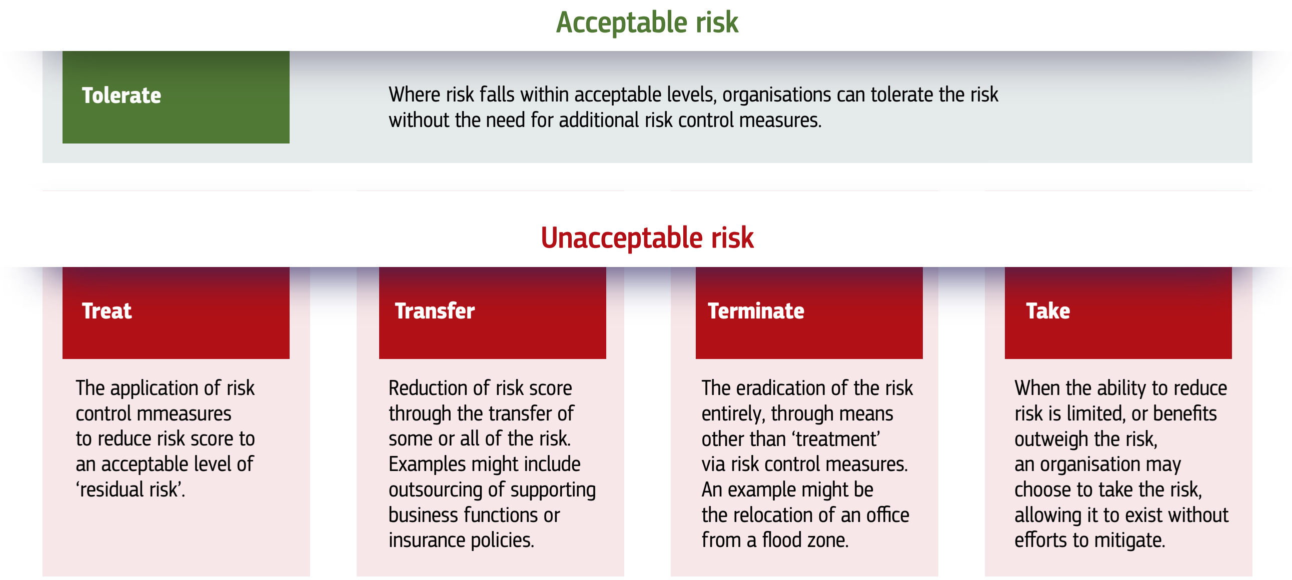
- How many people may be killed or injured after an attack with a UAS-driven tactic?
- What services may be disrupted if there is an attack? How long will the disruption last? Are there any backups for the services and how much will the repairs cost?
- Are there any cascading effects through interconnections with other assets or services?
- What are the expected costs of repairing any damage? Are replacements available?
- Does the CI include critical utilities or sensitive information that may be compromised? What are the repercussions of their loss or their disruption of service?
- Is there a possibility of any political consequences, reputational damage to the organisation/owner and/or security breaches (e.g. personal data breaches)?
- What are the indirect economic costs (e.g. to the tourism industry) and what are the consequences for the population's psychology?

2.3 RISK EVALUATION

UAS risk evaluation takes place following the UAS risk analysis. Once calculated, reviewed and agreed, baseline risks should then be assessed against risk acceptance levels to determine if additional mitigation is required. Each risk should be considered for levels of acceptability against a CI-business-owner-agreed tolerance level. Risk scores that exceed this threshold are deemed unacceptable, and action should be taken.

As illustrated in Figure 13, the 'five Ts' of risk treatment risks should be evaluated and possible action should be selected for each risk. Risks should be evaluated in order to select from the following actions.

Figure 13: The ‘five Ts’ of risk treatment



Acceptable risk

Tolerate

Where risk falls within acceptable levels, organisations can tolerate the risk without the need for additional risk control measures.

Unacceptable risk

Treat

The application of risk control mmeasures to reduce risk score to an acceptable level of ‘residual risk’.

Transfer

Reduction of risk score through the transfer of some or all of the risk. Examples might include outsourcing of supporting business functions or insurance policies.

Terminate

The eradication of the risk entirely, through means other than ‘treatment’ via risk control measures. An example might be the relocation of an office from a flood zone.

Take

When the ability to reduce risk is limited, or benefits outweigh the risk, an organisation may choose to take the risk, allowing it to exist without efforts to mitigate.

2.4 RISK TREATMENT

Responsive decision-making in C-UAS is built upon a combination of baseline understanding, tactical-level technical analysis (of UAS behaviour and/or UAS configuration, both physical and electromagnetic) and applicable regulations.

When it comes to the engagement of UAS, there are several elements within the C-UAS solution that should come together to take the engagement decision. Among these are the threat assessment, regulatory and legal parameters and the engagement authority.

This triage reflects a decision process that CI and public space owners can use to determine the right course of action when a threat is observed. The decision process highly relates to the threats that are expected and possible relevant countermeasures that can be leveraged. Triage reflects the CI’s response to UAS incursion and is therefore a key input towards the C-UAS solution design.

The detailed risk assessment should be documented so it can be used in the following phases.

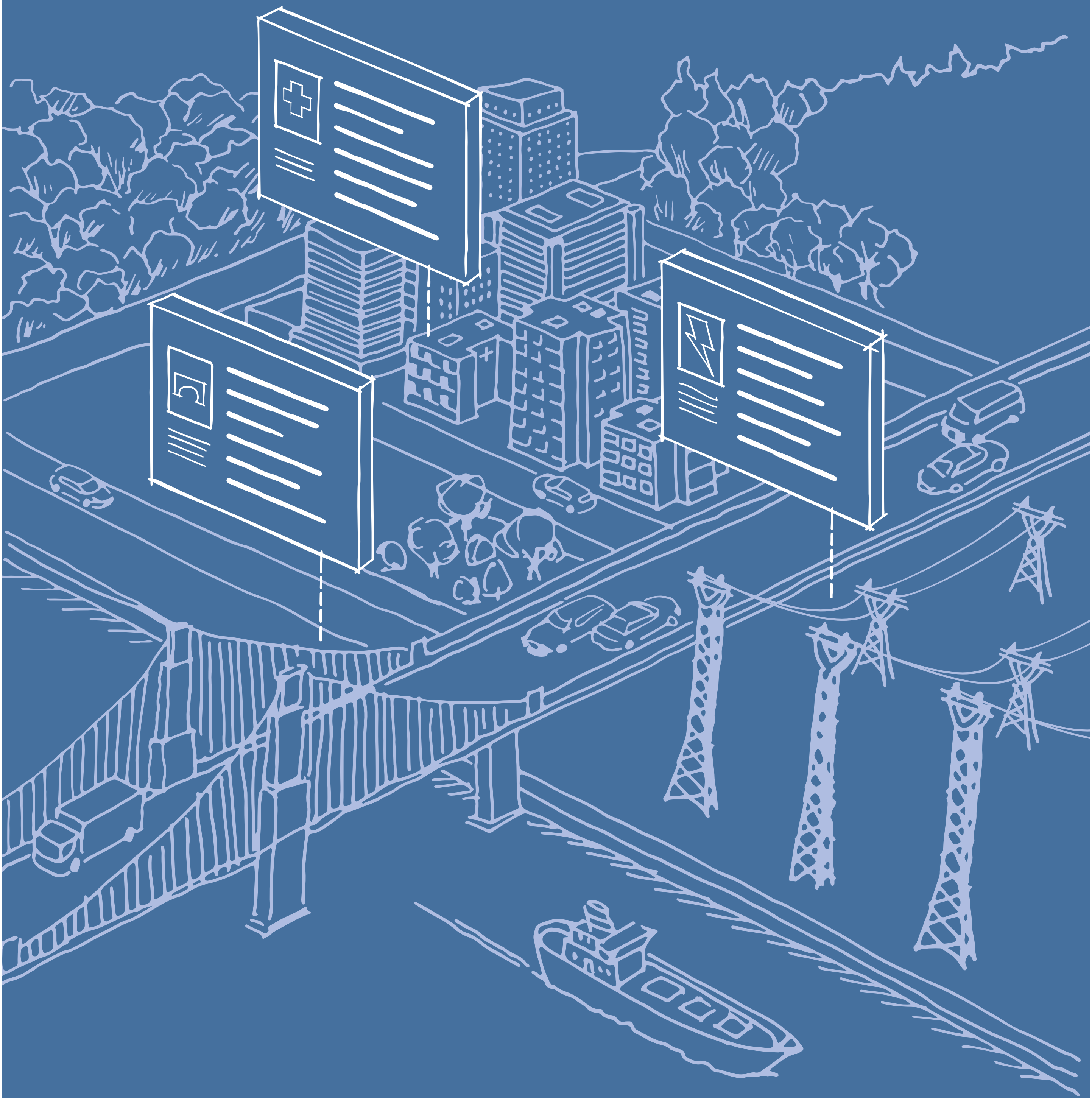
BOX 5: RISK AND THREAT ANALYSIS PHASE SUMMARY

At the end of this phase you should have a better understanding of:

- an understanding of the threat;
- an understanding of threat scenarios;
- identified the specific UAS threats that are applicable to the site;
- identified the vulnerabilities of the site;
- a site survey with information of where critical assets are placed;
- a mitigation plan of the risks identified;
- a risk matrix;
- an agreement of risk acceptance levels;
- a threat-response plan.

3

Phase three / C-UAS solution design



The ‘C-UAS solution design’ phase includes the process of selecting the appropriate mitigation measures and technologies that correspond to the risks identified and the needs from the site and stakeholders.

Common for all solutions are the foundational services (see introductory section), which make it easier to change mitigation levels up and down when needs change (e.g. VIP visits, temporary events like Christmas markets, large sporting events and concerts). The mitigation on top of the foundational services depends on many factors, which will be covered in this section. The aim is to implement a complete solution.

BOX 6: PHASE THREE – THE DESIGN PHASE

Information needed for this phase:

- a clear description of the requirements of the solution that will be designed (site needs, objectives and scope);
- site risk register;
- a clear threat-response plan;
- legislative understanding;
- high-level requirements;
- site and environment information.

At the end of this phase, you should have:

- a design that is appropriate for the site needs;
- high-level solution architecture;
- an updated site survey;
- solution implementation specifications;
- updated stakeholder analysis with clear roles and responsibilities.

The design of a solution is a challenging phase and will be the base of the implementation and operating phases. Where many factors can be common for C-UAS solutions, every element and setting should be tailored to the risk acceptance levels, site specifics, available budget, etc. A clear mandate from the highest level of hierarchy, authorities and CI regulators will be needed. A good design and methodology will help making changes easier when needed. A good design will also help involve and manage processes and procedures from the many stakeholders involved at all levels.

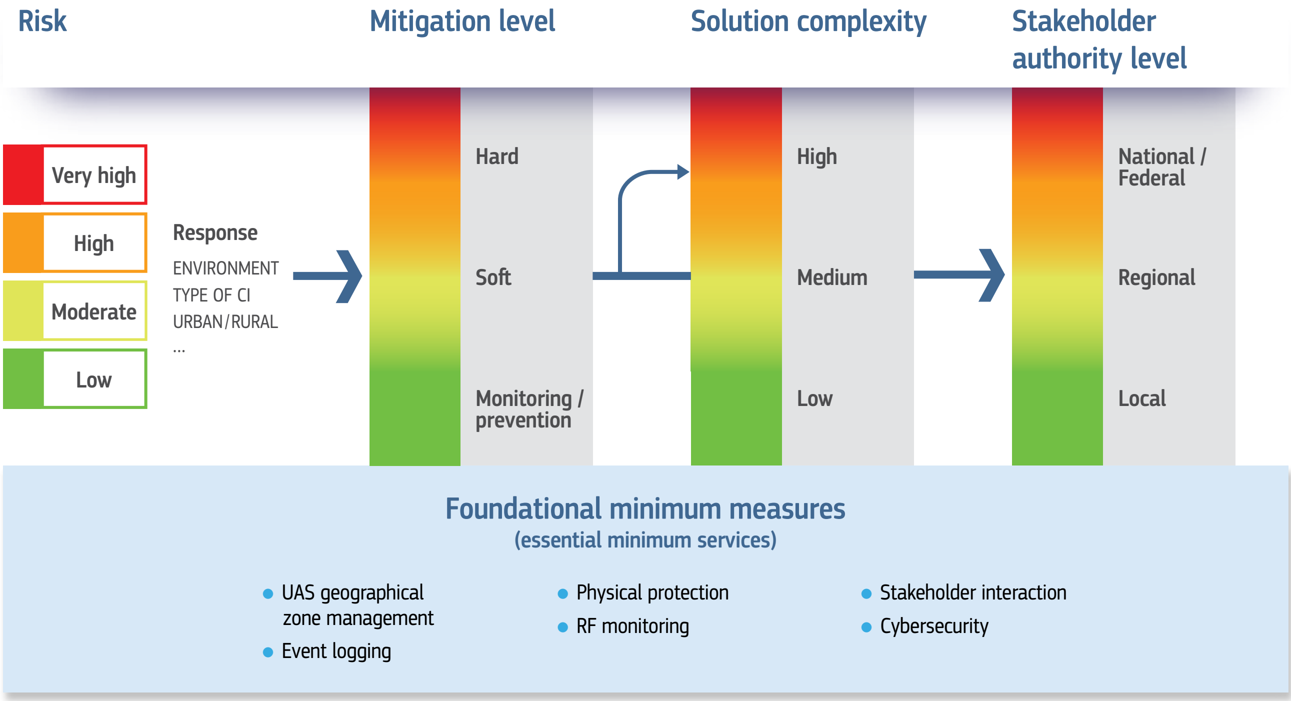
TIP

The objective of a C-UAS solution is to mitigate a UAS risk to a site with appropriate measures within legal, technical boundaries and with the correct stakeholders involved.

A simplified process roadmap solution development can be summarised in four main steps, see Figure 14.

1. Making a risk assessment and collecting environmental constraints and business needs.
2. Selecting the mitigation level fit for the problem and within the legal constraints.
3. Selecting the technologies and solutions appropriate to the mitigation selected.
4. Defining the processes and procedures with the stakeholders involved and implementing them. This will involve stakeholders at all levels.

Figure 14: C-UAS design process roadmap



At the end of the design phase, the site has a solution requirement specification, which is a description of the intended solution with procedures and processes linked to this. This can be the base for a solution procurement process.

Some important elements to be considered and decided in the design phase are the following.

- **Investment approach.** At this stage there should be a decision on how to finance the first phase of the design. Most solution designs will probably need C-UAS expertise to be involved. In many cases it would be an advantage to separate consultants from the technology providers, to minimise the bias towards solutions the tech company has already rolled out. A good design should be detailed enough that it could be used as a technical document for a procurement procedure. It should be considered whether the solution will be **procured, rented** or whether it will be acquired **as a service**. In addition, a **cost estimate** is recommended with an overview of the various cost factors (including both cost estimations for internal and external parties), together with how the solution will be operated and financed over its lifetime.

- **Legal considerations.** This includes the permissions to use technologies for detection and mitigation. It should also be investigated what possibilities there are to intervene in and around the perimeter of site. This will need the involvement of many stakeholders such as LEAs, authorities, neighbours, operators of other solutions, airspace management, UTM, air traffic management and U-Space operators. In the end, the design must ensure that all legal aspects of the solution are addressed and documented, including all the necessary **permits and licences** for the solution.

- **Scope and objective of the solution**. In any project it is important to define the scope and objectives to avoid confusion, misunderstanding and scope creep. This is to avoid an increase in expenditure and possible ineffective implementations that do not fulfil the relevant needs, or to avoid having a solution that cannot be changed or integrated when changes are needed.

- **Evolution of the CI, public spaces and surroundings.** The design should consider plans for the evolution of the site and its surroundings. This will include installations on other sites that could affect the detection systems.

- **Information exchange.** Stakeholders should discuss and agree on information exchange. This is important for test flights that could be detected by surrounding implementations, overlapping UAS geographical zones and warning zones, interferences from detection systems (e.g. radar frequencies), UAS activity developments and initiatives for airspace management (U-Space services and implementation of UTM systems), etc.

- **Assessment of side effects.** This is a very important point that should not be underestimated. It should be checked what effect the selected detection and neutralisation technologies will have on the site, its environment, other installations, surrounding implementations, etc. Checks should specifically cover the effect from use of mitigation measures. The frequencies used to communicate between ground stations and unmanned aircrafts are, in most cases, the same frequencies used for wireless communication by common industry and household equipment. Additionally, jamming or spoofing of global navigation satellite system signals could have unwanted side effects.

- **Site survey.** A clear and complete overview of the site and surroundings is essential for the design. There is a need for a comprehensive survey that contains height of buildings, trees, landscape, etc. This can be used to simulate, select and plan the placement detection sensors and neutralisation systems. The site survey used in phase two (risk and threat analysis) is linked to the risks list in phase four (implementing the solution to the definition of zone sizes). This survey should be clear and detailed enough to be used by third parties for the solution implementation.

3.1 FOUNDATIONAL MINIMUM MEASURES

The foundational minimum measures should be the foundation of all solutions. As described in the introductory section, these will be the basis for all the other services and will make changes easier when they are needed. Some of these could already be implemented as part of normal security processes, which will then just need updating with the C-UAS elements. The following sections describe these services and advises on how to implement these.

UAS geographical zone management

Around a protected site, it is beneficial to have the different zones defined where different actions are performed. The environment, location and type of the area to be protected are important factors for the design and definitions of these zones. The size and area that need to be monitored must be based on the threat that needs to be protected against. The findings will be important factors to define the size of the zones, where sensors are placed and what actions need to be taken and where. The larger the zones, the more difficult and expensive they are to protect. The configuration and number of zones can vary by implementation. In the end, these should be designed to give the amount of time needed to react and neutralise, causing the least amount of collateral damage. It should be planned so that all or the most sensitive parts of the site are protected. When defining these zones, it must be considered what authorities are needed to neutralise the threats and who has these rights. In many cases, there are different actors depending on the zone. All actors should therefore be included in the design of the processes and procedures. For this reason, it is necessary to closely analyse the needs and clearly define the processes and procedures around and inside the C-UAS security zones.

It is advised to have a multilayer of zones, as seen in Figure 15. The definitions and sizes must be aligned with the measures needed to mitigate the risk, what mitigation measures are authorised and with the stakeholders that are involved in the solution. The placement of sensors is closely related to the definition size and definitions of actions in the zones (see Section 3.2 for considerations on placement of sensors and what to take into account to get the correct coverage in all zones).

> The size of the zones and the actions linked to these should be defined in a way that gives all actors involved time to mitigate the UAS incident in an agreed way. The place of mitigation should be as safe and secure as possible, with minimum collateral damage and following rules and regulations.

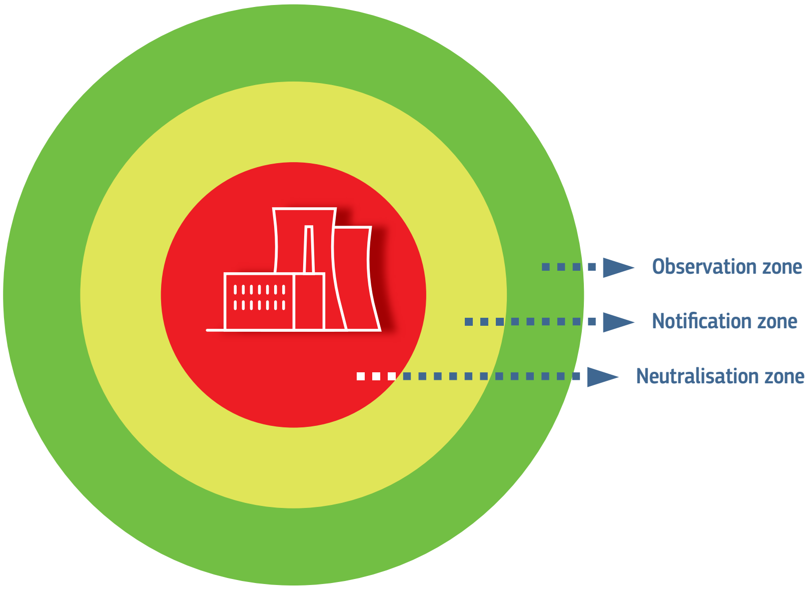
The UAS geographical zone is the airspace that can be allocated by the national civil aviation authority to a site owner to allow rules to be set for UAS operation[19]. This can be in the form of minimum specifications of the UAS, notifications, time limitations, where to operate, etc. It is also the zone where the zone manager will have some authorisation to intervene in the event of detected flights. Depending on the country and local regulations, this could include the use of mitigation measures. It is therefore very important to include the regulating authorities in the design and definition of actions that wish to be implemented.

[19] Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft.

In a layered C-UAS zones model:

- the inner layer is **the neutralisation zone.** It is the three-dimensional area of the UAS geographical zone where the CI or public space owner wants to neutralise any non-authorised UAS, using the measures defined to mitigate the risks identified. It is important that the size of this zone is defined correctly so that the neutralisation actors have the appropriate legal authority and the time to react when needed. This zone should be completely covered by detection systems.
- **The notification zone** is where threats are closely monitored and, when occurring, all actors get ready for mitigation following the processes and procedures defined. The size of this depends on the time needed to mobilise resources and get ready for intrusions into zones where neutralisation is needed.
- **The observations zone** is an area around the notification zone. This zone is used to observe activities that can be used to optimise the solution and awareness. This zone can be covered partially by detection systems.

Figure 15: Example of a layered C-UAS zones model



Some important considerations regarding these zones are the following.

- The **integration** and use of a UTM system is an important tool for airspace management and for integration with the U-Space and surroundings. Using a common UTM service (e.g. from the cloud) adds valuable information to any solution, **but a UTM is not a C-UAS solution**.
- If UAS usage is envisaged on the site or in the zones to be protected, how to manage and integrate this into the C-UAS solution should be investigated and planned.
- Request UAS geographical zone and airspace management from the responsible national civil aviation authority at an early stage of the solution design.
- Inform stakeholders and surroundings on this UAS geographical zone implementation.

- In most cases, it will be very useful to register as an UAS operator (as defined in EU legislation[20] [21]) to permit the use of flights for testing, training, surveys, etc.

- Make sure that all site insurances are updated to include the use of UAS of all types on and around the site to be protected. This is needed for site survey, for verification of sensors, penetration tests, training, etc.

- C-UAS System performance verification and validation tests should be designed to match the threat scenarios and be in line with what needs to be protected against. For example, it does not make much sense to perform a high-level terrorist attack test on a solution that is designed to protect against privacy issues monitoring is not a neutralization method.

- Putting up signs around the site in accordance with agreement with authorities and surroundings. This could be linked to an information campaign to inform surrounding stakeholders that the area is a no-UAS-flight area.

- Implement management processes and procedures internally and with external stakeholders (e.g. UTM, local stakeholders, LEAs, authorities).

Event logging

Logging of events is important to keep a solution effective and efficient. The design should be flexible enough to log manual observations, sensor detections and information received from external sources like UTM or from neighbours. The logs' retention time should be defined in a way that can be used to detect patterns. The analysis of logs should be done with regular intervals and used to update/upgrade the solution.

Information to be included must be sufficient to identify trends and to identify possible new threats (e.g. if somebody is trying to see if there is UAS protection). This could include detections that are not verified as UAS or classified as false positives. Logging should be centralised from all sources with information that is as complete as possible, examples are as follows.

- Direct and network remote ID as defined in Commission Delegated Regulation (EU) 2019/945 (UAS operator registration number and the verification code, unique serial number of the unmanned aircraft, time stamp, geographical position of the UAS, speed, route, pilot position, take-off position and emergency status).

- UAS information and all information available (media access control address, unmanned aircraft type, serial number, etc.).

- Detected by which detectors, persons, method, etc.

- Pictures, video and signal information to be used in forensics. Source of entry (e.g. external observation, UTM, other C-UAS solution, sensor and detector). Time and location information.

- Flight information and characteristics.

- Approved and non-approved flights.

[20] Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems.

[21] Commission Implementing Regulation (EU) 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft.

- Mitigation actions: if the system takes any actions to mitigate the detected threat, such as jamming or redirecting the UAS, these actions should be logged, including the time and type of action taken.
- False alarms: any false alarms triggered by the system should be logged, along with the reason for the false alarm and any corrective actions taken to prevent future false alarms.
- System performance: the system's performance metrics, such as detection rates and response times, should be logged to monitor the effectiveness of the system over time.
- User actions: any actions taken by authorised users of the C-UAS solution should be logged, including the time and nature of the action, and the identity of the user.
- System errors: any errors or malfunctions in the system should be logged, along with any diagnostic information that can be used to troubleshoot and resolve the issue.
- Operator actions.

All the information in the logging should be exportable so that it can be used in forensics by the appropriate authorities.

Physical protection

Physical protection[22] is an important mitigation measure against many UAS threats, however, it is often overlooked and it should be carefully evaluated. Physical protection measures can in some cases be easier, cheaper and faster to implement than expensive C-UAS systems.

Some examples are:

- foils on windows to counter threats from small UAS ramming windows;
- foils on widows to avoid filming from outside;
- nets above persons to avoid person injury;
- external blinds to avoid ramming;
- blast-proof glass and physical protection against small explosives;
- moving persons away from windows and positioning monitors so they cannot be viewed from outside.

RF monitoring

UAS use various communication frequencies for their operation. The frequency band used by UAS depends on the specific application, type of UAS and the region of operation. In general, UAS use both licensed and unlicensed frequency bands for communication with ground control stations, other unmanned aircraft and satellite communication.

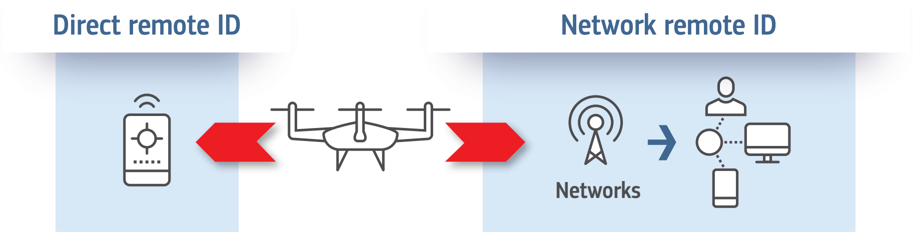
[22] Protection against Unmanned Aircraft Systems - Handbook on unmanned aerial systems risk assessment and principles for physical hardening of buildings and sites

The direct remote ID[23] is an open protocol signal that is transmitted in real time during the whole duration of the flight. This direct periodic broadcast from the unmanned aircraft using an open and documented transmission protocol can be received directly through existing mobile devices within the broadcasting range. It contains at least the following data.

- The UAS operator registration number and the verification code provided by the Member State of registration during the registration process.
- The unique unmanned aircraft serial number.
- Time stamp, the geographical position of the unmanned aircraft and its height above the surface or take-off point.
- The bearing measured clockwise from true north and ground speed of the unmanned aircraft.
- The geographical position of the pilot or, if not available, the take-off point.

The same information can be acquired using the network remote ID. While the direct remote ID is transmitted directly from the unmanned aircraft to a receiver, the network remote ID information is transmitted from the unmanned aircraft to the mobile networks (Global System for Mobile bands) from where it is distributed. This is illustrated in figure 17. When integrating a solution with external services that have available network remote ID information, it is desirable to integrate this information, but it is not considered an essential minimum service.

Figure 16: Types of remote IDs



While it is important to receive the ID from the UAS, it must be assumed that many UAS and especially non-corporative UAS will not transmit these. It is therefore essential to also monitor the most commonly used frequency bands for UAS communication, as indicated in Figure 18.

A commercial UAS can in many ways be compared to a Wi-Fi router, sending video frames and flight data to the pilot. Most commercial UAS use 2.4 GHz and 5.8 GHz, which are also the standard Wi-Fi connection frequencies. Detecting and interpreting the information of the UAS remote signals can provide valuable additional information, such as the UAS model and manufacturer, GNSS position, take-off position (normally related to the pilot position), percentage of battery, media access control address, type of UAS control commands and flight modes.

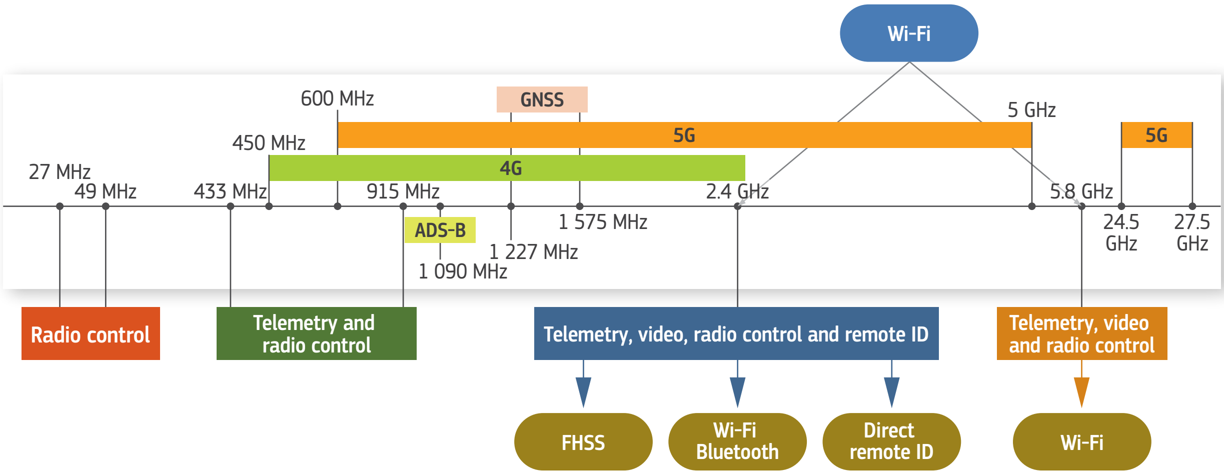
[23] https://www.easa.europa.eu/en/document-library/easy-access-rules/online-publications/easy-access-rules-unmanned-aircraft-systems?page=19.

UAS can also operate on licensed frequencies, such as the L-band (1–2 GHz) and S-band (2–4 GHz), which are commonly used for satellite communication. These frequencies provide reliable and secure communication over long distances, making them suitable for beyond visual line-of-sight operations. In addition to these bands, UAS also use other frequency bands such as the C-band (4–8 GHz) and Ku-band (12–18 GHz) for satellite communication, and the ultra-high frequency band (300–400 MHz) for defence applications.

The use of certain frequency bands may require regulatory approval, and different countries may have varying regulations regarding UAS communication frequencies. Therefore, it is essential to understand the regulatory framework of the region of operation to ensure compliance with local laws and regulations.

Despite being considered as 'easy-to-install' technology (passive RF antenna), the performance is directly related to the installation environment, such as the distance from buildings and trees. In addition, the RF technology detection range is dependent on receiver sensitivity and the power of the RF signal from the UAS transmitter.

Figure 17: Frequencies used by UAS



Stakeholder interaction

Stakeholder interaction is one of the essential minimum services that should be done in any solution design, since by including the stakeholders in the processes and procedures they are contributing to an effective and efficient implementation. Throughout all the C-UAS solution phases, various stakeholders will be involved. The exact stakeholders that should be involved in the C-UAS solution will differ for each site and the escalation level it adopts. The stakeholders should establish a common agreement on who does what, where and when.

Cybersecurity

For any implementation where ICT is used, ICT security hardening is mandatory. Since C-UAS systems are security information systems, and these are potentially integrated into other security systems, all network connections can potentially be used to enter and modify configurations or bring down systems. If the C-UAS solution is connected to the internet, these connections should be carefully analysed for security risks. The complete solution should be included in the site's business continuity plan, cybersecurity policy, security procedures and processes, and the accepted risk level.

3.2 SELECTING MITIGATION LEVEL AND MATCHING THE DETECTION TECHNOLOGIES

The design of a C-UAS solution includes selecting the appropriate threat response for the CI site or public space, and then matching those with the appropriate measures. Given the impact these measures can have on their targets, the environment they are operated in and the intention of operating these devices in civilian environments, the legality of such measures should be established before deciding on adopting them. Legislation on the use of technology differs per Member State. As such, each CI site or public space is recommended to inquire on the applicable rules with their national and local authorities.

An initial site assessment and survey will help to identify the best technology to meet the specified needs. Initial modelling should be used and be backed up by tests during the site survey.

Figure 14 illustrates the link between mitigation levels and technologies. The process of mitigation level definition, selection of technologies and stakeholder involvement should be repeated several times in the solution design. Regardless of the threat response, there will be several foundational measures that a CI site or public space should implement.

This methodology considers monitoring, soft mitigations and hard mitigations, but with no clear separation, see Figure 19. These are complementary and supplement the benefits that come with the foundational measures.

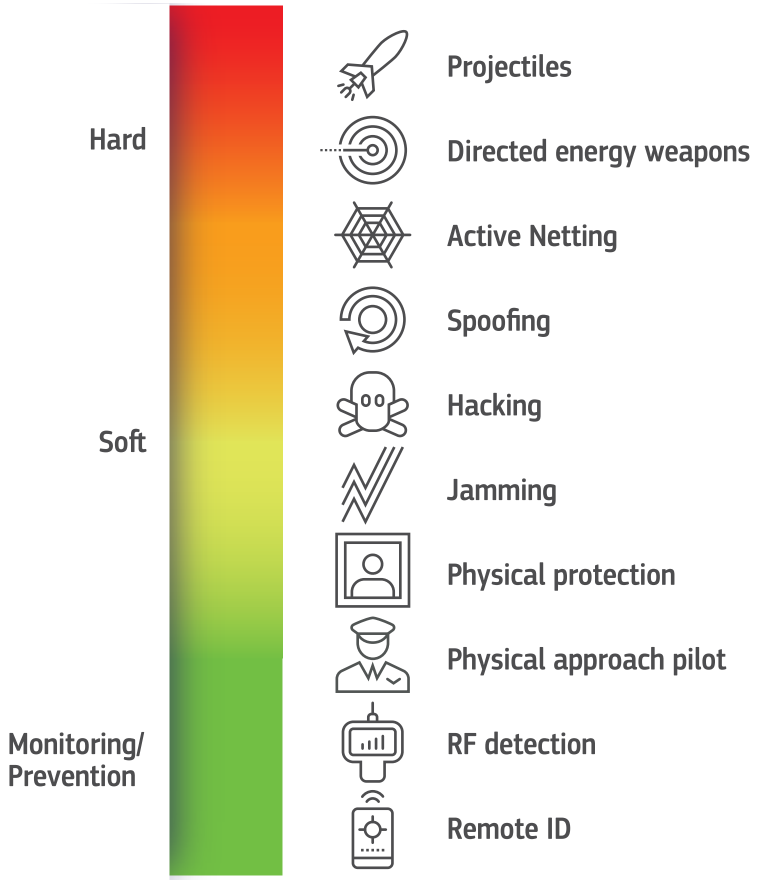
Monitoring/Prevention the lowest level of mitigation. This threat-response level refers to the detection and monitoring of UAS traffic within the zones defined and approaching UAS pilots. This involves taking non-intrusive actions if agreed boundaries or rules are breached. This lowest level of protection aims to create situational awareness of UAS use through the detection of UAS traffic in the area of the site to be protected.

Soft mitigation focuses on stopping current events with relatively harmless measures, which could include approaching the pilot(s) and the use of non-kinetic measures.

Hard mitigation is the highest level of mitigation out of the three. This level will use all available measures to stop UAS threats in the zones defined with the minimum collateral damage. This could be achieved with a combination of measures such as approaching the pilot(s), using kinetic and non-kinetic measures. All procedures will have to be properly implemented with approval from the authorities. The mitigation actors could be a combination of internal and external security, such as LEAs or the defence sector.

All measures and actions will need to be logged to improve the response capability.

Figure 19: Mitigation levels



It is important to have a well-defined mitigation process and procedures around this. This will be used for lessons learned and to be compared with other solutions. It can also be beneficial to use a methodology that is recognised and used by stakeholders of similar nearby implementations, and will help avoid misunderstanding and confusion when exchanging information. It must be stressed that there is no direct link between the risk mitigation level and the technology to use. The thresholds that attribute the risk scores with the escalation levels should be determined per solution individually.

These are to be complemented by additional design considerations linked to the mitigation needed to counter the UAS risk. Mostly, mitigation measures are considered to be kinetic or non-kinetic. Kinetic measures involve the use of physical force to disable or destroy a UAS, while non-kinetic measures involve the use of electronic or other means to disrupt or disable the UAS. The choice of measures will depend on the specific threat posed by the UAS and the operational environment in which the C-UAS system is being deployed. The use of and who can operate these mitigation measures must be implemented in accordance with national and regional rules and regulations.

The following describes the most common[24] and available measures.

[24] https://www.dhs.gov/sites/default/files/publications/c-uas-tech-guide_final_28feb2020.pdf.

Kinetic measures involve the use of physical force to disable or destroy a UAS. These measures include the following.

- **Directed energy weapons** (DEWs) use high-energy beams, such as lasers or microwaves, to disable or destroy UAS. DEWs are generally considered to be non-lethal, but can still cause damage to UAS components.

- **Projectiles or missiles**: anti-UAS missiles use explosives or other means to physically destroy the UAS. These missiles can be guided or unguided, and can be launched from a variety of platforms, including ground-based launchers or airborne platforms.

- **Small arms,** such as rifles or shotguns, can be used to shoot down a UAS. However, this approach can be difficult and dangerous, as it requires accurate targeting and can result in the unintended damage or destruction of other objects.

- **Netting** involves using specialised equipment to capture and immobilise a UAS in mid-air, preventing it from flying further.

Non-kinetic (electronic) measures, on the other hand, involve the use of electronic or other means to disable or disrupt the operation of a UAS. These measures include the following.

- **RF jamming** can be used to disrupt the communication between the UAS and its pilot, causing the UAS to lose control and potentially crash[25].

- **Spoofing** involves creating false signals to trick the UAS into believing it is receiving legitimate commands from its pilot. This can cause the UAS to change course or return to its point of origin.

- **Hacking** involves gaining unauthorised access to the UAS control system to take control or disrupt its operation.

When designing a C-UAS solution that takes into account the mitigation level, there are several factors to consider to ensure that the appropriate measures are chosen to effectively counter the specific threat posed by the UAS, see Figure 14. These are to be considered on top of the fundamental minimum services that should always be implemented.

Some important factors to consider include the following.

- Threat assessment. It is important to permanently assess the specific threats posed by the UAS. This includes understanding the UAS capabilities, flight characteristics, payload, along with the potential targets and the intended effect of the attack.

- The operational environment in which the C-UAS measures will be deployed should also be considered. Some factors (such as weather conditions, terrain, rural or urban area, noise, where sensors are installed, obstacles like high buildings) will affect the performance of the C-UAS system. For example, a solution used for a desert installation will be different to one used for protection in an urban area, a Christmas market, a water purification plant or a prison.

- The **zones** and their size, for example, are any of the parts of the zones shared with other protected zones.

[25] As the available devices are made to jam on frequencies approved for UAS communication, they will be ineffective to UAS with modified frequencies (see Section 3.1).

NO DRONES

- **Physical protection** measures implemented or plans to do so.
- UAS traffic information from **detection systems** and **data available from other sources**, such as airspace management initiatives (UTM and U-Space).
- Availability of **actors and stakeholders** that are authorised to operate mitigation measures. Are these available immediately or do they need to be contacted? For example, LEAs or the defence sector.
- Time needed to act in the end is probably the most important factor.
- **Cost** of the C-UAS measures should be considered. This includes the cost of the measures themselves, along with the cost of training personnel and maintaining equipment.
- **Interference and false positives** can be reduced by adding additional sensors or working with multiple types of sensors and fusing the data to gain better situational awareness. However, this will come at a cost.
- **Legal and ethical considerations**. The use of C-UAS measures can raise legal and ethical considerations. It is important to ensure that any chosen measures comply with relevant laws and regulations, and do not pose a risk to non-involved parties.

By carefully considering these factors, an appropriate mitigation level can be decided. It is important to revisit all these factors with regular interval to ensure the solution is updated with the current threat and updated technology specifications, see Figure 14.

Detection and tracking technologies used for C-UAS systems are many and their evolution is very fast. The following describes the most used.

- **A radar** is an electronic device that uses radio waves to detect and locate objects. It emits radio waves that reflect off objects in their path, and the radar system then detects the reflected waves to determine the location, speed and other characteristics of the object. Radars can be useful for detecting unmanned aircrafts at high altitudes and long ranges. However, radar waves may not penetrate through obstacles such as buildings or trees and may not be as effective in detecting smaller unmanned aircrafts at lower altitudes or in urban environments where there is a lot of clutter.
- **RF analysis** detect the RF signals emitted by the unmanned aircraft control system. As UAS use radio signals to communicate with their remote controllers, RF sensors can detect the signals emitted by the unmanned aircraft and its controller. RF sensors are useful for detecting smaller UAS at lower altitudes. However, they may not be as effective at detecting UAS that use frequency-hopping or other techniques that complicate detection.
- **Acoustic sensors** detect the sound generated by the unmanned aircraft rotors. As UAS fly, they emit a distinct sound signature that acoustic sensors can pick up. Acoustic sensors are useful for detecting low-altitude UAS and can be used in urban environments where other technologies may not be as effective. However, acoustic sensors may have limitations in detecting unmanned aircraft with quieter rotors or in noisy environments.
- **Electro-optical / infrared (EO/IR) sensors** use visual and thermal imaging to detect and track UAS. These sensors can detect the heat generated by the unmanned aircraft's motors or the visual signature of the unmanned aircraft itself. EO/IR sensors can detect unmanned aircraft in low-light conditions and can be useful in identifying the type of UAS. However, they may have limitations in detecting unmanned aircrafts at long ranges or in conditions where the unmanned aircraft's heat signature is masked by other environmental factors.

Sensor fusion software is used to combine signals from different sensors. This can be used to complement the sensors' signals and combine them into a common picture. This will allow for better detection coverage and ensure the best parts of all detection technologies available are used. For example, sensor fusion software can use computer vision and machine learning algorithms to detect UAS by analysing video feeds from cameras and combining them with radar information. This would allow UAS to be detected and tracked in real time and improve the monitoring of large areas.

While the technologies mentioned above are effective in detecting and tracking UAS, consideration has to be given when choosing a technology or combination of technologies for UAS detection. These variables are influenced by what UAS the site is trying to protect against. This relates back to the threat assessment from the previous phase risk and threat analysis. Additionally, checks should be done if the technologies are suitable for the site and if passive RF sensors or active radar technology are needed, the latter when legally allowed. Active measures are often more complex to deploy as more regulation applies to their use (e.g. spectrum licences and power limits for radar use).

The following are important elements to consider when designing the technical part of the solution.

- **Range.** Some technologies have a longer range and can detect UAS at greater distances, whereas other technologies may have a shorter range and may not be as effective at detecting UAS at long distances.
- **Environment.** The environment in which the UAS detection system is deployed can have a significant impact on the effectiveness of the technology. For example, radar may not be as effective in detecting UAS in urban environments where there is a lot of clutter or in areas with tall buildings or trees that can obstruct the radar signal.
- **Cost.** The cost of the technology is also an important consideration. Some technologies, such as radar, can be expensive to install and maintain, while others, such as RF sensors or acoustic sensors, may be more cost-effective.
- **False positives.** UAS detection systems can also be prone to false positives, which can reduce the effectiveness of the system. For example, RF sensors may detect signals from other devices or sources, and acoustic sensors may pick up sounds from other sources such as birds or aircraft.
- **Countermeasures.** Some UAS detection technologies may be susceptible themselves to countermeasures, such as signal jamming or spoofing. This can make the detection system less effective or even completely ineffective.

Some important UAS factors to take into account are the following.

- **Size of the UAS.** The size of the UAS can also affect the effectiveness of the detection technology. Some technologies may be better suited for detecting larger UAS, while others may be better for detecting smaller UAS.
- **Speed.** The speed of the unmanned aircraft determines the time there is to react to a threat. Considering a UAS flying at 60 km/h can travel 2 km in 120 seconds, as illustrated in Figure 21, during this 2-minute window, the C-UAS solution needs to detect, track, identify and mitigate the threat.
- **Type of flight.** If a perpetrator uses an automated flight, there will be no RF signal to be detected.

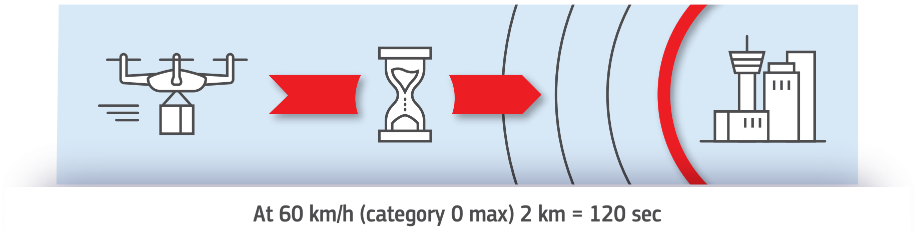
- **Position of pilot.** If the identification of the location of the pilot is an important factor, then the following should be kept in mind.
  - » Many detection systems read the pilot's position from the signals between the UAS and the remote controller. These can be modified or switched off.
  - » RF detection of the remote controller relies on the receipt of the signal transmitted the remote controller. The environment can make this very difficult or impossible.
  - » In case of an automated flight, there is no human pilot that controls the flight.

Side effects

The side effects of mitigation technologies are important and should be analysed carefully, especially for the following neutralisation measures.

- Jamming of control signals might also affect other equipment using the same RF band.
- Spoofing and hacking can affect the flight of the UAS, resulting in a possible crash or flying into other zones where it causes damage.
- Projectile or missiles travel beyond the target and can damage infrastructure and people.
- DEWs will damage the UAS, but they can also affect further devices.

Figure 20: UAS time needed to get to target



The more time needed to react and mitigate incidents, the larger the notification zone will need to be. A faster UAS needs to be detected further away to ensure there is time to launch mitigation measures.

TIP

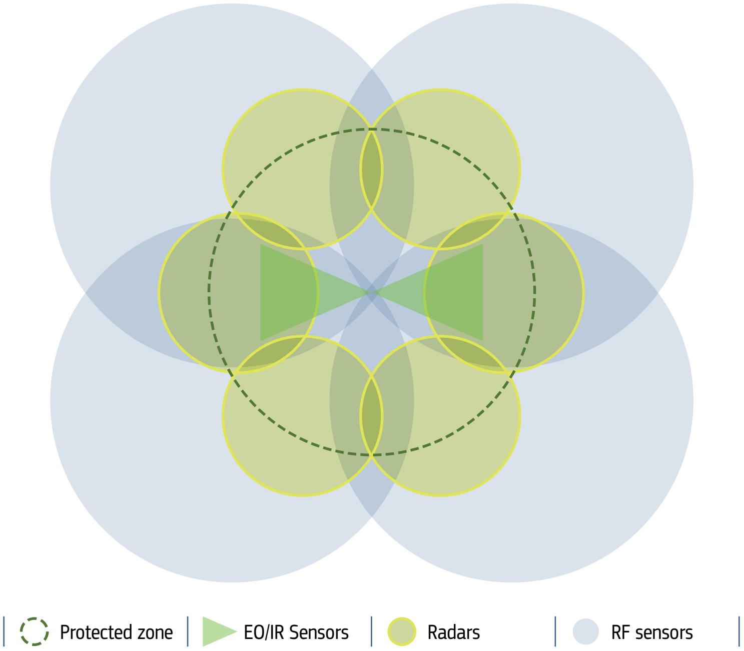
Once a potential threat has been detected and identified, the solution should respond quickly to mitigate the threat. This includes countermeasures such as approaching the pilot, jamming or other interceptions.

Placement of sensors

This part handles the placement of sensors that have been chosen to detect the UAS. To ensure the best detection coverage, the operational environment and potential threats regarding sensors should be analysed. This can be accomplished through the use of modelling and simulation tools, together with field testing and evaluation. All models and simulations should be verified in practice to ensure the correct detections and avoid blind spots.

Creating layered security using multiple detection systems, such as radar, cameras and acoustic sensors, should be considered to provide overlapping coverage and redundancy (i.e. Swiss cheese model[26]).

Figure 21: Example of zone protection with multiple different sensors



When implementing detection systems, it is crucial that the operational environment be taken into account. The terrain, weather conditions and potential obstructions will have a big influence on how good the solutions will work. Next deciding on the placement of detection systems needed for a solution, several factors are important and should be considered in order to ensure optimal protection coverage.

These factors include the following.

- Understanding of the specific threat posed by the unmanned aircraft, as described in the threat scenario's, in the area where the C-UAS solution will be deployed. This includes the type of unmanned aircraft that may be present, the operating altitude and speed of the aircraft, and the payloads that may be carried.

[26] The Swiss cheese model of accident causation illustrates that, although many layers of defence lie between hazards and accidents, there are flaws in each layer that, if aligned, can allow the accident to occur.

- Detection range and capabilities of the system should be taken into account when deciding on placement. The ability to detect different types of unmanned aircraft, as well as its range, accuracy and response time. Systems with longer range and higher detection capabilities are able to detect UAS from further away and with greater accuracy, which can provide more time for response.

- Terrain and obstacles in the area can impact the effectiveness of detection systems. For example, as shown in Figure 23 and Figure 24, buildings, trees or other structures can block or reflect signals, while hills or mountains can limit line-of-sight detection range.

- Placement that avoids attenuation or reflection from sources, such as buildings, foliage and water.

- The logistics of deploying the detection system should also be taken into account. This includes the availability of power and network connectivity, and the accessibility of the area where the system will be installed.

- The operational environment, including terrain, weather conditions and potential obstructions, should be considered when deciding the placement of detection systems. This includes identifying potential areas of vulnerability and placing detection systems in strategic locations to provide the best coverage. The environment and location will have a significant impact during the decision-making of a sensor's installation.

- To increase the detection range, mounting sensors on infrastructure, masts or towers could be considered. Additionally, a distributed system of sensors can be considered, see Figure 24.

- Integration with other C-UAS measures. The placement of detection systems should also be considered in relation to other C-UAS measures, such as kinetic or non-kinetic measures. Placing detection systems in strategic locations can enhance the effectiveness of other C-UAS measures.

Electromagnetic interference should also be checked for when deciding on the placement of sensors. This is also called RF interference in the RF spectrum. Electromagnetic interference is a disturbance generated by an external source that affects an electrical circuit by causing electromagnetic induction, electrostatic coupling or conduction. For example, the use of radar in mobility (e.g. speed cameras, car radar systems) can generate interference sources with C-UAS radar systems or vice versa, impacting the sensor data quality and possibly generating false positives. Other possible sources could be mobile phones, cosmic noise, lightning or electric power cables.

Sensors may require line of sight and detection can be directly impacted by obstructions. Signal attenuation or reflection sources that should be taken into account include structures (vicinity of high buildings, wind turbines, water towers and industrial plants), woods (dense foliage areas and potential growth of trees) and water (proper care should be given near rivers, sea, lakes, etc.). Additionally, higher frequency bands are often impacted by meteorological phenomena such as fog, rainstorms and snow accumulation on sensors.

Therefore, the operational environment, including terrain, weather and potential obstructions, must be thoroughly considered when deciding on the placement of detection systems. The detection range, physical obstructions and electromagnetic interference should be carefully evaluated to ensure accurate detection and to minimise false positives.

Figure 22: Example of sensor blind spots (orange zone)

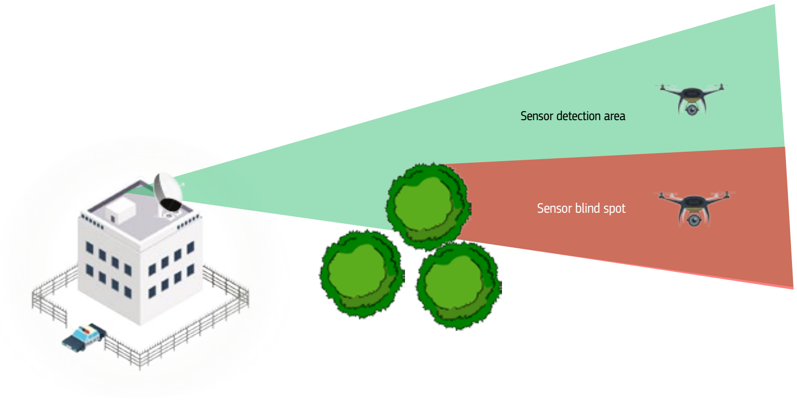
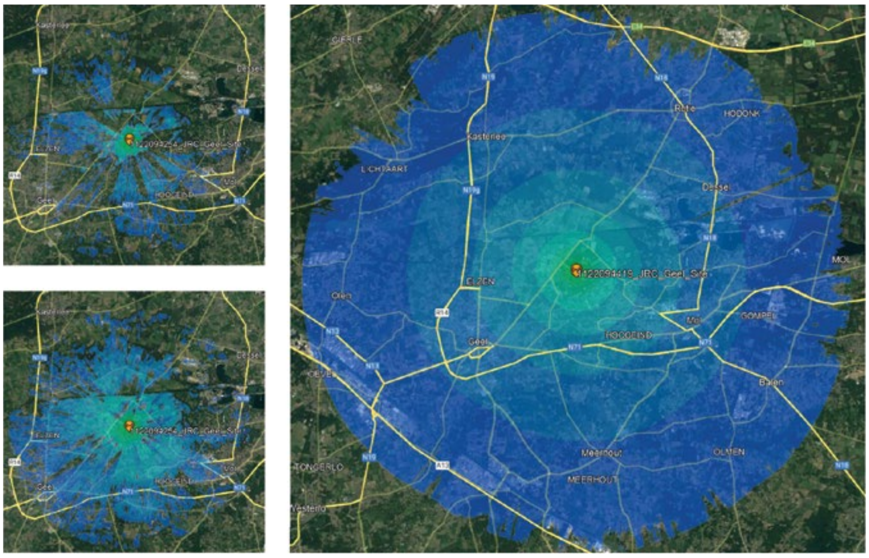


Figure 23: Blue area shows the detection coverage – different coverage was achieved by changing the placement of the sensor



3.3 SOLUTION ARCHITECTURE DESIGN – BRINGING IT ALL TOGETHER

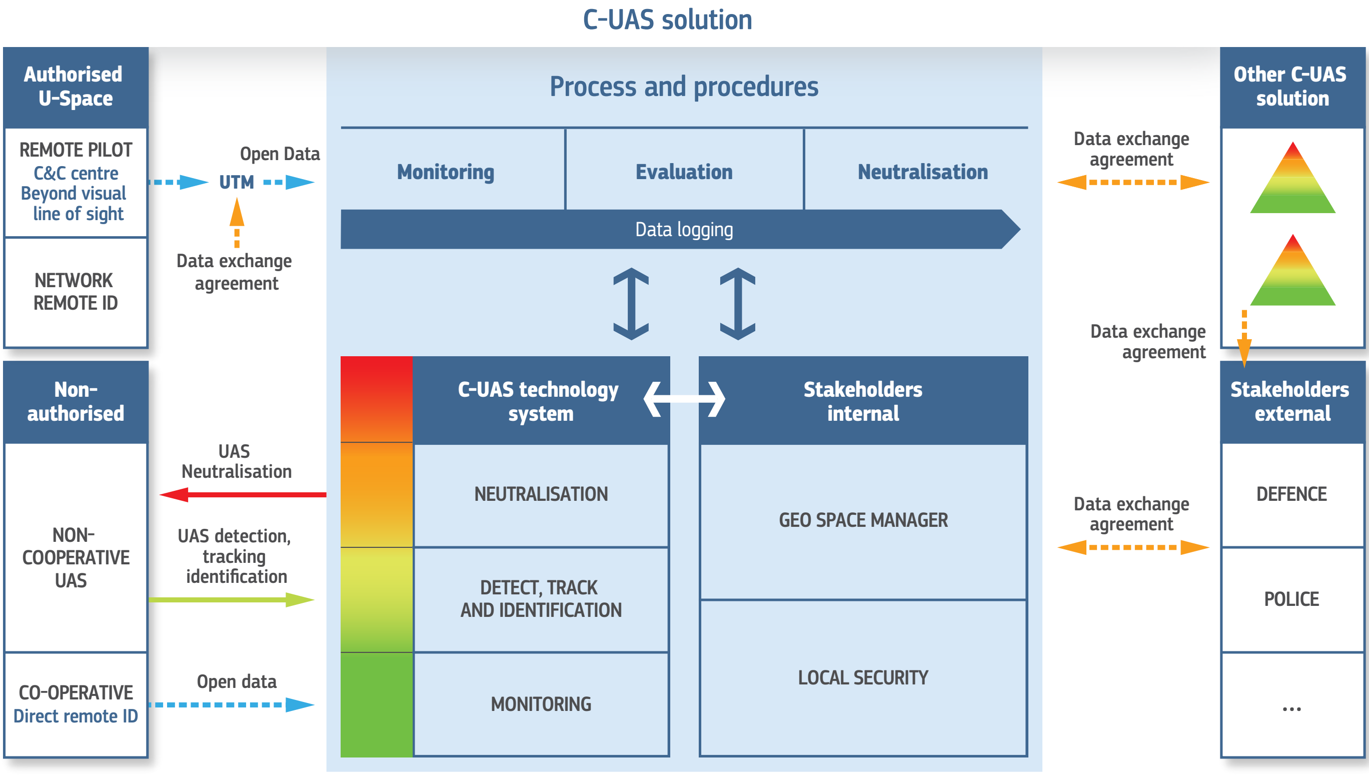
The solution design determines its future capacity to remain relevant and updated over its intended lifetime. The solution architecture is a key element that typically involves a combination of processes, procedures, hardware, software and network components.

Some key components that might be included in a typical C-UAS solution architecture are the following.

- **Sensors.** These might include various types of sensors, such as radar, EO/IR and acoustic sensors, which are used to detect and track potential UAS threats.
- **Communication systems and network Infrastructure.** These are used to transmit sensor data to a central command-and-control (C2) centre, where the data can be analysed and used to make decisions about how to respond to the threat. The C-UAS solution might include a range of network components, including servers, routers and switches that are used to transmit data between the various components of the system.
- **C2 centre and Graphical User Interfaces.** This is the nerve centre of the C-UAS solution, where all sensor data is received, analysed and used to make decisions about how to respond to potential UAS threats. The C2 centre might include a range of software tools for data analysis, visualisation and decision-making.
- **Effectors.** These are the tools used to mitigate UAS threats. They might include jamming systems that disrupt the UAS's communications or navigation systems, or other tools like lasers that are used to disable or destroy the UAS.
- **User interfaces to other stakeholders.** These are the interfaces to be used by stakeholders to interact with the C-UAS system. They might include graphical user interfaces for data visualisation and decision-making, or more specialised interfaces to communicate information or data and for controlling the effectors used to mitigate UAS threats.

Overall, the architecture of a C-UAS solution is designed to detect potential threats, analyse the data to determine the appropriate response, and then deploy effectors to neutralise the threat. The specific components of the solution architecture will vary depending on the specific requirements of the system and the types of threats that it is designed to address.

Figure 24: Example solution architecture

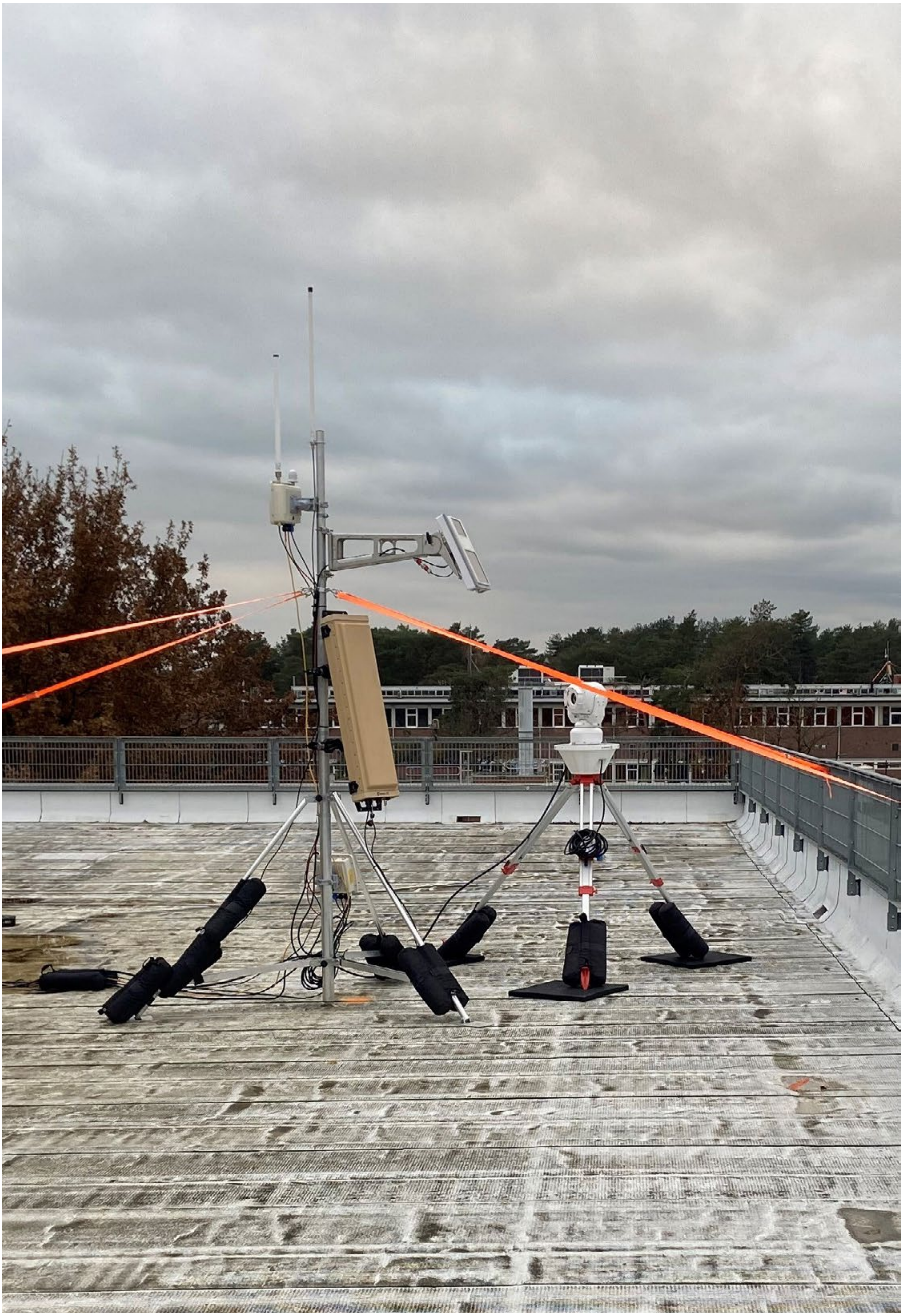


This handbook recommends designing a C-UAS solution with an open architecture, which allows for the integration of hardware, software and components using common standards. This makes it easier to add, change and replace components developed by other companies.

As technology inevitable progresses and evolves, additional capabilities become available on the C-UAS market and changes to a site's situation and consequent risks will result in the need to adapt its solution configuration. Consequently, having a solution in place that is built with an open architecture approach would lead to lower complexity and costs in the event of solution changes.

Open architecture systems sometimes suggest the following quality attributes in their designs.

- **Adaptability.** The applicability to the requirements of different platforms.
- **Modularity.** Components should be detachable from the system independently.
- **Portability.** The solution should be transferable from one system to another.
- **Scalability.** The solution should scale to be larger or smaller according to need.
- **Interoperability.** Effective data sharing with other systems.



Beyond these characteristics, an additional driver of design decisions will be the costs of the system. This will ultimately be a function of the C-UAS budget available. This handbook recommends searching for industry and architecture standards and generic protocols widely accepted in the C-UAS industry for their solution, to enable interoperability.

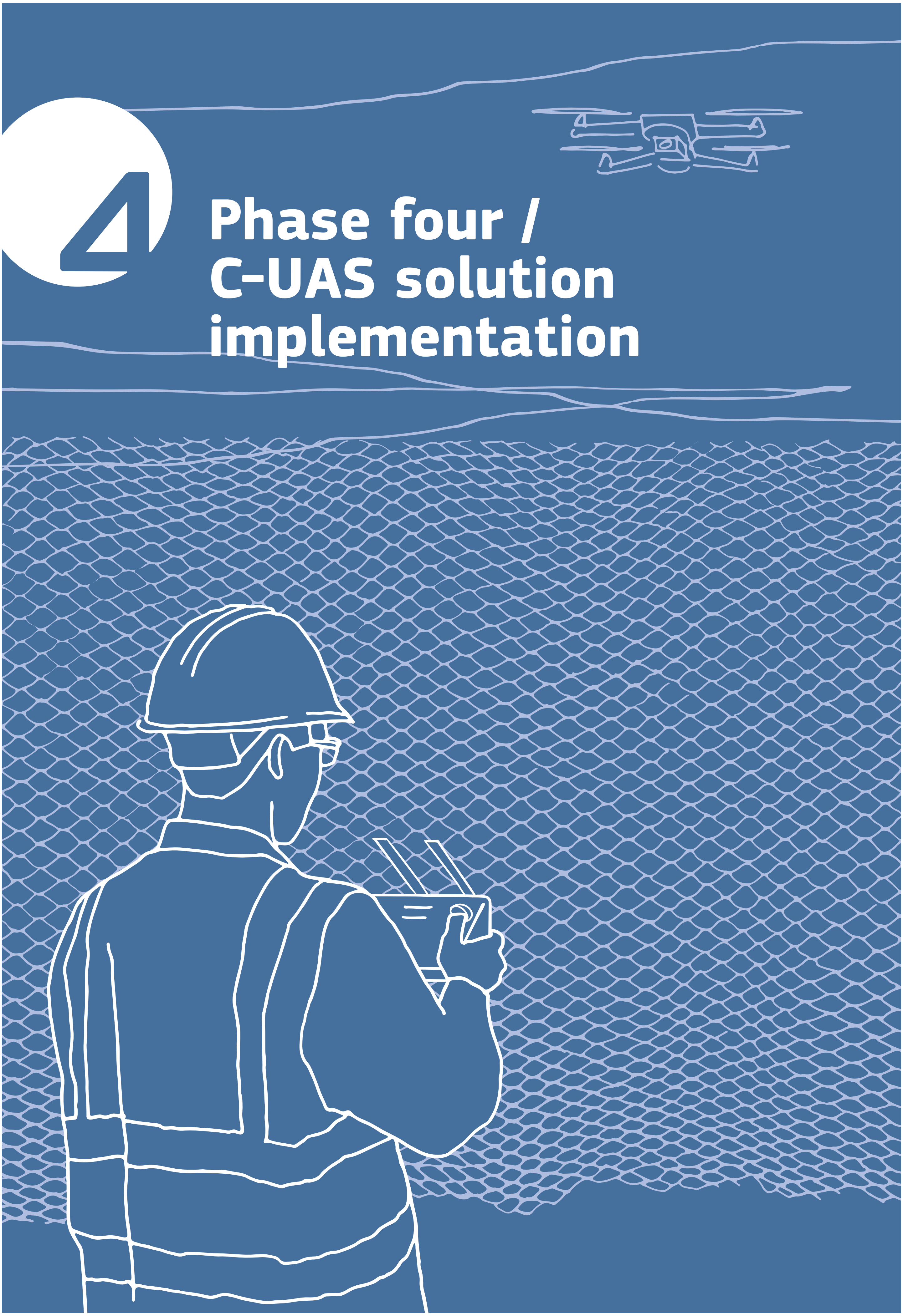
BOX 8: DESIGN PHASE SUMMARY

At the end of the design phase, information should have been collected and plans should have been made. These will include needs from the site, the location, the environment, stakeholders, regulations, authorities (national and regional), etc.

The format and detail of these documents and plans can vary and should be updated when necessary. Some examples of documents are:

- site risk register;
- threat understanding;
- legislative understanding;
- an updated site survey;
- a solution design that is appropriate for the site needs;
- solution architecture and specifications;
- site and environment information;
- processes, procedures and operation plans;
- updated stakeholder analysis with clear roles and responsibilities;
- risk and threat understanding and the threat scenarios that need to be mitigated and protected against;
- clear identification of roles and responsibilities of all stakeholders;
- high-level solution architecture;
- solution requirement specifications.

4 Phase four / C-UAS solution implementation

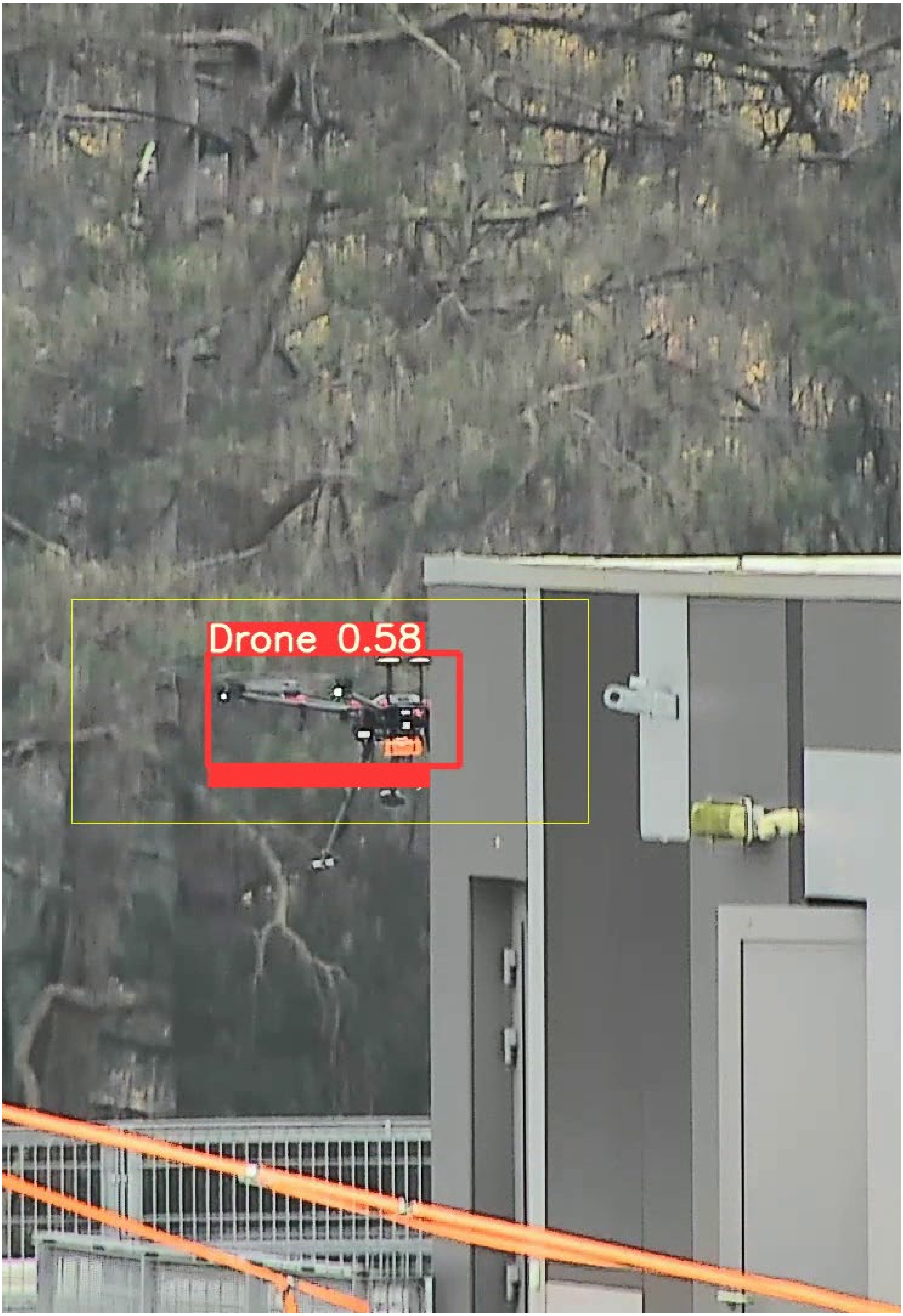


Once all requirements have been clearly defined, the solution designed, the integrator(s) selected and the system specification defined, a solution implementation plan should be made. This will need to be developed in collaboration with all stakeholders. Depending on the requirements, it may be necessary to use multiple integrators with complementary capabilities. For example, a UTM or UAS-oriented software provider that processes and visualises data generated by a C-UAS hardware provider. If this is the case for a site, it is advised to consider working with integrators that already have a regular set of partners. This will improve the chances of the solution being fully integrated and tested and proven. Working with multiple suppliers and coordinating their work to get to a common solution can be a difficult task. A good project manager with experience in the field is essential. Additionally, the contracts with the suppliers should be detailed and specific to clearly identify all stakeholders' responsibilities and, especially, the interfaces between processes. In many cases, it can be beneficial to use service models with specific and detailed service level agreements (SLAs). For the on-site implementation to start, all stakeholders, facilities and infrastructure should be ready. It is important to have a clear understanding of these implementation prerequisites from the C-UAS solution provider(s) as early as possible to minimise problems and avoid long delays. The implementation phase will include the time planning for installation, testing and calibration requirements, training of operators before acceptance and handover to operational staff. Not having identified prerequisites can reflect in a significant delay, last-minute workload and budget increase.

Examples of such prerequisites are:

- permissions to use technologies (e.g. frequency use licencing);
- regulatory approvals;
- dedicated buildings or changes to infrastructure;
- changes to the environment, such as removal of vegetation, and changes to topology and site surroundings;
- places on infrastructure where sensors can be mounted;
- cabling and network infrastructure, including network connectivity and telecommunication needs;
- availability of electricity where sensors will be mounted.

The advice in this section should be used as a guide to integrate the C-UAS solution into normal site security and operation.


Drone 0.58

BOX 9: PHASE FOUR – SOLUTION IMPLEMENTATION

The following are points that need to be collected before starting the implementation phase:

- solution design;
- site survey;
- clear requirement description of the solution that needs to be implemented;
- threat scenarios;
- solution and system specifications;
- architecture design;
- implementation requirements;
- stakeholder processes and plans (who does what, where and when?).

At the end of this phase, you should have:

- an implemented solution that is compliant with the organisation and risk mitigation needs;
- updated operational manuals with processes and procedures;
- test and calibration reports;
- a solution transition plan;
- updated stakeholder lists;
- completed training and updated training plans;
- integrated the C-UAS solution into normal operation;
- a complete file that enables handover from installation to operation.

4.1 CALIBRATION, SYSTEMS AND C-UAS SYSTEM PERFORMANCE VERIFICATION AND VALIDATION

Technical and calibration tests are an important step in the implementation phase. These tests need to be designed and performed in a way that will show the correct functioning of the complete solution. These tests could be broken down into smaller tests but, in the end, all elements should have been tested. A final solution test that covers all procedures and processes together with all systems should be carried out.

Test procedures and protocols should be clearly documented so that the tests can be repeated at regular intervals. The results, all sensor data and interactions should be documented in reports. Often this is done by the solution supplier, but having an independent party involved in both the design and the execution of these tests should be considered.

External experts could be beneficial, especially for penetration tests. Penetration tests should be representative of the identified risks, threats and scenarios for the particular solution. An external 'red team' test could ensure that these are more comprehensive.

All stakeholders that will play a future role in operating the solution should participate in all these tests. Their input and validations are essential. The tests are also a good opportunity to train stakeholders and demonstrate the solution to business.

4.2 INTEGRATING WITH EXISTING PROCESSES

Integration of the implemented solution and system with existing processes (like safety and security rooms), potentially creates the need for new processes. Depending on the threat-response level and corresponding technology choice, these needs will vary. Impact and integration analysis should be performed well in time to ensure a smooth transition into operations, especially if these process changes require internal or external approvals. Key outcomes from this analysis should be reflected in transition, training, operation and maintenance plans.

4.3 EDUCATE AND TRAIN THE OPERATORS AND STAKEHOLDERS

New or updated processes, additional systems and processes, ways of working and operational changes will introduce the need to train new or retrain staff and stakeholders. Users of new human-machine interfaces, monitoring tools or hardware use and maintenance should be trained accordingly.

A careful analysis and training plans are recommended. These should take into account key factors such as staff availability and training recurrences. Training mission-critical personnel typically requires longer upfront resource planning and poses challenges to capacity planning. The training plans will likely have been started during design phase.

Training of stakeholders on the C-UAS solution should be a priority to ensure optimal functioning of the solution. The interpretations and application of regulations (EU and local) should be included in training.

As the places of operations could change from inside a site boundary to operating in the zones around the site, this should be considered in training. The regulations and procedures in these zones will be different and training will help teams operate the solution optimally. Where possible, it could be beneficial to involve local authorities, LEAs, neighbours, airports, airfields and UAS clubs in training. This could test more elements of the C-UAS value chain.

4.4 ACCEPTANCE AND HANDOVER TO OPERATION

Project acceptance and handover to service mode refers to the process of transferring a completed project from the project team to the operational team, who will be responsible for maintaining, operating and delivering the solution protection to the site. The handover process is a critical step in ensuring that the project's objectives have been met, and the final protection is delivered in accordance with the risk, design and business needs. When installation, testing and training have been completed, the solution should be handed over to the operational team. This important step is often overlooked and underestimated, resulting in poor handover where the implementation phase gradually ends with production. This can lead to unclear roles and responsibilities and result in poor overall solution efficiency.

Project acceptance and handover to production should therefore include the following steps.

- The project team should conduct a final review of the project to ensure that it meets the defined solution requirements, is free of defects and meets the quality standards.
- The project team should document the solution including all relevant documents, such as design documents, test results and plans. This documentation will serve as a reference for the operational team.
- Handover meetings should be conducted between the solution implementation team, operational team and business owner to discuss the processes and the requirements for the handover process.
- Clearly define the roles and responsibilities of each team member involved in the handover process. This will ensure that everyone is aware of their duties and can perform them effectively.
- The implementation team should transfer all knowledge and expertise to the operational team so they can maintain and operate the solution effectively.
- The test and penetration results should be documented.
- All access to systems (ICT, passwords, access rights, etc.) should be reviewed and changed according to local security policies and procedures.
- A clear handover file and agreement between implementer and business owner should be made.

BOX 10: THE IMPLEMENTATION PHASE SUMMARY

At the end of this phase, you should have completed the solution implementation in accordance with the design documents and completed:

- the implementation of the solution that is compliant with the organisation and risk mitigation needs;
- updating operational manuals with processes and procedures;
- testing and calibration with reports;
- training and updated training plans;
- the updates of stakeholder lists;
- the integration of the C-UAS solution into normal operation;
- a solution transition file that enables handover from installation to operation;
- the installation and handover to business owner.

5

Phase five / operating the C-UAS solution

Following a successful risk analysis, design and implementation, the solution transfers into operational mode. The solution should now be integrated into the business processes and operated by the team responsible for site security. The procedures include all the information needed to mitigate the risks that the solution has been designed to protect against. All solutions will probably be unique as the complexity and integration of the solution will be different.

In this final section of the handbook, there are additional factors to consider when operating the implemented C-UAS solution. The C-UAS solution should now be integrated into the normal security processes and managed in line with the rules and regulations of the site where it is implemented.

BOX 11: PHASE FIVE – SOLUTION OPERATION

Information needed for this phase:

- operation manuals and procedures;
- trained and informed operators that are aware of the rules and procedures;
- testing and verification that the solution is working as required;
- monitoring and possible adaptation of key performance indicators (KPI) and SLAs to be complied with.

During the operation of a solution, the following should be recorded so it can be used for continuous solution updates:

- incident logging (manual and automatic system logging),
- lessons learned and list of problems,
- incident reports,
- feedback from law enforcement entities and external stakeholders.

5.1 KEEP STAKEHOLDERS INVOLVED AND INFORMED

Keeping stakeholders involved and informed is crucial for the success of any project or operation. For security reasons, this can of course sometimes be difficult, and the information shared should only consist of what is needed without compromising general security. Below are some considerations on how to keep stakeholders involved and informed.

- Clearly identify stakeholders, their interests and what they need to know. This will help you tailor your communications and engagement activities to their needs. This includes both internal stakeholders (employees, management) and external stakeholders (LEAs, customers, vendors, partners).
- Develop a communication plan that outlines how you will communicate with your stakeholders, what information you can and will share, and how often. Carefully analyse which channels to use (emails, social media, newsletters and meetings are the best ways to reach your stakeholders).
- Provide regular updates on the project's progress and any changes that may affect stakeholders. Make sure to highlight the positive impact the project is having on the organisation and its stakeholders.
- Solicit feedback from stakeholders to understand their concerns and suggestions. Incorporate their feedback into your project planning and execution.

- Where possible, engage stakeholders by inviting them to participate in meetings, workshops or other activities.
- Be as transparent as possible about the project's objectives, challenges and risks. This will help build trust with stakeholders and increase their confidence in the solution protection.

Clear identification of stakeholders' roles, responsibilities and involvement is therefore very important and must be managed well. Figure 26 is an example of a RASCI table, which can be used to map stakeholders. Such a table can be as extensive as is needed and should be tailored to the solution needs.

Figure 25: Stakeholder RASCI table example that can be extended as needed

	Stakeholder												
Task	Business owner	Local security	Solution operator	Mitigation actors	Law enforcement	C-UAS solution supplier(s)	U-space service provider	UTM service supplier	Authorities	Local community	Neighbours	Telecom operators	Government entities
Incident management													
Record and logging	A	R	R	I	I	I	I	I	I	-	-	-	I
Communication to stakeholders													
Inform authorities													
Forensics collection													
Update risk register													
Mitigate													
Approach pilots for soft mitigation	R	R		R	A	A	R			I		R	R
Supply information on 4G-5G flights	R	R		R	A	R	R			S		S	S
UAS flights													
Approve flights	A	R		I	-	-	I	I	-	-	-	-	-
Integrate flight plans													
Update flight logs	A	A		A	S	C	A			I		A	A
Update and service UAS													
Operation of solution													
C2 management	A	A		A	R	C	A			I		S	R
Service level performance checks													
Operator schedules													
Incident logging	A	A		A	S	C	A			I		I	I
Add incidents reported from other source to log	C	C		C	A	C	A			C		C	A
Observe and supply flight data	S	S		S	S	S	S			S		I	S
Operator training													
Communication to stakeholders													
Communication to business owner													

	Stakeholder												
Task	Business owner	Local security	Solution operator	Mitigation actors	Law enforcement	C-UAS solution supplier(s)	U-space service provider	UTM service supplier	Authorities	Local community	Neighbours	Telecom operators	Government entities
Penetration tests													
Plan tests													
Execute tests													
Log test													
Communicate and report results													
Solution performance													
Plan tests													
Verify results													
Update test plan													
Callibrations													
Service and repairs													
Maintenance schedules													
Service contracts													

R = responsible	A = accountable	S = supporting	C = consulted	I = informed	- = Not applicable

5.2 KEEPING THE C-UAS SOLUTION UP TO DATE

Any C-UAS solution is expected to be subject to several changes throughout its lifespan: it could face challenges such as technological advancements, change of legal framework, internal policy or process changes, or be subject to changes to the site's risk level acceptance. In all cases, close monitoring of the factors expected to influence a specific CI site or public space is advised. Building a solution roadmap that is monitored and kept up to date ensures that the CI site's or public space's C-UAS solution meets the needs and protects the site accordingly.

TIP

A solution is designed for protecting against and mitigating a specific threat. When any element such as the threat picture, the environment, business needs or the security level changes, all phases should be revisited. The fundamental minimum measures are the base of any solution and using these with design principles and open architecture will make updates and changes easier.

KPIs can be an effective method to measure the solution's performance over time and to monitor whether its objectives are met. Defining or selecting them can prove to be challenging, and KPIs should not end up identifying technical details but instead measure the protection level that the solution was designed to reach. Well-defined KPIs will reflect the performance of the systems the suppliers and integrators have used and can be used to compare the solution with another comparable implementation.

Facing technological changes can be a challenge, as not only detection equipment and software are subject to evolution, but so are UAS to be protected against. For example, the design changes of propellers and the material used to make the aircraft can make the UAS increasingly difficult to detect. Performing regular system tests and penetration tests will help to ensure the solution remains well tuned and aligned with current needs.

Avoiding a vendor lock-in serves as another commonly understood best practice. Making sure that the systems' core infrastructure is as vendor agnostic as possible will enable different suppliers to carry out services, maintenance and updates when needed.

When dealing with both hardware and software integrators, it is worth exploring an 'as-a-service' approach to the solution rather than owning it. The main advantage of an 'as-a-service' model is that the CI site or public space mitigates the risk of technological obsolescence. Naturally, such implementation models require site-specific analysis, taking other factors into account such as legal frameworks, data location, data ownership, operating cost, system monitoring and SLAs, internal capacity, know-how and training requirements.

It is important to carefully consider and mutually agree on SLAs with the vendor or integrators. These should be formalised into a detailed service agreement where mutual responsibilities, together with mitigation strategies for C-UAS solutions, are described. Here too a solid system specification and design, resulting from a comprehensive requirements analysis, helps avoid pitfalls and future discussions, for example, dealing with the detection of false positives or false negatives.

The proposed phase five methodology does not stop here. As indicated at the start of the handbook, this is a circular process, where lessons learned during the implementation and operational phases, along with the rapidly evolving threat picture and technologies involved, will lead to a continuous review of the solution operated.

BOX 12: THE OPERATION PHASE SUMMARY

This is the continuous process of operating the solution. During this phase you should:

- monitor that the solution meets the specification and protects against the risk identified;
- keep stakeholders informed;
- continuously update processes and procedures;
- operate the solution compliant with business needs, rules and regulations;
- monitor changes to business needs, technologies, stakeholders, the environment, threat pictures, etc. and when changes are needed restart all phases of this handbook – all information and changes should be recorded and kept updated.

Conclusion

In recent years, the use of UAS – commonly referred to as drones – has gained momentum. Europe, and the rest of the world, is observing a vast increase in the use of UAS for various purposes. The applications of UAS range from civilian use by hobbyists, to commercial use with new business models and defence use.

This handbook proposes **a five-phased methodology** for CI owners and those responsible for protecting public spaces on how to develop a solution to mitigate UAS threats. This methodology provides a wide perspective to the problems that UAS pose for CI and public spaces. It demonstrates the importance of developing solutions that include the complete value chain – integrating stakeholder processes with technological C-UAS systems. Where the C-UAS systems focus on the technical complexity of detecting, tracking and identifying UAS, the C-UAS solution involves all aspects and relevant stakeholders to mitigate threats that arise from UAS. The methodology describes the steps to be taken into account when creating a C-UAS solution.

The first phase of the methodology is advice on how to get started, by getting a clear business mandate and clearly defining the objectives on what and where to protect, and against who. It describes clear design principles and which stakeholders need to be involved when developing procedures and processes. In this phase, the essential minimum measures that all C-UAS solutions should be based on are described.

The second phase covers the UAS risks that need to be added to the current risk register and how to define relevant specific UAS-threat scenarios depending on which CI or public space should be protected.

Based on this analysis, **the third phase** describes how to design a solution that matches the business needs and the risks identified. It describes important consideration when implementing the foundational minimum measures, and how to build on these by selecting the correct mitigation level and matching the technologies needed. The end of the design phase will consist of designing an architecture that can be used in discussions with suppliers (who will implement the solution) and stakeholders (who will mitigate the risks).

The fourth phase of implementation is then described. This highlights the need for system testing and penetration tests before the stakeholders can be trained and the solution can enter into service mode. Identifying the correct stakeholders and their involvement is essential to ensure the solution is efficient and mitigation can be done within the time frame identified. As C-UAS will probably need additional stakeholders compared to normal security, it is important to contact and involve these at an early stage and develop the solution, procedures and processes together.

The fifth phase covers the operation of the solution, the need to keep stakeholders informed and keeping the solution up to date. Continued monitoring, well-defined KPIs, maintenance and updates ensure that current and new needs are added, as are additional stakeholders.

The business needs for C-UAS must be well understood. The vast and complicated technological landscape of C-UAS measures can sometimes divert the focus away from the original business problem that initiated the need for C-UAS. This can lead to inefficient use of resources and poor choices of technology that will fail to provide the required solution.

The foundational minimum measures should be implemented in all solutions. These form the base that enables a solution to evolve with changing risks and business needs. Additionally, the specific technologies needed to mitigate the risks can be connected and, when needed, the solution can be modified to cover environmental and risk changes.

There is no single solution that fits all implementations. Using solid design principles will make it easier to integrate a C-UAS solution into a site's security operations, making it more efficient. Each phase of the methodology must be tailored to the specific environment and risks. All sites operate in a different environment, with different relevant stakeholders, different markets, different communities and so on.

Sufficient time should be taken to explore the environment from a UAS perspective. Creating awareness by talking with neighbouring CI sites, local authorities and the civil communities will facilitate a C-UAS solution.

Lastly, the process of creating a C-UAS solution does not end with the last phase of this methodology. As the environment evolves, so does the threat landscape and the technological landscape. The five-phased methodology should therefore be repeated iteratively so that the C-UAS solution evolves accordingly.

List of abbreviations and definitions

Abbreviation or term	Description
Active measures	Measures designed to physically stop a detected UAS.
‘careful’ UAS operator classification	UAS operators that are aware of, and adhere to, regulations, drone control measures and safe drone operations.
‘careless’ UAS operator classification	UAS operators that may be aware of, but may not adhere to, regulations, drone control measures, and whose intentions are deemed to be reckless.
CI	Critical Infrastructure An asset or system that is essential for the maintenance of vital societal functions.
‘clueless’ UAS operator classification	UAS operators that are not aware of, and do not adhere to, regulations, UAS control measures, safe UAS operations but whose intentions are deemed to be non-malicious.
‘criminal’ UAS operator classification	UAS operators that may be aware of, but do not adhere to, regulations, UAS control measures, and whose intentions are deemed hostile.
C-UAS	Counter UAS is to lawfully and safely detect, track, identify and mitigate the risks of unmanned aircraft systems.
C-UAS system	C-UAS system is a component of a solution designed to perform C-UAS
C-UAS solution	C-UAS solution is a collection of C-UAS systems, stakeholders and processes involved in operating them
DEWs	Directed Energy Weapons
Direct Remote ID	‘Direct remote identification’ means a system that ensures the local broadcast of information about a unmanned aircraft in operation, including the marking of the unmanned aircraft, so that this information can be obtained without physical access to the unmanned aircraft.
EO/IR	Electro-Optical / InfraRed

Abbreviation or term	Description
Escalation level	Descriptions of the continuing and increasing level of risks. The attribution of escalation levels per risk score are decided by the site, based on perceived danger from the risk and threat analysis.
GNSS	Global Navigation Satellite Systems
Hacking	Hacking seizes the root privileges of the UAS's operating system and issues appropriate operations. The drawback of this method is that it only deals with specific operating systems and network protocols and, as with RF jamming, it interferes with other industrial, scientific and medical band devices.
ICT	Information and Communications Technology
ISO	International Organization for Standardization
JRC	Joint Research Centre
Kinetic measures	Kinetic mitigation techniques often involve some direct physical action for removing or reducing the risk posed by a UAS.
KPI	Key Performance Indicator
LEA	Law Enforcement Agency
Network remote ID	Network Remote ID makes use of communication by means of the internet from a network Remote ID service provider that interfaces directly or indirectly with the UAS, or with other sources in the case of non-equipped network participants.
RASCI	Responsible, Accountable, Supportive, Consulted, Informed RASCI is a matrix (i.e. chart, model or framework) that is used to help identify all the roles and responsibilities of each stakeholder on a project. It clearly defines who is working on a specific subtask of a project.
RF	Radio Frequency
RF jamming	RF jamming disrupts the RF link between the drone and its operator by generating large volumes of RF interference. Once the RF link (which can include Wi-Fi links) is severed, a drone will usually either descend to the ground or initiate a 'return-to-home' manoeuvre. However, this technique has no effect against drones that operate without an active RF link. Many signal jammers also have a limited effective range of a few hundred metres, meaning that the system must be very close to the intruding UAS to successfully mitigate its threats, and are not effective without a direct line of sight to the UAS. Jammers that are capable of operating at long ranges and beyond line of sight must be significantly more powerful, but more powerful jammers also pose a higher risk of interference to legitimate communications.

Abbreviation or term	Description
Risk management	An element of the UAS threat process that applies the findings from the threat integration and the threat analysis to evaluate in depth the CI site's specific risks and corresponding mitigation measures.
Risk score	Calculated by multiplying likelihood by impact.
SLA	Service Level Agreement
Spoofing	Allows one to take control of or misdirect the targeted UAS by feeding it a spurious communication or navigation link. Spoofing systems, however, are technically very difficult to build and implement, and may not be universally effective against all UAS. Unmanned aircraft that have been built with protected communication links, for example, could be resistant to spoofing attacks.
Threat analysis	An element of the UAS threat process aimed at understanding the UAS ecosystem.
Threat course of action analysis	An element of the threat integration, consisting of merging all understanding of threat, with the survey analysis of the site and potential vulnerabilities, to establish the most likely threat and the most impactful threat scenario.
Threat integration	An element of the UAS threat process that applies the findings of the threat analysis to highlight the most likely and dangerous UAS threats.
Threat triage	The phase immediately after the UAS threat process. It describes the process of defining the tactical-level decision-making, which will form the system response to UAS incursion. This phase represents the fundamental link between risk assessment and implementation of C-UAS measures.
UAS	Unmanned Aircraft Systems An unmanned aircraft and the equipment to control it remotely.
UAS geographical zone	A portion of airspace established by the competent authority that facilitates, restricts or excludes UAS operations in order to address risks pertaining to safety, privacy and protection of personal data, security or the environment, arising from UAS operations.
UAS operator	Any person, whether natural or an organisation, who owns or rents the UAS.
UAS risk register	List of identified risks, breaking down the problem set by threat type.

Abbreviation or term	Description
UAS threat process	Provides a guideline for CI operators to help understand and effectively manage UAS risks.
UTM	Unmanned aircraft system Traffic Management In its broadest sense, the International Civil Aviation Authority defines UTM as 'A specific aspect of air traffic management which manages UAS operations safely, economically and efficiently through the provision of facilities and a seamless set of services in collaboration with all parties and involving airborne and ground-based functions.' Consequently, a UTM system 'provides UTM through the collaborative integration of humans, information, technology, facilities and services, supported by air, ground or space-based communications, navigation and surveillance.'
VIP	Very Important Person A person of significant importance or influence who commands special treatment.

List of boxes

List of figures

GETTING IN TOUCH WITH THE EU

IN PERSON

All over the European Union there are hundreds of Europe Direct centres. You can find the address of the centre nearest you online (european-union.europa.eu/contact-eu/meet-us_en).

ON THE PHONE OR IN WRITING

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

- **by freephone:** 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),
- **at the following standard number:** +32 22999696,
- **via the following form:** european-union.europa.eu/contact-eu/write-us_en.

FINDING INFORMATION ABOUT THE EU

ONLINE

Information about the European Union in all the official languages of the EU is available on the Europa website (european-union.europa.eu).

EU PUBLICATIONS

You can view or order EU publications at op.europa.eu/en/publications. Multiple copies of free publications can be obtained by contacting Europe Direct or your local documentation centre (european-union.europa.eu/contact-eu/meet-us_en).

EU LAW AND RELATED DOCUMENTS

For access to legal information from the EU, including all EU law since 1951 in all the official language versions, go to EUR-Lex (eur-lex.europa.eu).

OPEN DATA FROM THE EU

The portal data.europa.eu provides access to open datasets from the EU institutions, bodies and agencies. These can be downloaded and reused for free, for both commercial and non-commercial purposes. The portal also provides access to a wealth of datasets from European countries.

The European Commission's science and knowledge service

Joint Research Centre

JRC Mission

As the science and knowledge service of the European Commission, the Joint Research Centre's mission is to support EU policies with independent evidence throughout the whole policy cycle.

EU Science Hub
joint-research-centre.ec.europa.eu

@EU_ScienceHub

EU Science Hub-Joint Research Centre

EU Science, Research and Innovation

EU Science Hub

EU Science

Publications Office
of the European Union