UK
Civil Aviation
Authority

# CYBER SECURITY GUIDANCE FOR **INNOVATORS**

UK Research
and Innovation

**Published by the Civil Aviation Authority, 2024**

Civil Aviation Authority,
Aviation House,
Gatwick Airport South,
West Sussex,
RH6 0YR.

First Published, March 2024
First edition

Enquiries regarding the content of this publication should be addressed to: cyber@caa.co.uk.

The latest version of this document is available in electronic format at: caa.co.uk.

UK Research and Innovation

This guidance has been created by the CAA Innovation Hub in association with the UK Research and Innovation Future Flight Challenge, delivered by Innovate UK and the Economic and Social Research Council.

# CONTENTS

CHAPTER 1

# 1. Introduction

With innovation, comes new technologies, bringing with it new challenges and cyber security risks. Whilst innovation projects continue to take place, we have written this Guidance for Innovators to utilise, so that your understanding of the cyber security risks to your specific project is broadened. We are by no means the experts in your projects, so we have taken a wide-ranging and general approach to explaining cyber security, whilst focusing on issues that have been raised to the Civil Aviation Authority (CAA) Cyber Team throughout meetings with innovation project teams. Projects that start through innovation usually lead to commercialisation, which may end up being the subject of current or future regulation. Giving you this head-start in understanding the risks that you may encounter over the lifetime of your project, ensures that you are being prepared to implement controls, when necessary, to allow an easier journey to certification, whilst maintaining or improving safety margins.

Innovation is extremely important to the CAA, and as the UK's aviation regulator, we are responsible for the safe and secure usage of UK airspace. This document is intended to serve as guidance for innovation projects taking place within the aerospace sector. It is not intended to set out a regulatory regime, nor serve as applicable means of compliance for any innovation projects.

The guidance will provide you with a general background to cyber security and who is most likely to attempt attacks on your technologies – either now or in the future. It focuses on the current and future regulations, whilst providing frameworks and resources for you to utilise, allowing you to begin incorporating cyber security into your future work.

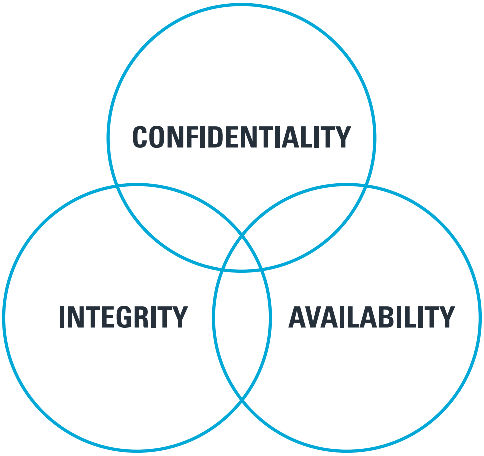
CHAPTER 2

# 2. Introduction to Cyber Security

## 2.1 Basics of Cyber

Cyber Security fundamentally has 3 key properties:

The data/information can only be viewed by the authorised individuals. This includes both inside the organisation and outside.



The data/information remains unmodified and complete while at rest or in transit. It must also only be modified by authorised individuals.

Authorised individuals should have access to the data/information when requested.

Any breach of these properties regarding digital systems is a breach of cyber security; but not all breaches are treated the same in the eyes of the CAA. There are 2 categories of implication from a breach: business implications and safety implications. Business implications could have a financial and reputational impact on your company; however, it is unlikely to affect the safety of your employees or the general public. Safety implications are caused by breaches impacting safety critical systems and that result in harm to the general public, it is these implications that the CAA are care most about.

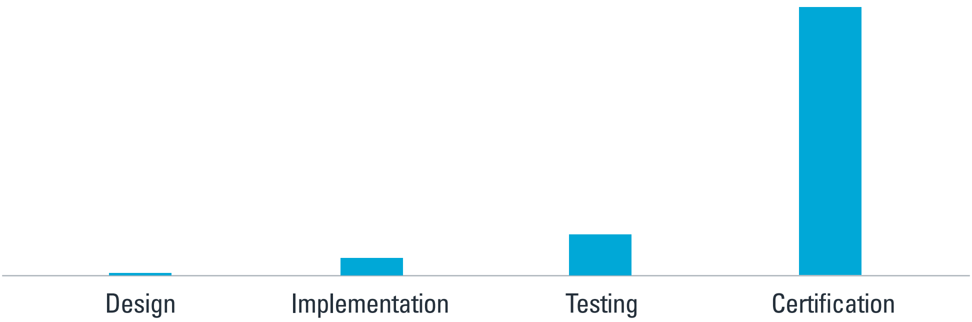
CHAPTER 2

# 2. Introduction to Cyber Security

## 2.1 Basics of Cyber (continued)

As you go through the development of your technology, costs of implementing cyber security will increase, as shown by the below graph.

Cost of Adding Cyber Security



In order to minimise the cost of adding cyber security it is best to implement it as early as possible. If cyber security is only considered during the certification process this will be very costly and may bankrupt your company. Nevertheless, we understand that your organisation may have to skip adding cyber security at the earliest stages in order to secure funding from investors. Despite skipping the implementation of such cyber security measures at early stages, it is vital it is included within planning for when the project begins gaining traction so can be picked up later down the line when further investment is secured.

CHAPTER 2

# 2. Introduction to Cyber Security

## 2.2 Threat Actors

You can break down cyber risk into the vulnerability of a system multiplied by the threat to the system. The threat will inherently come from a source which would be defined as a threat actor. These will come with their own capabilities and motivations to attack your technology. While the number of individual threat actors in the cyber sector is numerous, we can categorise them into 6 different groups.

### 2.2.1 Nation State / State Sponsored Actors

A nation state actor has the highest capability of any of the threat actors you could face. You can expect them to leverage zero-day attacks (exploiting vulnerabilities that have yet to be made public) against your technology. The main reason an adversarial nation state would target a UK company would be either to steal intellectual property (IP) for their own economic benefits, or to sabotage critical national infrastructure (CNI).

In more recent years we have seen certain nation states starting to utilise third party hacking groups. This allows the nation state, a degree of deniability after an attack is performed by the sponsored group. For the hacking group this gives them additional funding and resources as long as they go after the targets of the nation state. Each group in this section can become state sponsored and may operate above their described capabilities because of it.

Overall, while the nation state will have the highest capabilities of all threat actors, they are the rarest threat actor. A state sponsored actor is more common but will have lower capabilities than the nation state itself.

## 2.2.2 Criminal Organisations

Over the last couple of years, the cyber-criminal market share has risen dramatically with the advent of ransomware. This is expected to keep expanding into the future as more and more systems become digitised. Since fiscal gain is their key motivator, they are more likely to target your IP or other personal identifiable information (PII) which they can sell on to a third party. Additionally, they could also be hired by a third party to run distributed denial of service (DDoS) attacks against your organisation. Finally, a criminal organisation may attempt ransomware attacks, as they can provide an easy way to exploit money from your IT infrastructure. This has shown to become one of the leading attack methods in the industry, since they extort money from your organisation to unlock your IP whilst also exfiltrating with the intention of selling it.

Because there are a variety of different criminal organisations, we can expect them to have different levels of capability. The larger the organisation is, the more capability we can assume it has. Some of the largest organisations are likely to have similar capabilities to a nation state; however, they are less likely to leverage zero-day exploits against an organisation that is not perceived to have much financial value.

Overall, while a criminal organisation can have up to the second highest capabilities of any threat actor, the likelihood of them targeting you will be defined by how valuable your IP or PII is. Additionally, a high capability criminal organisation may have been hired by a third party.

## 2.2.3 Insider Threat

The insider is the only internally malicious threat actor. We can assume they are intentionally acting maliciously and may be connected to an external threat actor such as a criminal organisation or a nation state. The capability of an insider threat will entirely depend on their access level within the company, their technical ability, and how motivated they are. If an organisation is running on a flat network with little access control, the impact of a tech savvy intern could end up being similar to that of a department head. Additionally, if a profitable company has poor vetting policies, then there is a higher risk of a criminal organisation or a nation state getting a malicious insider into the company for a future attack.

There are a variety of motivations for insider threat. These will range from an insider seeking an opportunity to steal from their company with assistance from a criminal organisation to a disgruntled employee looking to get revenge on their organisation. This can result in attacks where the insider leaks information to third parties or maliciously tampers with systems in order to harm the company.

Overall, with good access controls, security policies, and vetting of employees you can help reduce the capabilities and opportunities of insider threat.

### 2.2.4 Terrorist Group

For this threat actor we are assuming they are not sponsored by a nation state and are acting independently. For a state sponsored terrorist group, we would recommend looking at the nation state threat actor. Because of the lack of sponsorship from a state, the capabilities of this threat actor are low when compared with other threat actors, especially since they are more likely to use physical means rather than cyber. If they are attempting an attack through cyber means this will most likely result in a DDoS style attack. The key reason a terrorist group may be targeting your organisation would be due to their ideology.

Overall, with good denial of service (DOS) protections you can protect yourself from this threat actor since they have some of the lowest capabilities of the 7 threat actors.

### 2.2.5 Individual Hackers / Thrill Seekers

An Individual hacker is likely to be stereotypical of whenever you think of a hacker. There are 2 key variants of individual hackers, black hat hackers, and white hat hackers. Quite often black hat hackers are attempting to break into places for the notoriety or just to show off their skills. The capabilities of these individuals vary drastically depending on their skill level, but they will never reach the level of a highly resourced team, typically seen in nation states or in high capability criminal organisations. If a renowned black hat hacker is contracted to work for these organisations, we would no longer classify them as an individual hacker.

White hat hackers are similar in the range of skills to a black hat hacker but are not malicious. Typically, these individuals are hired by organisations to perform penetration tests, in which these individuals will attempt to attack a organisations' systems with permission from them. After performing these attacks, the white hat hacker will disclose to the company how/if they were able to break into the company and how prevent similar attacks in the future.

A low capability individual hacker will typically be using attacks they discovered on the web and just recreating the attack. Therefore, if you patch all software that is supplied to your company, you will become quite resistant to this threat actor. A more capable threat actor will likely use more advanced techniques to attack your technology and even potentially zero-days if they are skilled and determined enough.

The reason this threat actor may target you can be quite random. Typically, it is more about the thrill of hacking something rather than having a target in mind. Overall, if you can keep your cyber hygiene to a good level, you can prevent most attacks by this threat actor.

## 2.2.6 Hacktivists

Like terrorist organisations, hacktivists are ideologically driven; however, they are more likely to have higher capabilities. Typically, the goal of a group of hacktivists is to draw attention to what their cause is and, like with real life, this normally takes the form of preventing daily business of a certain activity. While in physical life this may be in the form of blocking an entrance to a building or road, in the cyber domain this would be by either defacing or taking down a website.

Capabilities wise, at worst they are expected to be as good as a terrorist group and at best they are as good as a small criminal organisation. Typically, their attacks are more focused around DDoS style attacks and defacing, rather than attempting to steal IP or PII.

Overall, hacktivists are a threat to your organisation's reputation rather than any IP or PII. In addition, they are one of the most persistent threat actors due to their ideological motive. Like with individual hackers, good cyber hygiene will help mitigate this threat actor.

## 2.3 The Supply Chain

The supply chain is any dependency that your technology requires. This can be physical, software, or infrastructure based. Physical dependencies will be any physical tool or material that is used to construct your technology. This can range from the metal alloys to the wires, to the computer chips that are being used. Software dependencies will be anything that is used to create the software part of your technology; for example, any software packages that are imported, tools that are used to create your own code, or any off the shelf programs that are used. Finally, infrastructure dependencies are any services or processes that are outsourced to another company. In cyber security this mainly covers cloud services but can be other infrastructure you use. Your business may contain some dependencies of each category or none at all, the important thing to us is that you are able to keep track of them.

Sophisticated adversaries such as nation states or highly capable criminal organisations can attack your organisation though the software & infrastructural supply chain. This is primarily through embedding malware into an update or tool from your dependant organisation. This means the adversarial organisation can have their malware interact with your technology without directly interacting with your organisation. Additionally, there might be an exploit in a dependant piece of software that can be manipulated by an adversarial organisation. If your organisation is utilising cloud services, the adversary may choose to breach the service's security to get into your servers.

CHAPTER 2

# 2. Introduction to Cyber Security

## 2.3 The Supply Chain (continued)

There are different ways of mitigating a supply chain attack, for instance:

**Including security provisions into your cloud service/infrastructural contract**

Having this can help with ensuring that third party providers will keep your systems secure from their end. While it is up to you and your provider to define where responsibilities lie with each system, it is important to discuss cyber security with them.

**Keeping a good line of communication with infrastructural or software dependencies in case of a vulnerability or breach being discovered**

Typically, when a vulnerability or breach is discovered by an organisation, they will publicise it with the associated mitigations. Keeping a good line of communication with them will allow you to act upon the vulnerability and reduce the risk of it occurring.

**Validating updates from software dependency before implementing it into your code base**

To prevent a supply chain attack, it is best to validate the update from the supplier before implementing it. You can also test to make sure that the update doesn't break aspects of your technology.

**Auditing the supplier**

Auditing the supplier either by your organisation or an accredited third party can be a great way to assure that the supplier meets the baseline of cyber security. If this is done before a contract is signed, you can stipulate the required improvements by the supplier to meet the baseline as part of the deal.

## 2.3.1 Open-Source Libraries

There are a couple risks to using an open-source library that should be thought about from a cyber security lens. Because these libraries are open for everyone to use and read, there is potential for adversaries to use it as an attack vector. Before importing a library, you should check if it's still being updated regularly. Since the code is viewable by everyone, an adversary has the opportunity to find exploits within the library, which if imported means the adversary can exploit your code through the library. This isn't a major issue if the code is being actively updated, especially if they patch their exploits consistently and in a timely fashion. If the library no longer receives updates, then the older it gets the more unpatched exploits it will likely contain. Overall, the threat of an inactive library is more prevalent among open-source libraries since they are often more easily found than proprietary libraries.

The other key risk is an intentionally malicious open-source library. With the ability to import libraries through an integrated development environment (IDE), there is a risk for an adversary to trick a user into downloading a malicious library. Typically, adversaries will copy the functionality for a pre-existing open-source library, add the malicious code, and release them with either typo of the original name, a different name, or a different version number. To prevent these libraries from being installed, it is critical that you check the identifiable information of the intended library or download it directly from the repository site.

All in all, the risk of using open-source libraries is for you to decide. The most important thing is to understand the amount of risk you can take on. While for safety critical systems it would be best to vet open-source libraries heavily or avoid them all together, the same cannot be said for less critical systems. Nevertheless, if good cyber design is not implemented then we can have a scenario of a non-critical system being attack by an adversary, who will use it to laterally move to and attack a critical one.

```
function removeLinkHeaders(prev) {
  return prev.then($ => {
    $(':header').map((i, header) => {
      const children = $(header).children();
      if ($(children).length > 0) {
        $(header).text($(children).text());
        $(children).remove();
      }
      return header;
    });
    return Promise.resolve($);
  });
}

function embedImages(prev) {
  return prev.then($ => {
    if (!embed) return Promise.resolve($);
    const images = $('img').map((i, img) => {
      const src = $(img).attr('src');
        let d
```

## 2.3.2 Open-Source Applications

Open-source applications are very similar to an open-source library and contain the main risks described in the above section. However, because of the likely added complexity of an open-source application as compared with an open-source library exploits will be more common. This means that an inactive repository containing the application is more likely to contain an unpatched common vulnerability exposure (CVE). To help mitigate this you can duplicate the application, perform a vulnerability assessment, patch out the found vulnerabilities, and transfer the changes to the original application. This will allow you to use the application so long as you keep it up to date yourself. Additionally, if the source code is not available, you can decompile the application in order to better understand the risks that come with it. For example, the application may wish to use ports that you have blocked for security purposes. It is good practise to check what the application does and what services it requires before implementing it.

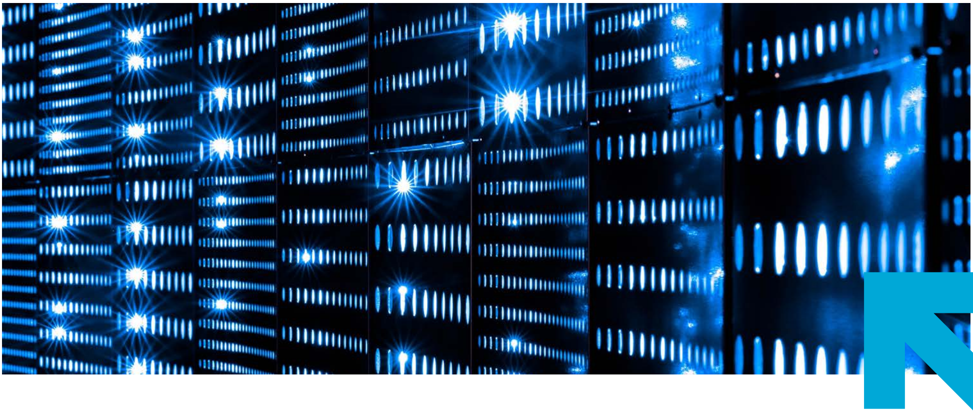
As with malicious libraries, malicious applications also exist, but if you are getting them from the genuine supplier, they are unlikely to be malicious. The only exception to this would be during a supply chain attack but the above sections will help mitigate the risk of this.

## 2.3.3 National Cyber Security Centre (NCSC) Guidance on Supply Chain

The NCSC can also give you guidance on how to help sure up your supply chain. You can find their advice here: https://www.ncsc.gov.uk/collection/supply-chain-security.

## 2.3.4 Log4j Case Study

The Log4j exploit is a great example of why you should keep track of your supply chain. For context, it was a critical exploit that was found in low level java code. This meant that it was widely used and commonly not reported in organisation's supply chains. This led those organisations to spending huge amounts of money to find which systems were vulnerable so they could put in temporary mitigations before the vulnerability fixing patch comes out.



CHAPTER 2

# 2. Introduction to Cyber Security

## 2.4 Examples of Serious Incidents

### 2.4.1 Casino Hack via Fish Tank temperature Controller

As systems get more and more connected, it will get harder to find out where the weakest part of your system exists. This was the case back in 2017 when a casino in North America was hacked through a high-tech fish tank thermometer controller. This thermometer had the problem of being connected both to the internet but also to the network of other systems in the casino. Because there was very little security designed into the thermometer, it was an easy target to break into, allowing an access point to the network. There are some key lessons we can learn from this case study:

**Your security is only as strong as your weakest section**

We can assume the more conventional entry points such as the email server of the casino had cyber security protections; however, because the fish tank thermometer was undefended the attack was able to occur. You should make sure there is a baseline for security for each device that is connected to the internet so as to prevent this problem.

**It is important to understand how supplied software and hardware feeds into your technology/network**

The casino didn't build the fish tank, but it is likely that they didn't check the full functionality of it. One of the critical steps in the cyber security risk process is asset management; therefore, it is vital that you are keep a list of each supplied piece of software and hardware as well as their capabilities.

**It is important to control the number of connections you have and keep them as low as reasonably possible**

The casino was using an Internet of Things (IoT) structure, which has a lot of different connections from different devices on a network. This means it can become very hard to track all the different connections a device may have; it also means that an adversary can more easily traverse the network and potentially move around the defences that are in place. If each device has its connections limited to the minimum it'll reduce the potential pathways of attack from an adversary, thereby making it easier to defend.

## 2.4.1 Casino Hack via Fish Tank temperature Controller (continued)

**Having security built into each system is stronger than having one very tough security layer**

While on the network via the fish tank thermometer, the adversary was able to extract terabytes of data without detection. This means that there were other security mitigations that had either been bypassed, ineffective, or non-existent on the network. This implies that there was probably one key security layer to the infrastructure. This is poor design because if a vulnerability can get through the security layer, it can get through the whole system. A good way to prevent this is through making each system cyber resistant, so that if an adversary can breach the first layer, they'll still have to go through more layers to complete their objective. In turn, this will reduce the amount of successful cyber-attacks.

## 2.4.2 WannaCry Exploit of the NHS

The WannaCry attack on the NHS back in May of 2017 is an interesting example of poor patching and updating. The patch that fixes the exploit used by WannaCry had been released on the April of that year. This means the attack would have been prevented had the NHS IT system been updated with the safety critical patch. This is a common method for ransomware to get itself onto a system and shows the consequences when supplied software is not patched in a timely manner.

CHAPTER 3

# 3. Regulations and Publications

The CAA has published many guidance documents to support regulations, taking the form of Civil Aviation Publications (CAPs), Guidance Material (GM), and acceptable means of compliance (AMC). AMC sets out specific requirements that must be followed to satisfy the regulations. The European Union Aviation Safety Agency (EASA) and The European Organisation for Civil Aviation Equipment (EUROCAE) have also published documentation that may be worthwhile considering, as well as undertaking working groups to establish what future regulations may look like in the future for innovative projects. Whilst your innovation projects may not currently be subject to any regulations, they may be in the future. Not all subjects involved with innovation will have a relevant regulation, however the ones that do may wish to begin looking into these now to prepare the projects for certification once that stage is reached.

However, once your project begins the certification process, we will no longer be able to provide guidance and assistance for cyber security matters, therefore it is key to engage with us now to ensure you are prepared once you reach this level of maturity. You can do so by going to our website at: caa.co.uk/our-work/innovation.

## 3.1 Initial Airworthiness

Cyber security for initial airworthiness comes under Panel 6 (Avionics) in the Design and Certification process. There are a few documents that we in the CAA look at to assess the cyber security of an aircraft for its initial type certification:

- AMC 20-42: Airworthiness information security risk assessment
- EUROCAE ED201-ED-206: These documents outline the overall airworthiness – security process specification, security methods & considerations, guidance for continuing airworthiness, and guidance on security event management.

## 3.2 Vertical Take-Off or Landing (eVOTL)

The current process for general certification of VTOL systems is to follow the EASA Special Condition Vertical Take-Off or Landing (SC-VTOL) documentations and there are discussions and work on-going through the EUROCAE Working Group 112 (Vertical Take Off and Landing). We do suggest that ED201-ED204 should provide general instructions for security measures and ED-12/DO-178 for airborne software certification for a VTOL system, but we also recommend that you look at new avenues for threat from systems such as battery management subsystems, machine learning based software production and smart plug-in charging systems.

CHAPTER 3

# 3. Regulations and Publications

## 3.3 Remote Piloted Air Systems (RPAS)

Currently for RPAS, there is a different certification process depending on the category you will fit into. While it is up to the operators to supply the regulatory information, if the cyber security of the chosen RPAS is unable to meet the safety level of the operation that is intended then it is highly unlikely it will be approved for operations.

The definitions of these categories can be found in Regulation (EU) 2019/945[1] and 2019/947[2] with acceptable means of compliance and guidance material, for additional guidance material you can use the document CAP722: Unmanned Aircraft Systems Operations in the UK Airspace – Policy and Guidance.

Depending on the factors outlined in 2019/945 & 2019/947, the operation of your RPAS will fall under the specific category or the certified category. If you are aiming for the open category to be the highest form of operation, then you will not have any cyber security requirements. If you are aiming for the specific category to be the highest form of operation, then we would recommend looking through 2019/945 & 2019/947 to find what level of requirements you should aim for. Fundamentally the regulation underpinning this is: Regulation (EU) 2019/947 section UAS.SPEC.50 1a(iii). If the certified category is the aim, we would recommend you go through section 3.1 above instead.

## 3.4 Air Traffic Controllers (ATC)

If you are planning to integrate your technology into the air traffic control system of a pre-existing aerodrome, then your system may fall within the scope of CAP 1753: The Cyber Security Oversight Process. This may also mean that the system may be audited and overseen to make sure it is secure. While fundamentally it is the aerodrome's responsibility to keep their systems secure, it would be unlikely for them to pick any new equipment or systems that aren't cyber resistant.

[1] Regulation (EU) 2019/945 as retained (and amended in UK domestic law) under the European Union (Withdrawal) Act 2018

[2] Regulation (EU) 2019/947 as retained (and amended in UK domestic law) under the European Union (Withdrawal) Act 2018

CHAPTER 3

# 3. Regulations and Publications

## 3.5 Aviation Cyber Security

If your piece of technology or system is designed to be utilised by an aerodrome, air operator or air navigation service provider (ANSP), then you may fall into the scope of CAP1753. If the aerodrome, air operator or ANSP are already certified and in operation, you won't need to certify your system; however, depending on the criticality, it may fall in scope of CAP1753. Because this process focuses on cyber security, the aerodromes, air operators and ANSP's are unlikely to select your technology if it does not show good cyber resistances.

- CAP1753: The Cyber Security Oversight Process is the primary document the CAA uses to assess the security of the safety critical processes in aerodromes.
- CAP1849: The Cyber Security Critical System Scoping Guidance for CAP 1753. This will define if your technology is a critical system of the aerodrome and subject to the cyber security oversight of CAP1753.
- CAP1850: The Cyber Assessment Framework (CAF) for Aviation Guidance. This details how the CAF for aviation should be used by the aerodrome as part of CAP1753. This document is based on the NCSC's CAF document but has been tailored to the aerospace and aviation industry.

## 3.6 Artificial Intelligence and Machine Learning

Currently, the CAA does not have official guidance or regulation on the use of Artificial Intelligence (AI) in safety critical applications. The CAA expect to release a Strategy for AI in 2024 which will accompany several work streams to develop policy and guidance.

The document below is the current publication from EUROCAE regarding AI and ML, that may be of use for information only.

- 'Artificial Intelligence in Aeronautical Systems: statement of concerns': Gap analysis conducted by EUROCAE Working Group 114 to review existing standards and why existing standards cannot be reliably used.

## 3.7 Electric Chargers

The current published guidance for aviation electric charging infrastructure is ED-308, published by EUROCAE and developed by Working Group 112. The CAA is currently investigating the regulatory requirement for electric charging infrastructure for the air environment. However, we recommend utilising ISO 15118-20:2022 as a baseline for good security practise but we do understand the primary focus of the document is ground vehicles electric charging.

CHAPTER 4

# 4. Risk Assessments and Secure Development

## 4.1 The National Cyber Security Centre

As the UK's national technical authority for cyber security, the NCSC manages national cyber security incidents, provides an authoritative voice and centre of expertise on cyber security, and delivers tailored support and advice to departments, the Devolved Administrations, regulators, and businesses. While having no regulatory responsibilities, the NCSC is the Single Point of Contact (SPOC), and the Computer Security Incident Response Team (CSIRT) under the Network and Information Security (NIS) Regulations. The NCSC can normally provide support in your cyber requirements and have a very detailed website.

## 4.2 Threat Analysis and Risk Assessment

### 4.2.1 System Scoping and Asset Identification

System scoping or critical system scoping is an activity that is intended to assist in the identification and documentation of cyber related mission critical processes, and the associated assets and services which support these processes that would impact safety. This activity will aid in applying comprehensive, appropriate, and proportionate cyber security measures. Appropriate personnel should be included in the scoping activity to ensure complete coverage of your systems and processes, for example, Subject Matter Experts within Safety, Security, and Engineering.

When identifying the scope of system critical processes, the CAA would recommend you make an informed and competent consideration of reasonable and expected impacts. The CAA recommends that you ignore implausible scenarios or highly complex chains of events or failures — a reasonable worst-case scenario should be used.

To ensure that the scope is accurate and includes mission critical processes that would reasonably be considered in scope, it is advised that you use a logical method and include all stakeholders deemed relevant by the organisation (e.g., workshops with supporting documentation, board level discussions and decisions, business impact assessments, etc). Also, ensure that all identified processes, systems, or assets identified are sufficiently detailed to perform the later activities mentioned in 4.2.2 to 4.2.4.

You are ultimately responsible for your own risks and the identification and validation of your mission critical process scope. Whereby if you are utilising third party systems in your product, then we encourage you to have assurance from your third-party vendors regarding their cyber security via some form of written record by a responsible person in the third-party organisation.

### 4.2.2 Threat Analysis

The threat landscape constantly evolves, with the number of new threats growing exponentially. It is therefore imperative that you have an approach to evaluate the threat at appropriate intervals or as an ongoing task. You may wish to use external organisations to perform threat analysis if you do not possess the knowledge to perform this internally.

The NCSC provide weekly threat reports as well as sector specific threat reports. We encourage you to engage with the NCSC to better understand the threat and to receive any other cyber security support. The latest threat reports can be found on the NCSC's website.

You can do an annual threat analysis of your corporate enterprise system as well as the system you are developing to understand system vulnerability. Threat analysis activities can be made through systematic and evidencable approaches such as STRIDE, TVRA, MITRE ATT&CK etc.

The threat analysis above, alongside asset identification will provide the fundamental information a developer will require to undertake a thorough cyber risk assessment.

### 4.2.3 Risk Assessment

The risk assessment can classify the risk in likelihood and severity or impact levels and should have a named individual assigned as an owner to each individual risk.

It is highly likely that there will be crossovers between safety risks and security risks. It is important that the developer clearly documents the relationships between these risks. Where these risks are already identified in a safety risk assessment, the link to the cyber event should be clearly identified in the safety risk assessment and noted in the cyber security risk assessment documentation.

Risks can be calculated to understand historic, current, and residual risks. Developers can also consider the controls that are in place for each risk, and these should be documented in the risk assessment. Where there is a control, a residual risk column can be included to indicate how the implemented control reduces the risk scores.

Where a developer is considering using third-party technologies, software, or services, consideration around the security impact and associated risks of such suppliers ought to be considered and documented within the risk assessment. Further guidance around supply chain security is available from NCSC.

### 4.2.4 Risk Response

Based on your risk assessment, each risk should have 1 of 4 risk responses:

**TREAT** **TOLERATE** **TRANSFER** **TERMINATE**

Risk responses of Treat, Tolerate, Transfer or Terminate are widely accepted terminologies when assessing what the appropriate response for a particular risk statement is. We recommend that you consider the 'why' behind your reasoning as part of the risk assessment documentation. Should you deem a risk is transferable, it is advisable you detail who the risk is being transferred to and why, alongside any formal agreements that will detail the risk transfer and a piece of evidence that confirms the risk has been transferred to the transferee. Where treat is used as a response, the appropriate evidence would need to be documented in the controls column of the risk assessment documentation.

# 4. Risk Assessments and Secure Development

## 4.3 Secure Development Process

The goal of secure development process (SDP) is to promote security into the software development lifecycle (SDLC), by integrating security processes or tools into every part of the SDLC from planning to maintenance. The CAA does not want to prescribe a particular SDP methodology as each of your organisations will have a particular methodology for software development. However, the below summary of activities[3] that we believe can be part of any software development process:

**Activities**
Threat modelling

**Phase**
Plan

**Example tools**
Threat modelling tool

**Features/Benefits**
Document system security design. Analyse the design for potential security issues. Review and analysis against common attack patterns. Allows software architects to identify and mitigate potential security issues early.

**Activities**
Secure code development

**Phase**
Develop

**Example tools**
IDE

**Features/Benefits**
Security policy enforcement script coding. View code changes, identify defects, reject, or approve the changes, and make comments on specific lines. Sets review rules and automatic notifications to ensure that reviews are completed on time.

**Activities**
Static code scan before commit

**Phase**
Develop

**Example tools**
IDE security plugins

**Features/Benefits**
Scan and analyse the code as the developer writes it. Notify developers of potential code weaknesses and suggest remediation. Scan and analyse the code as the developer writes it, notify developer of potential code weakness, and may suggest remediations.

# 4. Risk Assessments and Secure Development

## 4.3 Secure Development Process (continued)

**Activities**
Code commit scan

**Phase**
Develop

**Example tools**
Source code repository security plugin

**Features/Benefits**
Check the changes for sensitive information before pushing the changes to the main repository.

If it finds suspicious content, it notifies the developer and blocks the commit.

**Activities**
Static application test and scan (SAS)

**Phase**
Build

**Example tools**
SAS Tool (SAST)

**Features/Benefits**
SAST analyses application static codes, such as source code, byte code, binary code, while they are in a non-running state to detect the conditions that indicate code weakness.

Catch code weaknesses at an early stage.

Continuous assessment during development.

**Activities**
Dependency vulnerability checking

**Phase**
Build

**Example tools**
Dependency checking/Bill of Materials (BOM) checking tool

**Features/Benefits**
Identify vulnerabilities in the dependent components based on publicly disclosed open-source vulnerability.

Identify vulnerabilities in the open-source dependent component.

Secure the overall application. Manage the supply chain risk.

CHAPTER 4

# 4. Risk Assessments and Secure Development

## 4.3 Secure Development Process (continued)

**Activities**
Dynamic application security test (DAST) and scan

**Phase**
Test

**Example tools**
DAST tool or Interactive Application Security Testing (IAST) tool

**Features/Benefits**
DAST tools analyse a running application dynamically and can identify runtime vulnerabilities and environment related issues.

Catch the dynamic code weakness in runtime and under certain environment setting.

Identify and fix issues during continuous integration.

**Activities**
Manual Security testing (Pen Test)

**Phase**
Test

**Example tools**
Multiple tools

**Features/Benefits**
Such as penetration test, which uses a set of tools and procedures to evaluate the security of the system by injecting authorized simulated cyber-attacks to the system. Validate system security; increase attack readiness; reduce the risk of system degradation.

**Activities**
Post-deployment security scan

**Phase**
Deploy

**Example tools**
Security compliance tool

**Features/Benefits**
System and infrastructure security scan after deployment of software and applications into your systems.

## 4.3 Secure Development Process (continued)

**Activities**
Operational dashboard

**Phase**
Operate

**Example tools**
Backup

**Features/Benefits**
Provide operators a visual view of operations status, alerts, and actions. Improve operations management.

**Activities**
System security monitoring

**Phase**
Monitor

**Example tools**
Information Security continuous monitoring

**Features/Benefits**
System configuration (infrastructure components and software) compliance checking, analysis, and reporting. Detect unauthorised personnel, connections, devices, and software. Identify cybersecurity vulnerability. Detect security compliance violation. Verify effectiveness of protective measures.

[3] The reference: DevSecOps Fundamentals Guidebook: DevSecOps Tools and Activities, US DOD 2021

APPENDIX A

# Abbreviations and Acronyms

**ATC**
Air Traffic Control

**BOM**
Bill of Materials

**CAA**
Civil Aviation Authority

**CAF**
Cyber Assessment Framework

**CAP**
Civil Aviation Publication

**CNI**
Critical National Infrastructure

**CVE**
Common Vulnerability Exposure

**DAST**
Dynamic Application Security Testing

**DDOS**
Distributed Denial of Service

**DevSecOps**
Development, Security and Operations

**DO**
RTCA Document

**DOS**
Denial of Service

**EASA**
European Union Aviation Safety Agency

**ED**
EUROCAE Document

**EUROCAE**
The European Organisation for Civil Aviation Equipment

**eVTOL**
Electric Vertical Take-Off or Landing

**IAST**
Interactive Application Security Testing

**IDE**
Integrated Development Environment

**IoT**
Internet of Things

**IP**
Intellectual Property

**NCSC**
National Cyber Security Centre

**NIS**
Network and Information Security

**PII**
Personal Identifiable Information

**RPAS**
Remotely Piloted Air Systems

**RTCA**
Radio Technical Commission of Aeronautics

**SAS**
Static Application Test and Scan

**SAST**
Static Application Test and Scan Tool

**SC-VTOL**
Special Condition Vertical Take-Off or Landing

UK
Civil Aviation
Authority

caa.co.uk/innovation
@UK_CAA

UK Research
and Innovation