STPA-based Safety Analysis of eVTOL Operations

CAP 3141

Contents

CAA Introduction

Electric Take-Off and Landing aircraft (eVTOLs) are being developed by a mixture of start-ups and traditional aviators and are testing the frontier of battery technology for inter-city and regional flight in the coming years. They promise to be quieter with potentially lower operational costs than traditional rotorcraft, bringing the opportunity to undertake significantly higher volumes of journeys, unlocking the economic and social benefits associated with improved connectivity. This futuristic model for aviation is known as Advanced Air Mobility.

To successfully launch electric vertical flight services, new ground infrastructure needs to be developed, and the airspace infrastructure reimagined to cope with additional traffic. CAA and the Department for Transport are enabling this through the Airspace Modernisation Strategy explained in CAP1711.

Creating a new form of transport will naturally bring unforeseen risks between various actors in the aviation system. Before services can start, we need to pre-empt these risks and either seek to remove them or minimise their likelihood. This is the rationale behind the work we, working with the eVTOL Safety Leadership Group, commissioned Warwick Manufacturing Group (WMG) to undertake through this System Theoretic Process Analysis (STPA) of eVTOL operations.

eVTOL Safety Leadership Group

The eVTOL Safety Leadership Group (eVSLG) was established in 2022 and seeks to emulate the model set by the Onshore and Offshore Helicopter Safety Leadership Groups (SLGs).

The aim of the eVSLG is to create and maintain an open safety culture between all members of this nascent sector’s ecosystem, so that those accountable for safety can take appropriate action where needed. This is a core tenet of a good Safety Management System (Regulation (EU) No 376/2014). Hence, the group’s membership includes Original Equipment Manufacturers (OEMs), operators, infrastructure owners, NATS, and government bodies such as the Air Accident Investigation Branch.

The key difference between eVSLG and the extant SLGs is that eVTOL revenue services have not commenced, and many aspects of the sector’s operational system are under development. Furthermore, regulations are not fully developed to control the novel operational and aircraft risks arising for new aviation systems with electric vertical take-off and landing. For instance, new operations rules for airspace management, flight control systems and energy management will be required.

UK Future of Flight Programme

The UK Future of Flight Programme encompasses the CAA's work to support the integration of novel aviation technologies, currently focussed on Uncrewed Aviation Systems (referred to informally as drones) and eVTOL aircraft. The programme is sponsored and funded by the Department for Transport, with the DfT's Minister of Aviation also chairing the Future of Flight Industry Group which brings together industry, government and the regulator to oversee the programme.

The funding provided by DfT allows the CAA to undertake research to ensure we implement effective regulation, including through this STPA research.

System Theoretic Process Analysis

The UK CAA has recognised that it needs to augment its safety risk assessment and management tools to deal with ever-increasing complexity of aviation systems.

With eVTOL aircraft approaching technological and operational readiness, the UK aviation system has an excellent opportunity to look at the future systemic risks and build an optimal system by design.

For this reason, the testing and validation of System Theoretic Process Analysis (STPA), an innovative hazard analysis tool, is being undertaken to validate the CAA-wide implementation of this powerful technique.

STPA was devised by Professor Nancy Leveson of Massachusetts Institute of Technology, the need for which she sets out in her 2011 book, '*Engineering a Safer World*' (2011)[1]. The technique provides a *systematic* framework in which to analyse and control for system level hazards and risks, identifying and addressing risks that exist due to weaknesses in the interactions between actors in a system, and not just risks within its components. It was developed with the aviation sector in mind and has received the endorsement of other key regulatory bodies such as the United States' FAA and NASA.

Further detail regarding the theory of STPA is provided within a Technical Annex at the rear of this CAP.

STPA and the eVSLG

The eVSLG provided many of the components required for such an exercise to be undertaken in the British context. The group contains high-ranking safety professionals from a number of players in the industry, and aviation public servants with cumulative experience running into centuries. Many members of the group have technical backgrounds in rotorcraft, a sector which shares significant operational commonalities with eVTOLs.

In the United Kingdom, WMG University of Warwick are recognised as a champion of the STPA technique, having produced numerous studies looking at connected and automated vehicles (Khastgir, 2021), and the UK response to COVID-19 (Chen, 2021). Through collaboration with WMG, we have been able to produce the first comprehensive usage of STPA in the British aviation context, and the first official usage of STPA by the UK CAA.

[1] https://direct.mit.edu/books/book-pdf/2280500/book_9780262298247.pdf

STPA Aims

The CAA’s aims for this exercise were twofold:

1. To validate Systems Theoretic Process Analysis as a technique for examining complex systemic aviation risks, complementing the CAA’s current suite of tools, e.g. Bow Tie.
2. To utilise STPA to undertake a systemic hazard analysis for conventional helicopters and electric vertical take-off and landing aircraft

The eVSLG elected to partner with WMG on this piece of work for which the first of two phases commenced in June 2023.

- The first phase looked at the network of relationship between actors within a high-frequency conventional helicopter operation (British Formula 1 Grand Prix weekend). This was undertaken so that the eVTOL operation hazard analysis had a basis in real-world current operations.
- The second phase examined the similarities and differences between event-day rotorcraft operations and an equivalent eVTOL operation.

Given that this analysis looked at conventional helicopter operations as a means of identifying eVTOL systemic hazards, this paper is also an opportunity to look anew at the system-level risks associated with helicopter flight.

Outcomes

The analysis has produced advice on aspects of the eVTOL aviation system requiring further consideration from a safety perspective, and suggestions on how to control for them. These fall into categories actionable by the:

- Regulator
- Operator
- OEM
- Infrastructure owner, e.g. Vertiport operator

From industry’s perspective, these findings can assist in the development of eVTOL stakeholders’ Safety Management Systems, a key factor in addressing and meeting the Air Operations regulations in this country.

From the regulator’s perspective, the report has undertaken a gap analysis whereby the WMG have presented safety factors brought to light by workshops and has consulted with Subject Matter Experts to assess whether they constitute regulatory gaps.

As expected, this STPA review has elicited a significant number of potential issues for the regulator and industry to assess and consider (432). Given the high number of recommendations that the analysis has uncovered, researchers at WMG have also developed an innovative prioritisation methodology, taking into account:

- Operational Disruption
- Criticality
- Detectability
- Effect on Other Stakeholders
- Likelihood of Occurrence

This will help the CAA and industry to respond to the findings most effectively. Details on the nature of the findings and their prioritisation are provided within the main report.

The project has shown that STPA is capable of effectively analysing the advanced features of next generation aviation technologies and the complexity of proposed operational improvements. The findings elicited from this project demonstrate that STPA offers a thorough framework to identify shortcomings in existing regulations, policies, and procedures. The report validates the CAA’s current ‘crawl-walk-run’ approach to airspace modernisation and reflects the current state of maturity of this emerging sector.

The findings of this assessment are contained in full within WMG’s report; the theoretical background to the work is found within a Technical Annex at the back of this CAP.

Further work/next steps

Using the results of this exercise

The CAA will now consider the findings of this exercise as part of our regulatory programme of works. Many of the determinations of the STPA have implications for the CAA's procedures, policies and regulations. Where regulatory changes are required, we will work with the CAA's Rulemaking team to begin the process of converting the study into aviation legislation. This process typically takes two years to complete. This timeframe coincides with the government's roadmap for initial eVTOL commercial operations.

Whilst this work has uncovered key safety considerations for the CAA as safety rulemaking material that may result in Requirements, Alternative Means of Compliance and/or Guidance Materials, the work has also produced a significant number of other lower priority considerations. These will be followed up collaboratively with industry, through the eVSLG Risk Sub-Group.

Further uses of STPA

The mapping of both the eVTOL aviation system and its integration with other airspace users acts as a useful framework for emerging risks to be examined and controlled. In due course, these 'control structures' can be further developed to increase knowledge about a more diverse range of VTOL services and technologies. For example, will hybrid-electric be a viable alternative mode of propulsion for these operations, as we further understand battery capabilities? Will hydrogen be part of the energy mix, and will the hazards associated with their transport and storage need to be examined?

The STPA can also be further developed to assess risks within parts of the system we have not yet explored. For instance, relationships with wider eVTOL system stakeholders, such as the National Energy System Operator could be evaluated, and the consequences of further automation of air traffic management modelled, to aid the development of the CAA's Airspace Modernisation Strategy.

The onus on ensuring that this STPA stays 'alive' will fall to all members of the eVSLG, as well as WMG, as part of the AAM community's commitment to starting eVTOL operations with a robust Safety Management System and mature safety culture.

Acknowledgements

The CAA would like to thank all members of the eVTOL Safety Leadership Group, and others who participated in the numerous workshops and technical sessions, both in-person and remotely. Without industry’s contribution to this exercise, this already complex exercise would have been rendered impossible.

We would also like to thank the CAA’s Subject Matter Experts who volunteered their time in the face of a multitude of other pressures to share their views throughout, helping to prove the technique’s worth and start a wider conversation about proactive approaches to system safety.

Lastly, but by no means least, we wish to thank the researchers from the Safe Autonomy unit at WMG, who have undertaken a sterling effort to complete this exercise.

Executive Summary

Problem Statement

With the rapid development of Advanced Air Mobility (AAM) concepts and electric Vertical Take-off and Landing (eVTOL) operations, ensuring safe deployment of eVTOL aircraft in the current aviation airspace presents unique challenges. This is because of their novel technology, operational complexity, and regulatory uncertainties. These challenges span various stakeholders of the eVTOL operation, from design and airworthiness at the eVTOL manufacturer side, to the operational and infrastructure management at the vertiports or aerodromes, and further to the humans (passengers and the public). The UK Airspace Modernisation Strategy is **focused on integration rather than segregation** of diverse airspace user groups, with different operational requirements and capabilities. Integrating a novel technology (e.g. eVTOL) into the current air navigation system can pose emerging risks and hazards which require both identification and assessment.

Although regulatory bodies have been developing eVTOL-specific regulatory requirements, considering the complex interactions between different stakeholders of the eVTOL operation, the identified requirements yet still cannot be claimed complete or fully assessed. Furthermore, due to the potentially large number of requirements that need to be implemented imminently, identifying and managing these requirements has brought more challenges. Current safety approaches fall short when analysing systems with emergent behaviour, especially multistakeholder systems with human-technology interactions.

Approach

To assess the risk posed by eVTOL operations in UK's current airspace, a systems thinking based safety analysis method, STPA (Systems Theoretic Process Analysis), was chosen. A comparison of STPA against other current safety analysis methods can be found in **Annex C**: Comparison between Safety Analysis Methods, which highlights its advantages over other safety analysis methods and underpins the choice of STPA for this purpose. For successful results from an STPA, two types of experts were needed: 1) STPA experts; 2) domain experts. WMG, University of Warwick provided the STPA expertise while the project also brought together several stakeholders who would be involved in the eVTOL operations to provide the domain expertise (as Subject Matter Experts – SMEs). This includes the UK Aviation Regulator- Civil Aviation Authority (CAA), eVTOL Operator (Flexjet, Bristow Group), Air Navigation service provider (NATS), British Helicopter Association, Vertiport Operator (Skyports), OEM (Lilium, Vertical Aerospace) and Helicopter Pilots.

Summary of the findings

The original STPA results identified 432 Mitigations across the various stakeholders. To rank and prioritise these Mitigations, a **novel Mitigation prioritisation methodology (STPA extension) was proposed by WMG**, which allowed to identify a more focussed set of 124 Mitigations.

In this document, a 'Gap' refers to a mitigation recommended by STPA that is not covered by the current regulations, policies, or procedures concerning Helicopters and/or eVTOLs. Out of the 124 Mitigations, **56 were identified as 'Gaps'.**

The finalised 56 gaps represent targeted, high-impact opportunities for regulatory enhancement in various aspects such as:

- **Organisational performance**
- **Process review and improvement** (example - UCA(Ph0.1)-50.2.1-RQ8: Process review of the relevant team issuing Aircraft Release To Service within the eVTOL Operator shall be conducted periodically to ensure that the team operates properly and safely)
- **Assessment criteria**
- **Acknowledgement and Confirmation for certifications**
- **Training process for individuals involved in the regulatory process** (example - UCA(Ph0.1)-17.1.2-RQ2: Regulator shall be properly trained to be able to correctly review the supplementary documents [Supp. Doc for safety certification]).
- **Collision and Energy management**
- **Automation and Simulation** (example- UCA(Ph1)-18.2.1-RQ9: ANSPs should implement mechanisms to detect and alert controllers/service providers to deviations in aircraft performance (e.g., altitude, speed, trajectory) from expected parameters)

The section titled **Gap Analysis** contains a comprehensive list of all the identified Gaps, linked to various stakeholders. **It is important to recognise that the gaps identified related to NATS in this study are broadly relevant to all Air Navigation Service Providers and are not limited solely to NATS.** These gaps may have the potential to directly support safer, more reliable deployment and operation of eVTOL aircrafts.

Out of these 56 gaps for eVTOL operations, **27 were identified to be applicable to <u>both eVTOL and current helicopter operations</u>** (Table 1) thus, making the latter an area of focus for the CAA to consider.

This project has shown that STPA can effectively assess the sophisticated aspects of emerging aviation technologies and the intricacies of planned operational improvements and could potentially serve as a valuable approach for the CAA in the future.

Stakeholder	**Number of Mitigations NOT addressed by current aviation regulations**	**Number of Mitigations NOT addressed with current aviation regulations which are applicable to both eVTOL & current helicopter operations**
Regulator (CAA)	17	11
Air Navigation Service Provider (NATS)	8	8
eVTOL Operator	2	
Vertiport operator (also considering them as helipad operator)	29	8

Table 1 Summary of gaps linked to different stakeholders

Key recommended actions

The following actions are recommended as an outcome of this study to implement a robust safety management system that proactively mitigates risks and adapts to the challenges introduced by emerging eVTOL technology:

1. Review and assess the risk posed due to the **27 gaps on current helicopter operations**
2. CAA to review **17 "gaps"** under its purview for eVTOL operations.
3. CAA to provide guidance on the "gaps" identified for Air Navigation Service Providers, eVTOL operators and Vertiport operators, and **incorporate the findings in the development of the UK Airspace Modernisation Strategy**.

Project Overview

About STPA and its proposed novel extensions

System Theoretic Process Analysis (STPA) is a top-down approach based on the conceptual accident causality model called System Theoretic Accident Model and Processes (STAMP). It treats accidents as a control problem instead of a failure problem and it prevents accidents by enforcing constraints on the behaviour of the system. STPA considers a diverse range of causal factors of the hazardous interactions, including flawed control algorithms due to flaws in their specifications, communication errors, and delays, conflicted controls, processing delays, misinterpretations of the received data or signals, etc. The conventional STPA approach involves four distinct steps. At WMG, we have formulated a concept aimed at prioritising the STPA results to effectively manage the project's considerable complexity and volume of results. Figure 1 illustrates the flowchart capturing both standard STPA process (blocks filled in yellow) and extensions for prioritisation of STPA results (blocks filled in blue).

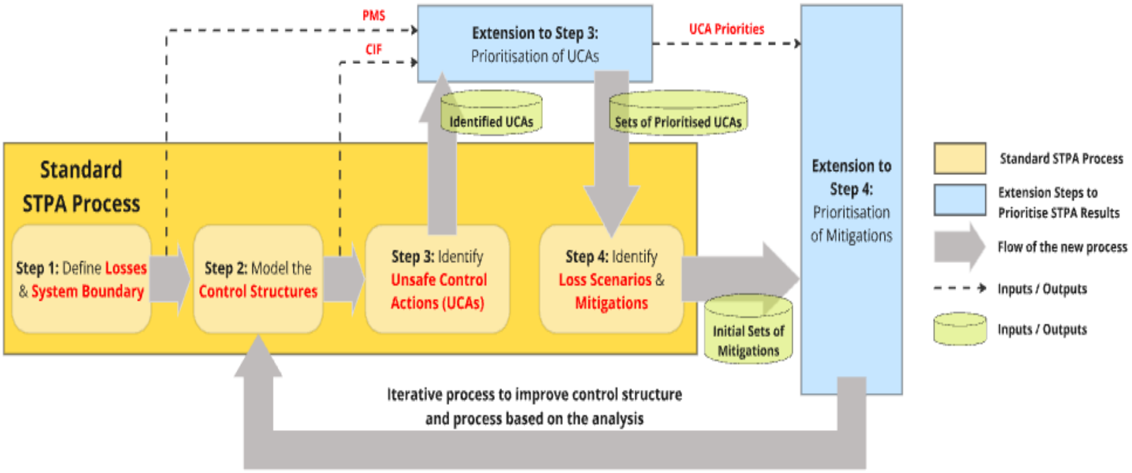
PMS
CIF
Extension to Step 3: Prioritisation of UCAs
UCA Priorities
Identified UCAs
Sets of Prioritised UCAs
Standard STPA Process
Step 1: Define Losses & System Boundary
Step 2: Model the Control Structures
Step 3: Identify Unsafe Control Actions (UCAs)
Step 4: Identify Loss Scenarios & Mitigations
Extension to Step 4: Prioritisation of Mitigations
Initial Sets of Mitigations
Iterative process to improve control structure and process based on the analysis
Standard STPA Process
Extension Steps to Prioritise STPA Results
Flow of the new process
Inputs / Outputs
Inputs / Outputs

Figure 1 Standard STPA Process (yellow blocks) and Extensions to Steps 3 and 4 (blue blocks) for Prioritisation of UCAs and Mitigations

Step 1: Define purpose of the analysis

STPA starts by identifying any losses which are unacceptable to the stakeholders and system-level hazards. The system boundary is also defined in this step. The system boundary defines the range of ownership and analysis – i.e., the components outside the system boundary are not accessible to the designer for any potential upgrades required, and the components within the boundary can be appropriately managed or redesigned if the analysis outcome suggests.

Step 2: Model the Control Structure

The subsequent step involves developing a system model referred to as a control structure. The control structure consists of hierarchical functional blocks illustrating the **functional** interactions between the system components by representing the system as a series of feedback control loops. Each control loop consists of a controller that provides control actions (CA) to control some processes and enforce constraints on the behaviour of the controlled process. The control algorithm represents the controller's decision- making process, it determines the control actions to provide. Controllers also have process models that represent the controller's internal beliefs (which may include beliefs about the process being controlled or other relevant aspects of the system or the environment), used to make decisions.

Step 3: Identify Unsafe Control Actions (UCA)

After identifying Control Actions (CA) in the control structure, each CA is further analysed to identify how the CA would manifest into an Unsafe Control Action (UCA). Depending on the context of providing a CA, it could lead to one or multiple system-level hazards, which in turn lead to the losses (identified in Step 1). If a CA were always unsafe, then it would never be included in the system design. The CA is analysed in four categories to identify UCAs:

- **Not providing** the CA leads to a hazard.
- **Providing** the CA **incorrectly** or when not needed leads to a hazard.
- **Providing** the CA **too early** or **too late** or **in the wrong order** leads to a hazard.
- **Providing** the CA **too long** or **stopping providing the CA too soon** leads to a hazard.

Step 4: Identify Loss Scenarios

Once the UCAs are identified for all the control actions in the control structure, possible Loss Scenarios, which describe the Causal Factors (CFs) that can lead to the UCAs, are identified by analysing the specific control loops of the Control Actions. For a UCA to occur, the process model of the controller has a belief based on which it believes that the CA it is directing is safe when it is unsafe. The causes of such beliefs can be identified based on two types of Loss Scenarios – i.e., 'Type A' and 'Type B'. Type A Loss Scenarios mainly explain what triggers the CAs to be unsafe. Type B Loss Scenarios explain how correct CAs are not executed or are improperly executed, leading to UCAs. Once the Loss Scenarios and their corresponding Causal Factors are analysed, Mitigations are then defined for prevention or mitigation of these Causal Factors.

A more detailed overview of STPA and its steps can be found in **Annex A**: Overview of various safety analysis approaches including STPA (base version).

Extension of Standard STPA Process for Results **Prioritisation**

STPA can identify numerous UCAs and Mitigations depending on the level of granularity of the analysis and the complexity of the system being analysed. Managing these large number of results can become challenging. Consequently, there has been extensive research on methods to enhance the STPA process to manage the large number of UCAs and Mitigations, especially when dealing with large, complex systems to enable the stakeholders and the analysts to focus on the most critical aspects, to improve system safety. Prioritisation of UCAs would provide the option for the analysts to perform STPA Step-4 for only the highest priority UCAs and not the entire list of UCAs identified in Step-3. It is worth noting that the prioritisation of results may not be required for every STPA analysis. Figure 1 illustrates the flowchart capturing both standard STPA process (blocks filled in yellow) and extensions (developed by WMG) for prioritisation of UCAs and Mitigations (blocks filled in blue). These two extended steps will be elaborated in the subsections - **Extension to Step 3: Prioritisation of UCAs** and **Extension to Step 4: Prioritisation of Mitigations**.

Extension to Step 3: Prioritisation of UCAs

The methodology for the prioritisation of UCAs is based on three factors: Pre-Mitigation Severity (PMS), Controller Impact Factor (CIF), and Expert Judgement Score (EJ).

PMS is assigned based on the severity of the ranked losses (identified in STPA Step-1) that the UCAs lead to. CIF is assigned by identifying the position of the UCA Controller in the hierarchical control structure (created in STPA- Step 2). The EJ is calculated by collecting inputs from the SME. The following five factors of EJ were considered: Operational Disruption, Criticality, Detectability, Effect on Other Stakeholders, and the Likelihood of Occurrence.

To better evaluate and communicate the criticality of each UCA considering these three major factors- PMS, CIF and EJ, the development of a risk matrix was necessary. Risk assessment matrix is a classic tool to conduct semi-quantitative risk assessment. Recognising that safety is not an exact science, we opted for a matrix presentation that depicts criticality across five levels, which starts from very low to very high, instead of using a unique number.

The process for calculation of the Expert Judgment score and creation of UCA Prioritisation matrix is detailed in **Annex B**: Detailed Process for Prioritisation of UCAs and Mitigations.

Extension to Step 4: Prioritisation of Mitigations

The STPA Step-4 analysis can generate numerous (several hundreds) mitigations. A Mitigation prioritisation framework would help the stakeholders to prioritise and address the most critical sets of mitigations. The methodology for prioritisation of

Mitigations developed by WMG as an extension to the standard STPA methodology is briefly described in this section.

There are two key factors considered for the prioritisation of Mitigations: **1) UCA Priority**; and **2) Mitigation Score**.

The UCA Priority is defined as the product of EJ and CIF that were identified in the UCA Prioritisation step. The Mitigation Score of each Mitigation is calculated based on four factors: Time; Cost; Type of Mitigation; and Likelihood of occurrence. The inclusion of UCA Priority ensures that each proposed Mitigation (to prevent or mitigate the UCA) inherits the priority of the UCA that it links to. The Mitigation Score ensures that the criticality of each Mitigation is considered.

The process for calculation of the Mitigation Score and generation of the Mitigation prioritisation matrix is detailed in **Annex B**: Detailed Process for Prioritisation of UCAs and Mitigations.

Methodology

The Project comprised of two phases:

- Preliminary Phase focused on Helicopter Operations,
- Dedicated phase for eVTOL operations.

The objective was to analyse existing Helicopter operations as a starting point and identify the variations when applied to the relatively novel eVTOL technology. The timeline in Figure 2 illustrates the links between the two phases of the project. It further highlights how STPA, with its extended steps for prioritisation was applied throughout the project. It captures the progression from initial planning, scoping activities, and the definition and prioritisation of losses to modelling five control structures covering both organisational and operational aspects. This was followed by the identification of UCAs, highlighting those requiring consideration and mitigation strategies incorporating stakeholders' inputs during one-to-one workshops, and ultimately, the derivation and refinement of mitigations, along with the identification of gaps in procedures, regulations, and policies in one-to-one workshops. By integrating experts' inputs at each phase and focusing on critical UCAs and Mitigations, the process ensured that regulatory gaps were effectively identified and addressed, supporting the safe deployment of eVTOL operations.

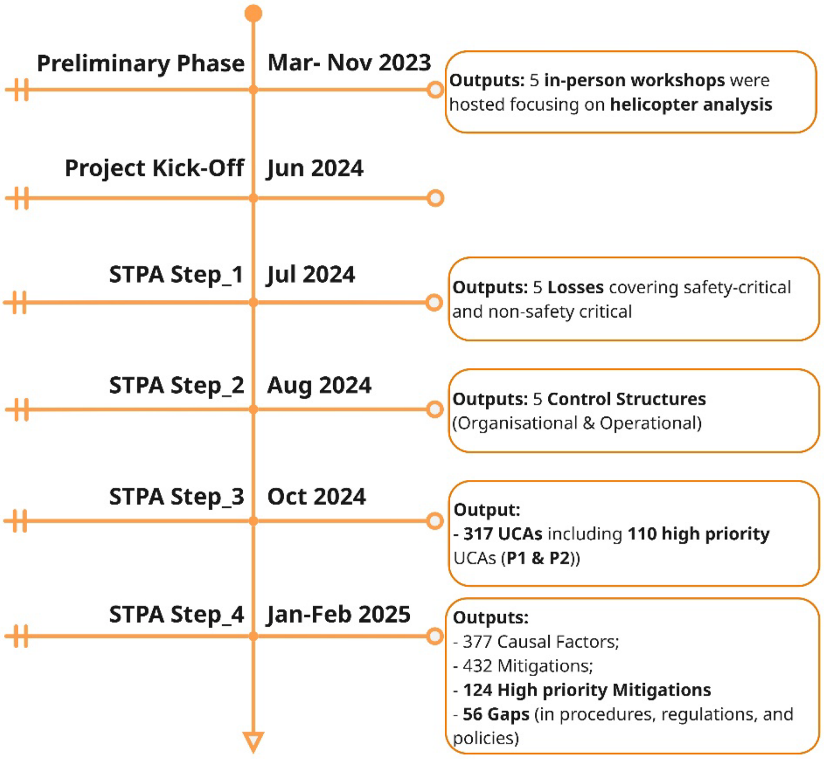
Preliminary Phase
Mar- Nov 2023
Outputs: 5 in-person workshops were hosted focusing on helicopter analysis
Project Kick-Off
Jun 2024
STPA Step_1
Jul 2024
Outputs: 5 Losses covering safety-critical and non-safety critical
STPA Step_2
Aug 2024
Outputs: 5 Control Structures (Organisational & Operational)
STPA Step_3
Oct 2024
Output:
- 317 UCAs including 110 high priority UCAs (P1 & P2))
STPA Step_4
Jan-Feb 2025
Outputs:
- 377 Causal Factors;
- 432 Mitigations;
- 124 High priority Mitigations
- 56 Gaps (in procedures, regulations, and policies)

Figure 2 Project timeline and approach

Preliminary Phase: STPA for Helicopter Operations

System under analysis: The eVSLG identified the Helicopter Operations from London Heliport to Silverstone Aerodrome (as represented in Figure 3) on the day of the British Grand Prix, as the system under analysis. This was selected since the number of movements at this particular event replicates the daily high frequency utilisation of an Urban Air Mobility model of a standard eVTOL operation as identified in the UK Future of Flight programme. The route from London Heliport to Silverstone Aerodrome was split into three zones: 1) London Heliport zone (Phase 1): this zone is covered by London Heliport ATC; 2) Between London Heliport and Silverstone Aerodrome (Phase 2); and 3) Silverstone Zone (Phase 3).

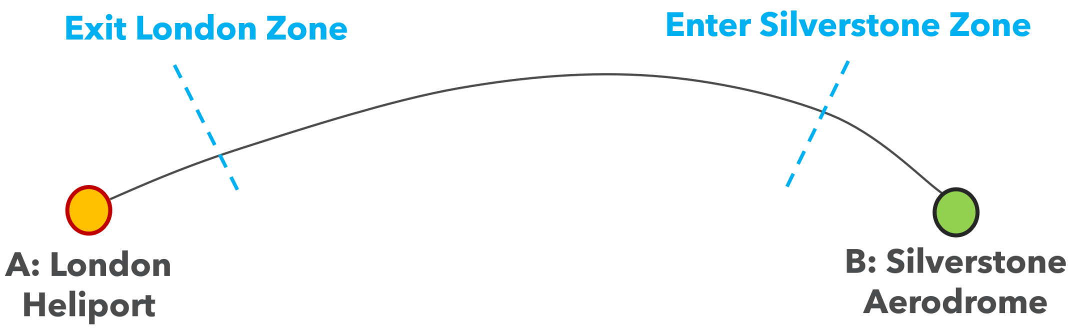

Figure 3 Route chosen for the system under analysis

Process: To undertake the STPA, five in-person workshops were held between March and November 2023, attended by different stakeholders involved in the operation from London Heliport to Silverstone Aerodrome. These included helicopter pilots, London Heliport SMEs, NATS SMEs, CAA SMEs, and Silverstone Aerodrome site manager etc. Because of the complexity of the analysed system, the analysis was also split into organisational part and operational part. The organisational analysis focused on modelling and analysing the interactions between the organisations before the day of the operations. The operational analysis focussed on the interactions for specific flight on the day.

Results: As part of this exercise, all four steps of STPA were conducted. Because of the complexity of the eVTOL Operation system, two-levels of control structures were created initially. Level 1 captures the main components and their interactions. The Level 1 analysis was done during the initial phase of the project when available information of the system was very limited. It helped identify initial results and broader issues before analysing more detailed control structures. Level 2 details the decompositions and interactions of those main components at the sub-components level.

The control structures were initially modelled as a white board exercise and transferred into a software tool (Astah System Safety). The control structures were reviewed in a workshop (Sep 2023) with the entire eVSLG membership and updated based on the feedback received during the workshop.

In Step 3 of STPA (identification of UCAs), high priority CAs were identified from the control structures and corresponding UCAs were identified. Some of the CAs used for analysis included: “Take-off Clearance”, “Weather Information”, “Route Approval”, “Remain Outside ATZ”, “Clearance in Silverstone Aerodrome” and “Clearance to Final”. It was impressive to observe that some of the UCAs identified from the analysis were already known to the stakeholders, yet no corrective safety measures were implemented.

Policy implications - STPA for eVTOL Operations: While the analysis uncovered many new UCAs that were new or unknown to the stakeholders, some were already known but no actions were taken to make the system safer. Part of the reason being that these unsafe situations were not presented consequently as part of a rigorous analysis before and were primarily seen as a one-off experience. “See and Avoid” is a fundamental tenet of visual flight operations and is used by pilots as their main mitigation of aircraft separation when operating under the visual flight rules. However, it is the only current regulatory safety mitigation while waiting for onward “Clearance” into the Silverstone temporary restricted airspace alongside other converging air traffic. The analysis showed a need to implement Electronic Conspicuity (EC) (or similar capabilities) especially for helicopter operations when used for special events, and other high density traffic scenarios, due to the volume and workload of each of the stakeholders involved.

The STPA for helicopter operations highlighted the need to perform such a systems-thinking-based approach to the emergent eVTOL technology with new and amended potentially unsafe interactions between stakeholders. Following on from this analysis, it was planned to undertake STPA to identify unsafe interactions between the stakeholders with the goal to generate recommendations to mitigate risks associated with the introduction of eVTOLs.

STPA for eVTOL Operations

Building upon the STPA conducted for helicopter operations, the STPA for eVTOL Operations was started, involving eVTOL ecosystem stakeholders. The goal was to identify the primary distinctions in terms of STPA outcomes and to develop recommendations for the safe integration of eVTOLs into the current airspace. The problem statement and objectives of the project are listed below.

Problem Statement

Introduction of eVTOL will require input from multiple stakeholders (i.e., technology, policy, operations, infrastructure, airspace etc). The UK Airspace Modernisation Strategy is focused on integration rather than segregation of different airspace user groups. Therefore, new and amended interactions may take place in the new operational environment, which will lead to emergent behaviours in the ecosystem. These emergent behaviours pose a risk both to the current ways of operating, and may introduce new risks as the ecosystem develops, particularly at scale. Applied research is therefore required to inform future policy and operational development to manage the safe introduction of eVTOLs within a challenging environment. The timeline for the introduction of eVTOLs is short, with leading OEMs forecasting early operations within the next 2-3 years so the requirement to understand and mitigate the emergent risks is short.

Objectives and Planned Actions

Objective 1: To identify new and amended interactions between stakeholders that already pre-existed in helicopter operation.

- **Action 1.1:** To review previous helicopter safety analysis model already developed by eVSLG to capture high volume operations (Refer to section - STPA for Helicopter Operations (Preliminary Phase))

- **Action 1.2:** To identify differences between Helicopter and eVTOL application.

Objective 2: To conduct analysis of unforeseen and unexpected interactions, which may compromise the stability and safety of the ecosystem.

- **Action 2.1:** To conduct analyses of UCAs for eVTOL application.

- **Action 2.2:** To conduct gap analyses between current policy development and the UCAs identified

Objective 3: To capture Mitigations to prevent these unsafe interactions between stakeholders, thereby mitigating emergent risks.

- **Action 3.1:** To identify scenarios leading to unsafe interactions between stakeholders.

- **Action 3.2:** To develop Mitigations to detect or prevent unsafe interactions.
- **Action 3.3:** To implement ranking and prioritisation of Mitigations

Objective 4: To develop those mitigations into recommendations for each relevant stakeholder group, resulting in policy updates, operational instructions and practical guidance.

- **Action 4.1:** To develop practical, implementable recommendations for action.

Objective 5: To communicate the analysis and outcomes with stakeholders and develop momentum for change.

- **Action 5.1:** To organise regular workshops and discussions with the stakeholders.

Following the standard STPA process for eVTOL operations, in STPA Step-1, the System Boundary and five Losses were defined. The Losses covered both safety-critical (i.e., human loss and material loss) and business-critical losses (i.e., mission loss, consumer demands loss, and business goal loss). Throughout the project, the results created by the STPA experts were reviewed by domain experts through both in-person workshops and virtual meetings. The domain experts come from a diverse range of backgrounds - this includes the UK Aviation Regulator (CAA), eVTOL Operators (Flexjet, Bristow Group), Air Navigation service provider (NATS), British Helicopter Association, Vertiport Operator (Skyports), OEM (Lilium, Vertical Aerospace) and Helicopter Pilots. A timeline for the project is shown in Figure 2.

In Step-2 five Control Structures (one for each phase) were created to capture both organisational and operational aspects of eVTOL. In Step-3, 317 UCAs were identified in total across the five phases.

Due to the large number of UCAs generated, they were prioritised based on a concept developed by WMG (extension to standard STPA Step 3 and Step 4) and 110 of these 317 UCAs were identified as high priority ones for further analysis in Step-4. Following Step-4, 377 CFs were identified from these 110 high priority UCAs. 432 Mitigations were proposed to prevent or mitigate these CFs. The mitigations were further managed and prioritised following the prioritisation concept. 124 high-priority unique mitigations out of the 432 mitigations were identified. To create a Gap Report, CAA Subject Matter Experts (SMEs) further analysed these high priority Mitigations to determine whether they were ‘gaps’ in the existing regulations / policies / procedures. Those ‘gaps’ will be further considered by the CAA.

Results of the STPA Analysis for eVTOL operations

Assumptions

The STPA for eVTOL Operations was based on the following assumptions about the system.

Assumptions about eVTOL features/ characteristics:

- Electrically powered
- Vertical take-off and landing capability
- One onboard pilot
- Seating capacity in the range of 4 to 6 passengers and one pilot
- No autonomous flight operations considered
- Operation under Visual Flight Rules (VFR)
- See and avoid principles

Assumptions about the Operating Environment:

- A service area focused on a large modern city with features including an urban metropolitan landscape, high-rise buildings or a major airport hub
- Airspace shared with other manned and unmanned air traffic and eVTOL
- Operation in Visual Meteorological Conditions (VMC)
- Infrastructure sufficient for battery charging, dispatch, passenger management, and other associated needs, including purpose-built vertiports for take-off and landing are available

Other Assumptions:

- The battery management system of the eVTOL is safe and reliable. Fire hazards are not considered in the current scope of the analysis.
- Batteries will be charged *in situ*, swapping of batteries is not considered.

The eVTOL aircraft itself is treated as a black box and the eVTOL technical system is not analysed for potential causes that can lead to accidents.

STPA Step-1 (Define Purpose of the Analysis)

As part of STPA step 1, the losses that were unacceptable to stakeholders were identified. An initial list of losses was defined by the STPA analysts based on prior experience. These losses were then reviewed and ranked/prioritised by the stakeholders, based on their stake in the system, i.e. what they valued and what their goals were.

Table 2 shows the list of ranked losses. Safety-critical losses (example – L1) were ranked high while non-safety critical or business-critical losses (example- L-4, L5) were ranked low.

Loss-ID	Losses	Ranking
L-1	Loss of life or injury to 1st, 2nd or 3rd parties *(Human Loss)* *Note: 1st party- eVTOL crew, 2nd party - passengers and 3rd party- any one external to the eVTOL aircraft*	1
L-2	Loss of or damage to the eVTOL or surrounding item/property/infrastructure (*Material Loss)*	2
L-3	Loss of transportation mission (*Mission Loss)*	3
L-4	Loss of customer satisfaction or public confidence in eVTOL *(Consumer Demands Loss)*	4
L-5	Loss of business goal of eVTOL Operator *(Business Goal Loss)*	5

Table 2 List of Losses

Based on discussions with the stakeholders, the system boundary was also defined in this step. The system under analysis comprised of the Regulator (CAA), the Local Authorities (associated with the take-off and landing sites), Air Navigation Service Provider (NATS), Licensed Vertiports/Aerodromes (at take-off and landing sites), the eVTOL Operator, eVTOL aircraft (including the Commander) and the eVTOL Manufacturer. The local landowners (at both take-off and landing sites), the local emergency authorities (outside the Licensed Vertiport/ aerodrome) and the infrastructure providers - UK Power Network and UK Data Network, were excluded from the system (outside the system boundary).

STPA Step-2 (Model the Control Structures)

The analysis was split into an organisational analysis and operational analysis. Organisational analysis primarily focussed on modelling and analysing the interactions between the organisations prior to the flight operations. Operational analysis focussed on the interactions for specific flight operations on the day. The analysis was split into five phases (Phase 0.1, Phase 0.2, Phase 1, Phase 2 and Phase 3) with one control structure for each phase. This was done to make the complex analysis more manageable and for better readability of the control structures. Phase 0 was split into two phases – a) Phase 0.1- covering the organisational interactions as part of the preparation for the flight (including regulatory aspects) and b) Phase 0.2- covering operational interactions in preparation for the flight (until and including passenger boarding).

Route from London Heliport to Silverstone Aerodrome was split into three zones: 1) London Heliport zone (Phase1): this zone is covered by London Heliport ATC; 2) Between London Heliport (North London) and Silverstone Zone (Phase 2); and 3) Silverstone Zone (Phase 3). Separate control structures were created for each phase (5 control structures in total). The control structures were created at the highest level of abstraction - Level 1 (less detailed), using the tool Astah System Safety (refer to 'STPA for Helicopter Operations- Phase 1' section for information about abstraction levels). While the STPA analysis for eVTOL Operations based on the Level 1 control structure has provided insightful results, the possibility of performing further analysis based on a more refined and detailed control structure (Level 2) based on this activity, could be explored as part of future work.

Following phases were defined (Figure 4) with a corresponding control structure for each:

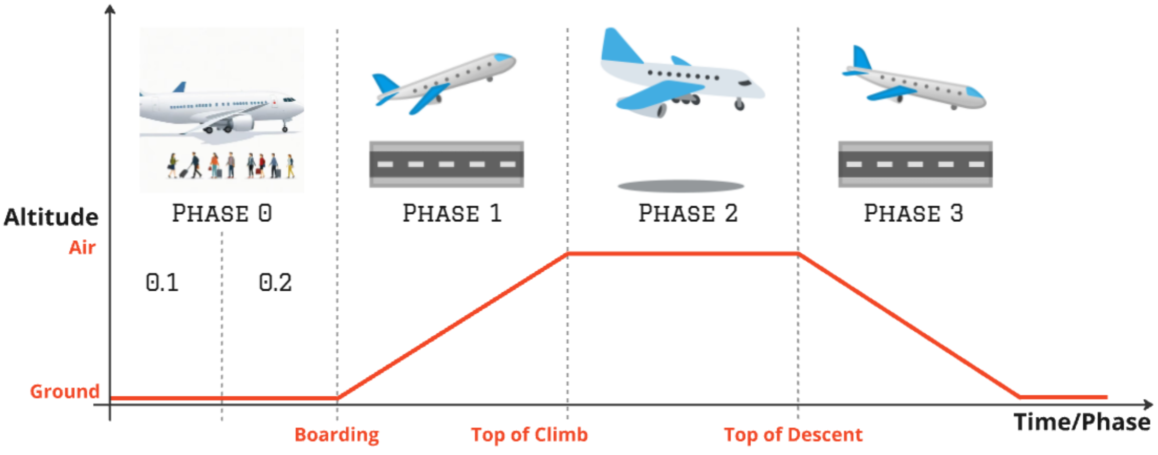

Figure 4 eVTOL Flight Phases

- **Phase 0.1** covers the **regulatory preparation** for the flight (organisational). This control structure (Figure 5) shows the interactions between the various stakeholders prior to the start of flight operations. It is worth noting that the 'Regulator' is included only in this control structure.
- **Phase 0.2** covers the **operational preparation** for the flight (until and including passenger boarding). This control structure (Figure 6) shows the interactions between the various stakeholders as part of the preparation for the flight operation (up to and including passengers boarding the eVTOL aircraft).
- **Phase 1** covers the **take-off from London Heliport** when the eVTOL aircraft is in controlled airspace. This control structure (Figure 7) shows the interactions between the various stakeholders during the flight take-off phase (in controlled airspace).
- **Phase 2** covers the **cruise phase** – i.e., after the aircraft has climbed, mostly in uncontrolled airspace. This control structure (Figure 8) shows the interactions between the various stakeholders during flight operation after the aircraft has climbed (major part of the trip is in uncontrolled airspace).
- **Phase 3** covers the flight operation from the **start of the descent to completion of landing** (landing at Silverstone Aerodrome). This control structure (Figure 9) shows the interactions between the various stakeholders during the flight landing phase.

Phase 0.1 - Regulatory Preparation for the Flight

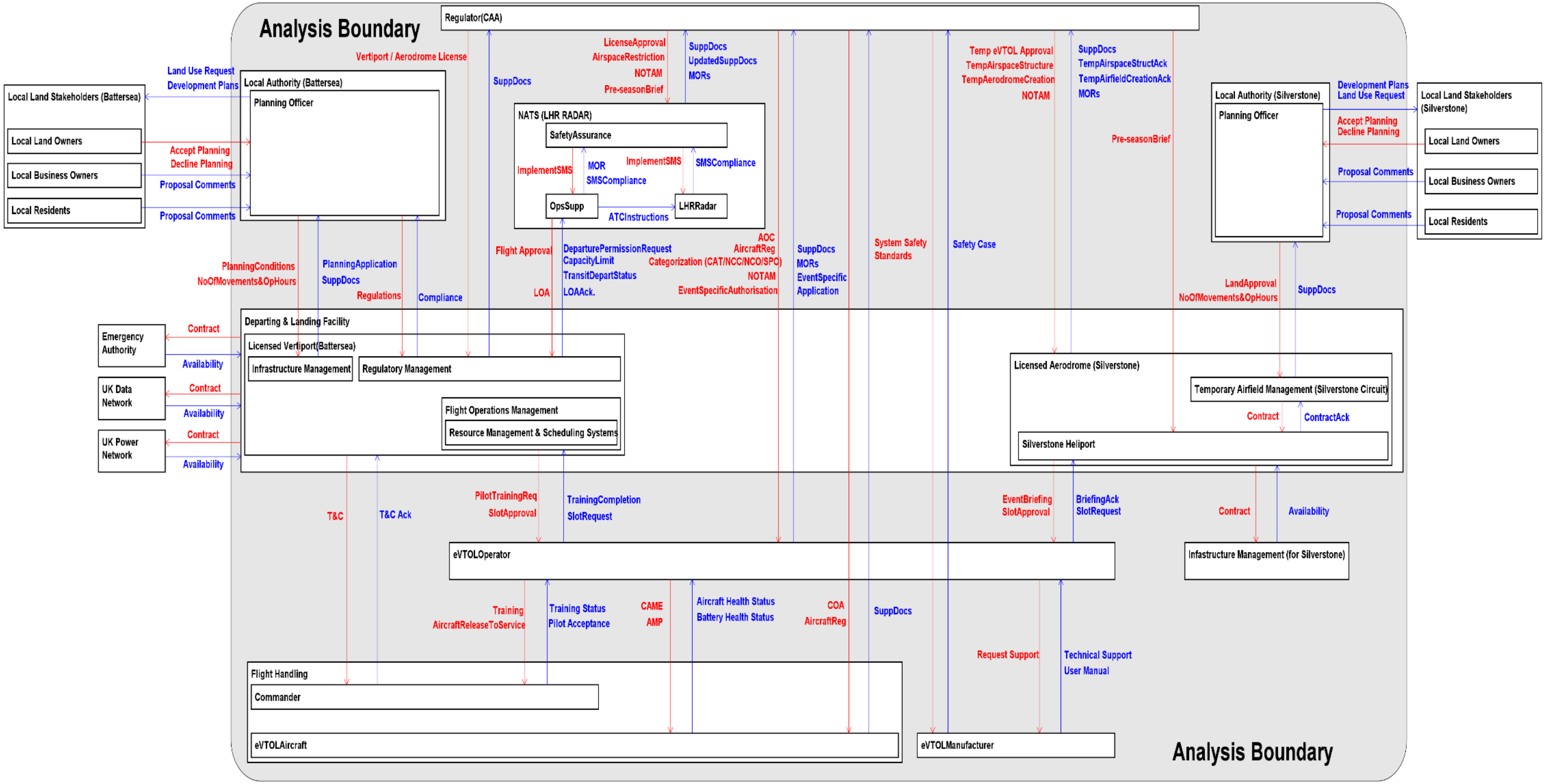

Figure 5 Control Structure for Phase 0.1

Phase 0.2 - Flight Operation Preparation

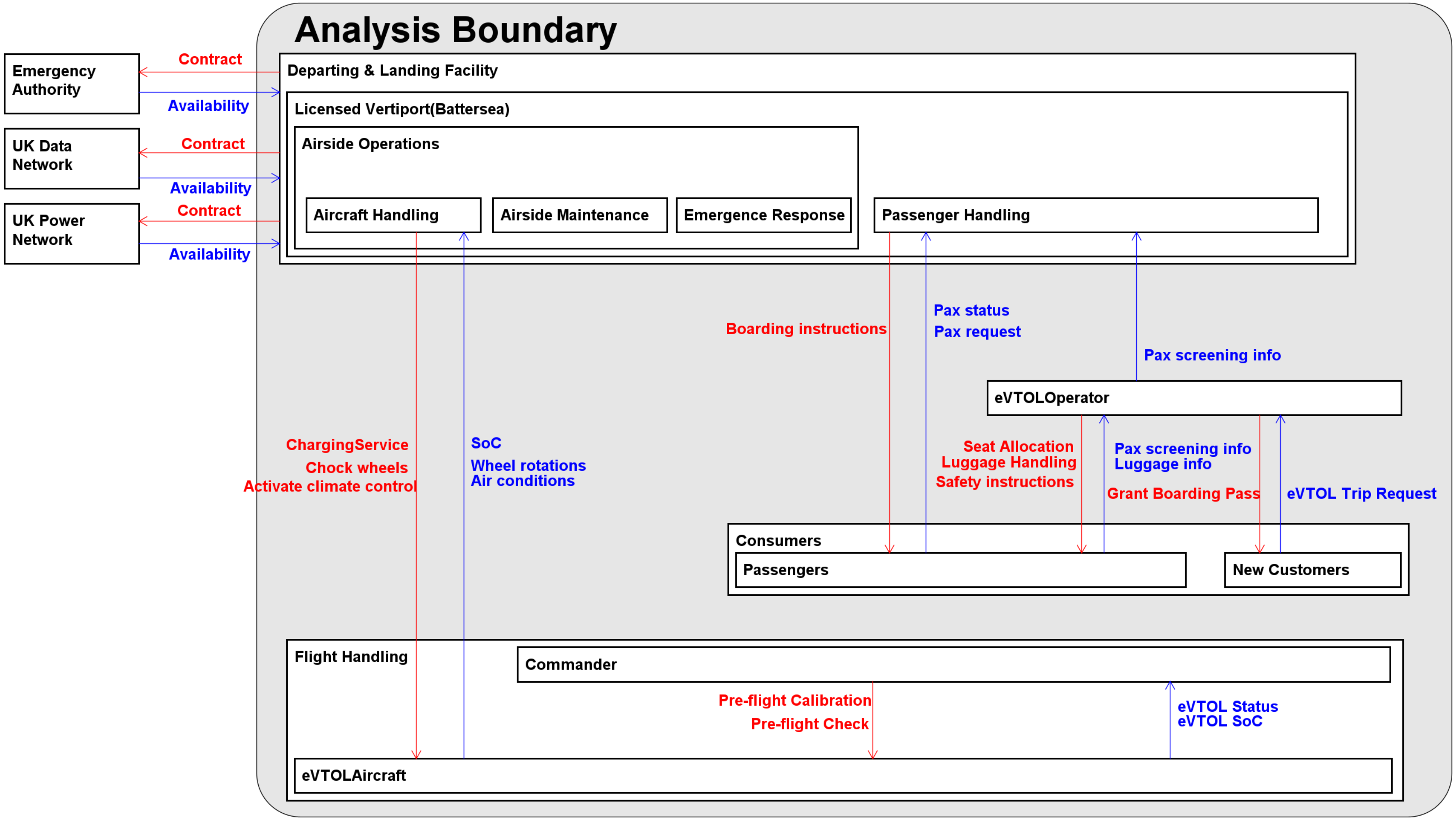

Figure 6 Control Structure for Phase 0.2

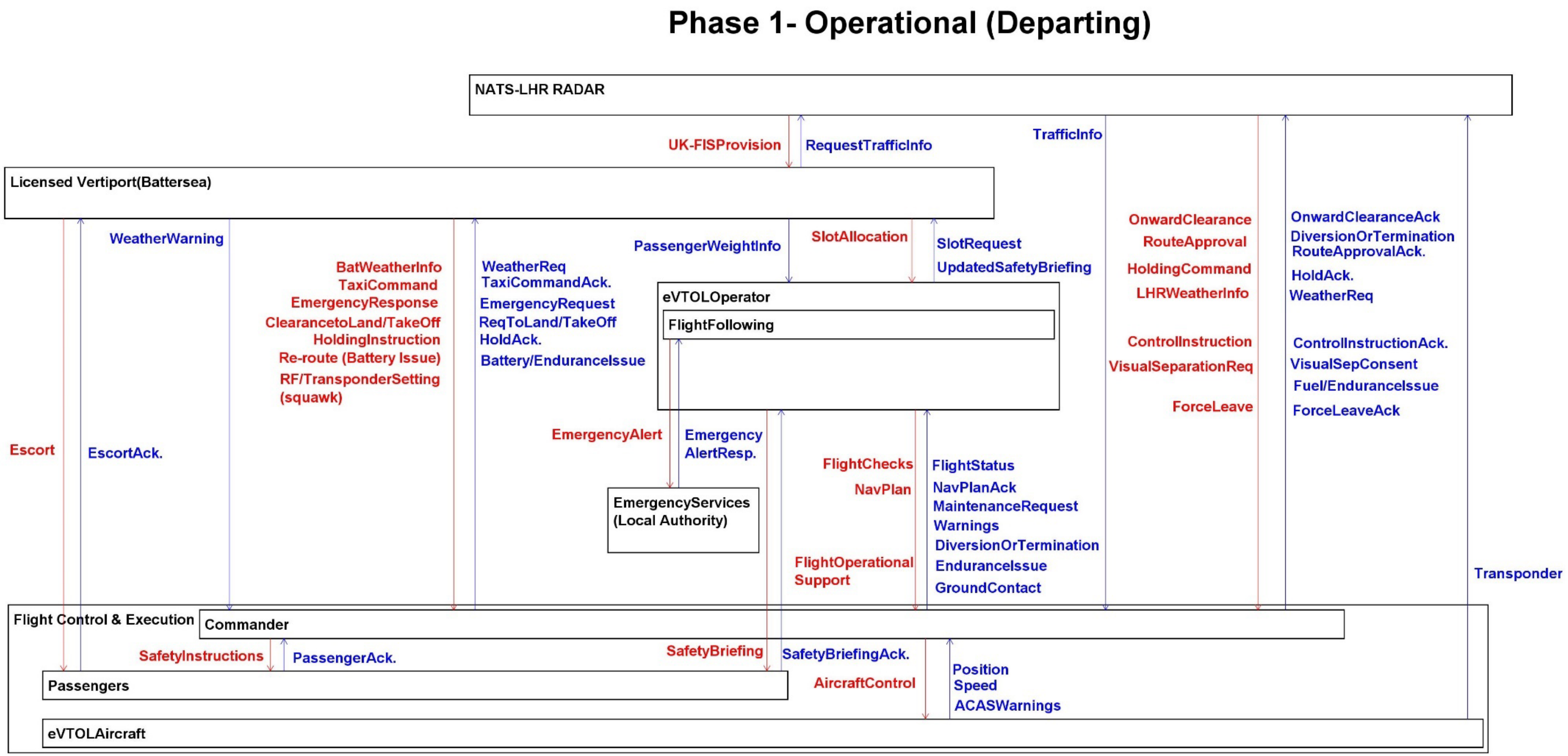

Figure 7 Control Structure for Phase 1

Phase 2-Operational (In the Air)

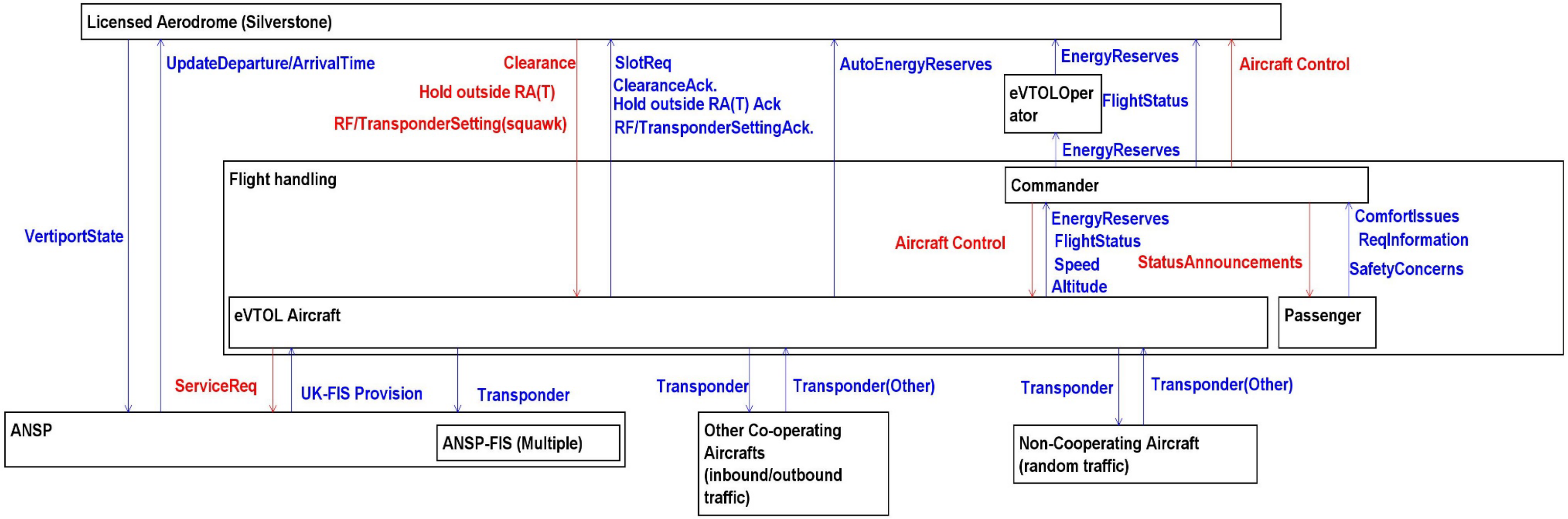

Figure 8 Control Structure for Phase 2

Phase 3 -Operational (Landing Phase)

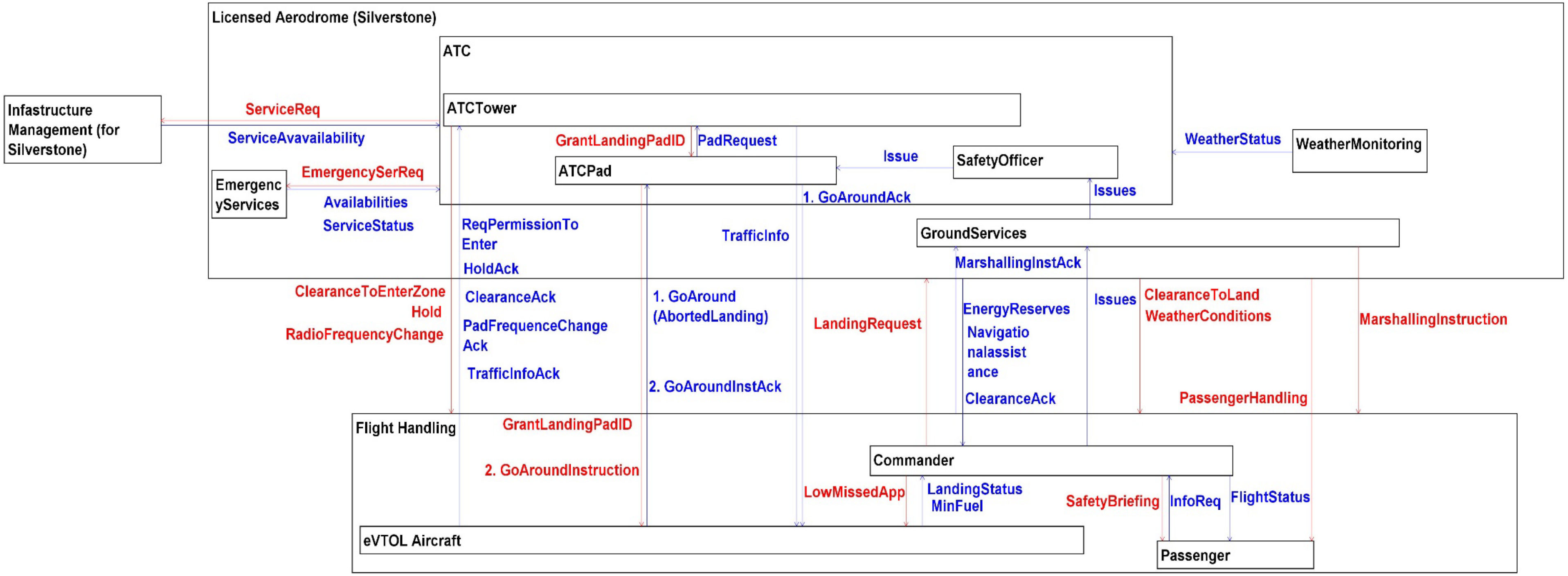

Figure 9 Control Structure for Phase 3

Differences Report between Helicopter and eVTOL Control Structures

This section gives an overview of the differences between the STPA control structures for Helicopter Operations and eVTOL Operations. At a very high abstraction level (less detailed, showing only the main components), there were not many differences in control structures between helicopters and eVTOLs. Some of the key differences that emerged during the workshops are discussed in this section. Although only some of these differences were visually represented in the control structures, the later steps of the analysis shed light on the specific Mitigations for eVTOL operations.

Given that eVTOLs are powered by Lithium-Ion batteries, the control structure considers infrastructure management for charging and corresponding interactions.

Currently, eVTOL aircraft have only a flight range of approximately several tens of kilometres to a few hundreds of km (endurance of less than an hour) which is shorter than that of helicopters which is approximately 600-800km (endurance of 3 or more hours). The limited range of eVTOLs compared to other aircraft, along with reduced carrying capacities, don’t lend themselves to things like search and rescue or making long-haul deliveries that helicopters can do. Hence, they would be more suitable for usage as air taxis and for leisure activities. In terms of the Air Operator certificates (AOCs), the number of AOCs for Helicopters (48) is significantly larger than that for early adopter eVTOLs.

Considering maintenance provisions, helicopters can be taken to general maintenance facilities while eVTOLs would need local maintenance provisions at the operating vertiports/aerodromes. Another factor considered was flight crew licensing. While CPL(H) was the requirement for Helicopter pilots, for eVTOLs, it would initially be a 'type rating' added to either a CPL(H) or a CPL(A).

The differences in effects of downwash/outwash for the safe operation between eVTOLs and Helicopters are not clearly known. (CAP 2576 - Understanding the downwash/outwash characteristics of eVTOL aircraft, 2023) & (CAP 3075 - Protecting the Future: Trials and Simulation of Downwash and Outwash for Helicopters and Powered Lift Aircraft, 2025) present some initial observations on the effects of downwash and outwash on the safe operation of eVTOL aircraft. Our understanding of downwash and outwash from helicopters is being challenged by eVTOL designs and configurations, potentially necessitating new control approaches and mitigations. Furthermore, as our comprehension of helicopter downwash and outwash evolves, existing control measures might also need to be revised. In the later phases of the project, once the downwash effects of eVTOLs are better known, policies and procedures to be adopted by the ground handling personnel, passengers, crew and uninvolved third parties can be formulated.

It was noted that certain specific interactions between the ATC and the Operator for Helicopters – such as 'Landing Pad ID Change' and 'Special Requests' were not applicable to eVTOLs.

eVTOLs may possibly be quieter than Helicopters, when the entire operation is considered, because much of their forward flight is using wing-borne lift, which pulls the aircraft forward once it acquires a certain velocity reducing the total energy needing to be produced by the thrust/propulsion system. During vertical manoeuvres, the rotor speed for eVTOLs is generally expected to exceed 1000 RPM while the main rotor speed of a helicopter is typically about 380 RPM. Although noise levels are influenced by various factors like rotor speed, pitch angle, and tip speed, there is a possibility that eVTOLs still might produce less noise compared to helicopters. This may pave the way for better public acceptance of eVTOLs when compared to helicopters. Noise abatement procedures can be tailored for eVTOLs considering this factor.

eVTOLs are divided into two categories: Enhanced and Basic, mirroring the principles of the helicopter categories A and B. Categories Enhanced and A requires continued safe flight and landing in almost all failure cases. Conversely, categories Basic and B do not have the same level of redundancies and might have to make an immediate safe landing. Both categories can operate safely, but category B and Basic are limited as to where they can operate (generally not over congested areas) as they must always have a safe landing area.

STPA Step-3 (Identify Unsafe Control Actions)

After the creation of control structures, Unsafe Control Actions (UCAs) were identified for each of the Control Actions (CA) in all the control structures, as part of STPA Step-3. There were 317 UCAs identified in total across the five phases (as shown in Table 3). As the number of UCAs identified was high, it was necessary to prioritise the UCAs to streamline the activities for the next phase (identification of loss scenarios and Mitigations) and focus on the most safety-critical UCAs (which led to the highest ranked losses in STPA-Step-1). Based on the application of the prioritisation concept (see section **Extension to Step 3: Prioritisation of UCAs**), the UCAs were populated in the UCA Prioritisation Matrix and assigned priorities from P1 (Highest) to P5 (Lowest). The 110 high priority UCAs (i.e., P1 & P2) were further analysed in the next step of STPA (Step-4).

Phase	No. of UCAs reviewed and prioritised	No. Of High Priority (P1 and P2) UCAs
Phase 0.1	124	53
Phase 0.2	47	7

Phase	No. of UCAs reviewed and prioritised	No. Of High Priority (P1 and P2) UCAs
Phase 1	75	31
Phase 2	37	15
Phase 3	34	4
Total	**317**	**110**

Table 3 UCA Statistics

Each UCA was assigned a unique ID (as indicated by the 'UCA-ID' column in Table 4) depending on the control structure/phase the corresponding UCAs were covered in.

UCA IDs are structured as follows: UCA (Ph U)-X.Y. Z where:

- U refers to the phase in which the UCA is identified.
- X denotes the number of the CA.
- Y represents the type of UCA, where:
  - Type 1: The CA is not provided
  - Type 2: The CA is provided incorrectly
  - Type 3: The CA is provided when not needed
  - Type 4: The CA is provided too early
  - Type 5: The CA is provided too late
  - Type 6: The CA is provided too long
  - Type 7: The CA is provided too short
- Z denotes the number of the UCA identified for the CA and same type.

For example, the **UCA(Ph1)-18.2.1** in Table 4 is the first UCA (i.e., Z = 1) of the CA number X = 18 (i.e. 'Onward Clearance') from Phase 1 (i.e. U = 1) Control Structure with type 2 - i.e., Y = 2 (The CA is provided incorrectly).

In this project, the UCAs were directly linked to losses instead of hazards, deviating from the typical STPA process. This approach was chosen as the analysis centred on interactions between various organisations and the eVTOL aircraft, as opposed to the analysis of a technical system (example: eVTOL aircraft, a collision avoidance system etc.). Moreover, this approach made it easier for SMEs who may not be STPA experts to comprehend the potential consequences of occurrence of UCAs.

The UCAs linked to each stakeholder were grouped, reviewed (through in person workshops and virtual meetings with the Regulator, Air Navigation Service Providers, Vertiport Operators, eVTOL Operators, Pilots and eVTOL Manufacturers) and then updated. A sub-set of the STPA step-3 results showing some of the UCAs linked to different stakeholders- Regulator, NATS, eVTOL Operator, Licensed Vertiport/Aerodrome and Commander in different phases (Phase 0.1, Phase 0.2, Phase 1, Phase 2, and Phase 3) is presented in Table 4 **.** The entire list of prioritised UCAs can be found in **Appendix A:** Deliverables.

UCA-ID	UCA Description	Link to Losses
UCA(Ph0.1)-28.2.1	**Regulator** reissues 'Vertiport / Aerodrome Licence' incorrectly (e.g., with insufficient risk assessments) when the vertiport is actively being used for flight operations. *Note: This does not stop the flight operation, accidents might occur.*	L1.1, L2.1
UCA(Ph1)-18.2.1	**NATS** (LHR RADAR) provides '*Onward Clearance'* incorrectly (incorrect height, routing) when there is a conflict (proximity to other aircraft, such as eVTOLs, helicopters, and fixed wing)	L1.1, L2.1, L3.2, L4.3, L5.2
UCA(Ph0.1)-50.2.1	**eVTOL Operator** provides 'Aircraft Release To Service' for aircraft despatch incorrectly when adequate checks on the aircraft have not been carried out, this has not been detected, and the eVTOL aircraft flies.	L1.1, L2.1
UCA(Ph2)-6.6.1	**Licensed Aerodrome (Silverstone Aerodrome)** provides 'Hold Outside RA(T)' too long when the eVTOL approaches its destination and does not have sufficient energy reserves for a safe 'hold'.	L1.1
UCA(Ph1)-17.1.1	**eVTOL Operator** does not provide 'Safety Briefing' (on fastening seat belts, stowing away cargo and use of portable electronic devices (PED) and the eVTOL experiences a turbulence while flying Note: The safety briefing could be provided by the ground crew or the aircraft operator. PEDs could interfere with the eVTOL's avionics and communication systems, particularly during critical phases of flight such as take-off, landing, and cruising at low altitudes.	L1.2, L2.4

UCA-ID	UCA Description	Link to Losses
UCA(Ph1)-25.5.1	**Commander** provides 'Aircraft Control' too late when the eVTOL aircraft is about to collide with an object (e.g.: infrastructure or other aircraft/drones)	L1.1, L2.1

Table 4 Some of the UCAs identified as part of Step-3

Following the application of the UCA prioritisation concept, a UCA prioritisation Matrix was created. A snapshot of the UCA prioritisation Matrix, showing a sub-set of the prioritised UCAs is presented in Figure 10.

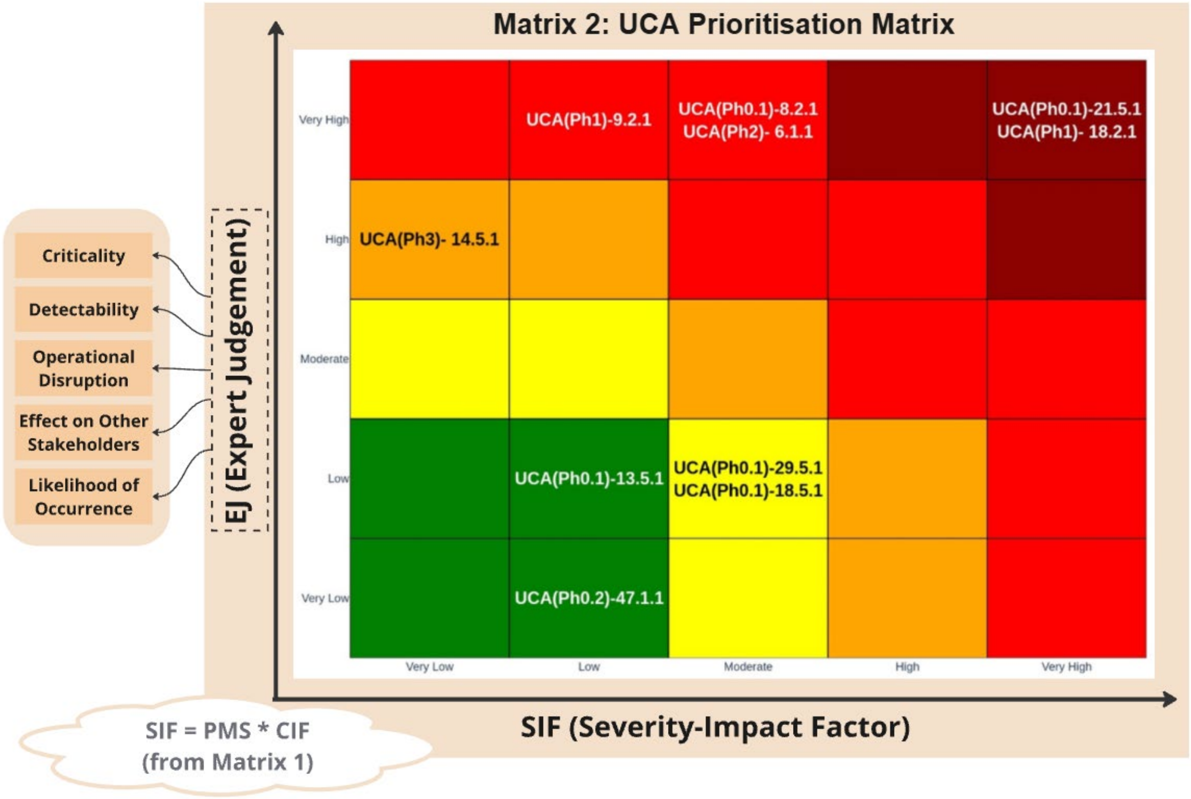

Figure 10 A snapshot of UCA Prioritisation Matrix

An extract from the prioritisation results showing some of the highest priority (P1) and lowest priority UCAs along with their PMS, CIF and EJ values are presented in Table 5.

UCA-ID	Priority	Description	PMS	CIF	EJ Score
UCA(Ph1)-22.2.1	P1	**NATS (LHR RADAR)** provides incorrect 'Control Instruction' when there is a situation that can cause air traffic conflict.	20	7	97.384
UCA(Ph1)-	P1	**NATS (LHR RADAR)** provides	20	7	29.859

UCA-ID	Priority	Description	PMS	CIF	EJ Score
18.2.1		'Onward Clearance' incorrectly (incorrect height, routing) when there is a conflict (close proximity to other eVTOLs, helicopters and traditional aircraft)			
UCA(Ph0.1)-13.5.1	P5	**Regulator** provides 'Temp eVTOL Approval' too late (by x weeks) when the flight is already scheduled.	4	8	208.844
UCA(Ph0.2)-47.1.1	P5	**eVTOL Operator** does not provide 'safety instructions' when passengers who are boarding have very limited knowledge/awareness of the safety procedures.	7	4	266.845

Table 5 UCAs and their respective PMS, CIF, and EJ

Implementation of the Prioritisation approach produced promising results in effectively ranking the UCAs. The colour-coded presentation helped focus on areas of criticality and identify UCAs that required immediate consideration. For example, UCA(Ph1)-18.2.1 and UCA(Ph1)- 22.2.1 (Table 5) were in the dark-red area of the UCA prioritisation matrix (Figure 10), indicating high criticality and requiring immediate mitigatory actions. These two UCAs were linked to catastrophic losses (e.g., loss of life), which were critical (as defined by stakeholders). They were also assigned a very high CIF, and failure to mitigate these UCAs could affect other Controllers and lead to severe losses. Stakeholder input also confirmed that these UCAs were highly relevant and likely to occur (EJ Score), justifying their placement in the dark-red area (highest priority).

In contrast, the UCAs in the green area of the matrix (Figure 10) were estimated to be non-critical. For instance, UCAs 13.5.1 and 47.1.1 were associated with partial tactical mission losses and significant customer satisfaction losses. Experts also ranked these UCAs as unlikely, which was reflected in their EJ scores derived by the Monte Carlo simulation, thereby justifying their placement in the green area.

When safety is paramount, objectivity is essential in ranking these UCAs. While reducing the number of UCAs can help manage the analysis outputs, it is crucial not to overlook any UCA that might lead to catastrophic losses. It was observed that there were considerable differences in values assigned to different EJ factors for the same UCAs, by different individuals. Performing the EJ assessment for UCAs as a group activity for each stakeholder, was one way to address this. The Monte Carlo simulation (MCS) is a probabilistic model that can include an element of uncertainty or randomness in its prediction (Rose, 2023). Another approach to tackle the subjective nature of EJ assessment was application of MCS to reduce the uncertainties induced by differences in EJ factor values assigned for the same UCAs, by different individuals. We adopted the latter and by combining inputs from STPA analysis with expert judgments and verifying these through MCS to reduce uncertainty, we generated significant data to assess risks and rank the UCAs effectively.

Following the application of the concept for the prioritisation of UCAs,110 High priority (P1 & P2) UCAs were taken up for the identification of loss scenarios and mitigations in the next step.

STPA Step-4 (Identify Loss Scenarios)

In this step, all the high priority UCAs (P1&P2) from the previous step (Step-3) were analysed to identify the potential CFs that could lead to the occurrence of these UCAs. Later, Mitigations were proposed to prevent or mitigate these CFs. The Step-4 analysis of 110 P1 & P2 UCAs resulted in the identification of 377 Causal Factors. 432 Mitigations were proposed to prevent or mitigate these Causal Factors. As domain experts, the stakeholders (Regulator (CAA), eVTOL Operator (Bristow Group), Air Navigation service provider (NATS), Vertiport Operator (Skyports) and Helicopter Pilots) reviewed these potential Causal Factors and Mitigations.

To deal with the large number of Mitigations generated, they were further analysed (to identify unique ones) and prioritised (using the concept mentioned in section – Extension to Step 4: Prioritisation of Mitigations) to create a list of unique high priority Mitigations assigned to different stakeholders – the Regulator, Vertiport Operator, eVTOL Operator and Air Navigation service provider (NATS). The Mitigations were analysed further to filter out all duplicates (as one Mitigation could address multiple CF) which resulted in 202 unique Mitigations. These unique Mitigations were prioritised generating 124 unique high priority Mitigations (Regulator – 58, Vertiport - 40, Operator – 16 and NATS –17). Table 6 presents the statistics of the STPA Step-4 analysis results.

Phase	Total No. of CFs	Total No. Of Mitigations	Total No. Of Unique Mitigations	No. Of Unique High Priority Mitigations
Phase 0.1	181	234		**124** Regulator-57(P1-P2)
Phase 0.2	45	35	**202**	Vertiport Operator -36 (P1)
Phase 1	71	97		eVTOL Operator–15(P1-P3)
Phase 2	74	61		Air Navigation Service Provider (NATS)-16(P1-P4)
Phase 3	5	5		
Total	**377**	**432**		

Table 6 Statistics of STPA Step-4 Results

An extract of the Step-4 results showing the Mitigations proposed to address the various types of Causal Factors (organisational issues, communication errors, missing Feedback/information, inadequate Control Algorithms, delayed Feedback/information etc.) that could lead to UCAs associated with different stakeholders (eVTOL Operator, Regulator, Air Navigation Service provider (NATS) and Licensed Aerodrome), is presented in Table 7.

The entire list of loss scenarios describing the Causal Factors that can lead to the UCAs (grouped by stakeholder) and the corresponding Mitigations proposed to prevent or mitigate these Causal Factors, can be found in **Appendix A**: Deliverables.

UCA Description	CF(s)	Mitigations
eVTOL Operator provides 'Aircraft Release To Service' for aircraft despatch incorrectly when adequate checks on the aircraft have not been carried out, this has not been detected, and the eVTOL aircraft flies	eVTOL Operator is unable to correctly provide Aircraft Release To Service (although it should) due to the degradation of the internal process over time (e.g., overloaded tasks, flawed process).	Performance review of the relevant team issuing Aircraft Release To Service within the eVTOL Operator shall be conducted periodically to ensure that the team operates properly and safely.
Regulator does not issue 'vertiport / aerodrome licence'' when the vertiport is actively being used for flight operations. Note: this would affect the flight operations schedule, leading to business-critical losses.	The supplementary documents (compliance with regulatory standards, safety management systems, training and competency of personnel, operational readiness, data integrity and cybersecurity, environmental compliance etc.) was incomplete although the licensed vertiport met the criteria to be granted vertiport / aerodrome licence approval. As a result, the licence approval was not granted.	Licensed Vertiport shall ensure that the provided supplementary documents for vertiport / aerodrome licence application are complete and up to date.
NATS (LHR RADAR) provides 'Onward Clearance' incorrectly (incorrect height, routing) when there is a conflict (proximity to other eVTOLs, helicopters and traditional aircraft)	There is an aircraft which has deviated from its flight plan and both NATS and the eVTOL Crew are unaware	ANSPs should implement mechanisms to detect and alert controllers/service providers to deviations in aircraft performance (e.g., altitude, speed, trajectory) from expected parameters.
Licensed Aerodrome (Silverstone Aerodrome) provides 'Hold outside RA(T)'	The Feedback about the current state of airspace congestion is delayed.	Licensed Aerodrome (Silverstone Aerodrome) shall conduct automated self-checks of

UCA Description	CF(s)	Mitigations
too late when airspace congestion has already built up.		feedback systems every x sec (to be confirmed).

Table 7 An extract from the STPA Step-4 Results

Based on the application of the concept for the prioritisation of Mitigations, a Mitigation prioritisation matrix was created. The Mitigations were prioritised after grouping them according to stakeholders. A snapshot of the Mitigation Prioritisation Matrix showing a subset of the prioritised Mitigations is presented in Figure 11. Based on the prioritisation concept, a Mitigation assigned type A, requiring minor effort, low cost for implementation and Likelihood of Occurrence- 1, would be ranked highest (ReqP1). The Mitigation **UCA(Ph0.1)-16.2.1-RQ1** was placed in the dark-red area (ReqP1) of the Mitigation Prioritisation Matrix as it was assigned Type - A, Moderate effort (Time), Medium cost for implementation and Likelihood of Occurrence-1(not mitigated by existing regulations). Additionally, this Mitigation was also assigned the highest CIF rating and a PMS score of 20, as the UCA linked to this Mitigation could lead to catastrophic losses, justifying its position in the Mitigation Prioritisation Matrix. The Mitigation **UCA(Ph0.1)-25.4.1-RQ1** was allocated to the green area (ReqP5) of the Mitigation Prioritisation Matrix, primarily due to its type D classification, and because this Mitigation is already covered by existing regulations.

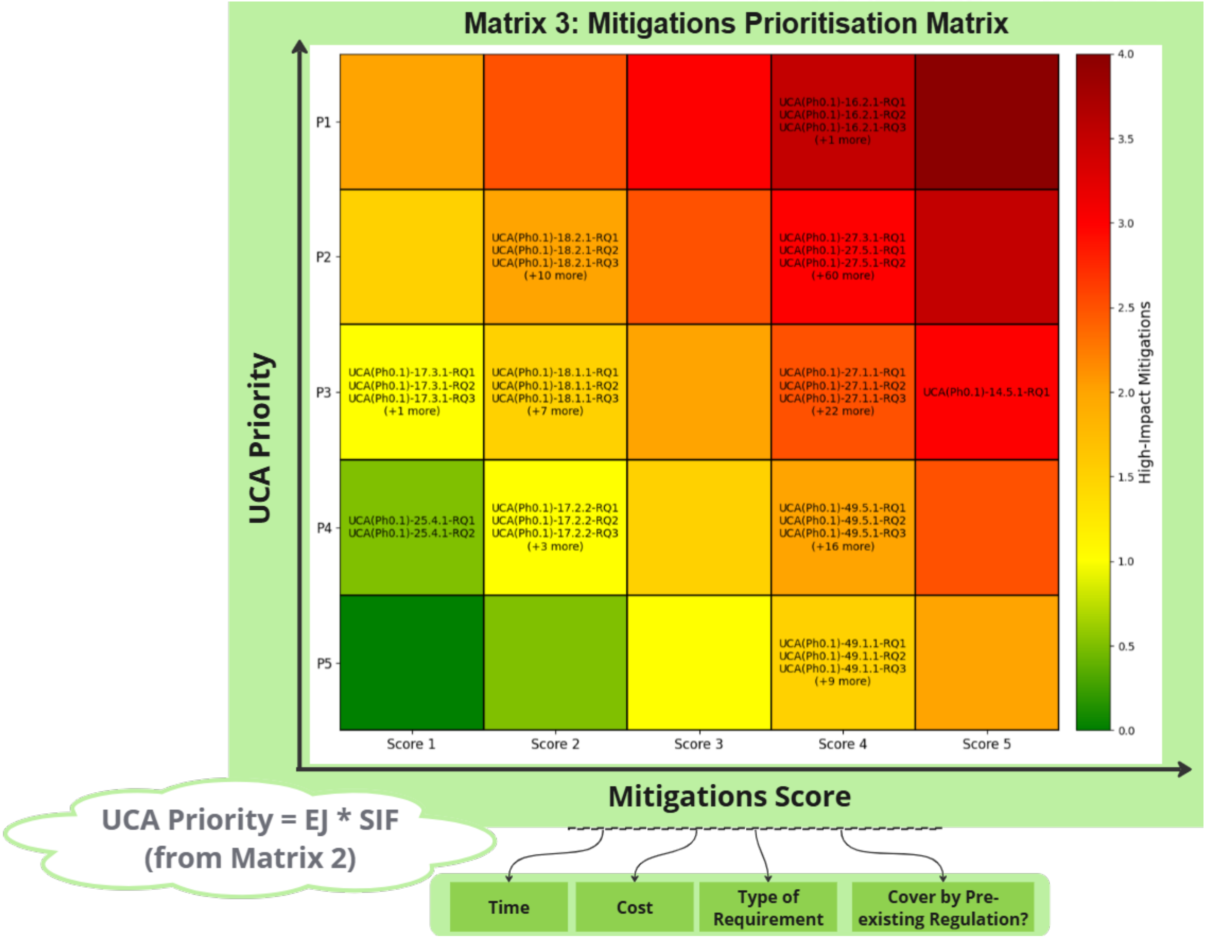

Figure 11 A snapshot of Mitigation Prioritisation Matrix

It is to be noted that some of the Mitigations which were assigned P3 and P4 were also marked as high priority Mitigations to ensure that there was a broad range of Mitigations pertaining to multiple stakeholders for the next phase of the analysis (Gap analysis).

The entire list of high-priority Mitigations corresponding to the different stakeholders can be found in **Appendix A**: Deliverables, and a sub-set of this is presented in Table 8.

Req ID	Mitigations	Priority	SIF	EJ Score	Mitigation Score
UCA(Ph0.1)-13.5.2-RQ1	**Aerodrome / Vertiport** shall actively seek for confirmation of receiving the supplementary documents after they have been sent to the regulator.	ReqP1	160	6.945803	0.95

Req ID	Mitigations	Priority	SIF	EJ Score	Mitigation Score
UCA(Ph0.1)-50.2.1-RQ7	Performance review of the relevant team issuing ‘Aircraft Release to service’ within **eVTOL Operator** shall be conducted periodically to ensure that the team operates properly and safely.	ReqP1	40	29.86514	0.63
UCA(Ph1)-21.1.1-RQ2	**ANSPs** should ensure access to accurate and timely meteorological data to support operational decision-making and flight safety.	ReqP3	140	208.3412	0.69
UCA(Ph2)-7.5.3-RQ.1	**Aerodrome control systems** shall deploy robust communication protocols.	ReqP1	60	30.03034	0.68

Table 8 Snapshot of high-priority Mitigations corresponding to the different stakeholders

Gap Analysis

It is assumed that most of the existing aviation regulations will also apply to eVTOL operations. However, to evidence this assumption, an analysis of the identified eVTOL Mitigations was undertaken against existing aviation regulations. **The term 'Gap' was used to denote a mitigation proposed by STPA that is not covered by the existing regulations, policies, or procedures related to Helicopters and/or eVTOLs.** This section discusses the results of the Gap analysis.

After the completion of STPA Step-4, the list of unique high priority-Mitigations corresponding to various stakeholders were carefully evaluated by the Subject matter experts to identify whether these Mitigations were 'Gaps' in the existing regulations, policies, or procedures for Helicopters and/or eVTOLs.

As shown in Table 9, there were **56 'gaps' identified in total**. The STPA methodology played an important role in identifying potential safety and regulatory gaps by analysing interactions within the system, based on the control structures.

Stakeholder	Unique highest-priority Mitigations	Mitigations identified as Gaps
Regulator (CAA)	57	17
Vertiport Operator	36	29
eVTOL Operator	15	2
Air Traffic Service Provider (NATS)	16	8
Total	**124**	**56**

Table 9 Statistics of Gaps linked to various Stakeholders

The tables below provide an overview of the gaps associated with each stakeholder. A detailed Gap analysis document showing whether each of these gaps apply only to eVTOLs or both Helicopters and eVTOLs can be found in **Appendix A**: Deliverables. The findings from this analysis will serve as a foundation for future improvements, helping to refine the regulatory framework and policies to ensure they remain comprehensive, effective, and cater to the evolving aviation ecosystem.

Note: The Mitigations with their ID (Mitigation ID) in **bold** text in the tables below are referenced in the section – **Discussion on identified regulatory gaps for eVTOL Operations**

Regulator (CAA):

Table 10 lists the Mitigations identified as gaps, linked to the Regulator (CAA).

Mitigation ID	Mitigations	Recommendation Type
UCA(Ph0.1)-28.1.1-RQ6	Performance review of the relevant team issuing vertiport / aerodrome licence approval within Regulator shall be conducted periodically to ensure that the team operates properly and safely.	Procedures
UCA(Ph0.1)-28.2.1-RQ1		Procedures
UCA(Ph0.1)-16.1.1-RQ3	Performance review of the relevant team issuing NOTAM within Regulator shall be conducted periodically to ensure that the team operates properly and safely.	Procedures
UCA(Ph0.1)-15.2.2-RQ5	Performance review of the relevant team issuing Temporary Aerodrome Creation (TAC) within Regulator shall be conducted periodically to ensure that the team operates properly and safely.	Procedures
UCA(Ph0.1)-28.1.1-RQ7	Review of the vertiport / aerodrome licence approval process within the Regulator shall be conducted periodically to ensure safe operation.	Procedures
UCA(Ph0.1)-16.1.1-RQ4	Process review of the relevant team issuing NOTAM within Regulator shall be conducted periodically to ensure that the team operates properly and safely.	Procedures
UCA(Ph0.1)-15.2.2-RQ6	Process review of the relevant team issuing TAC within Regulator shall be conducted periodically to ensure that the team operates properly and safely.	Procedures
UCA(Ph0.1)-28.5.1-RQ2	Regulator shall actively seek for confirmation of receiving the vertiport / aerodrome licence approval after they have been sent to the Vertiport.	Procedures

Mitigation ID	Mitigations	Recommendation Type
UCA(Ph0.1)-24.2.1-RQ1	The regulator shall be properly trained to review the supplementary documents correctly (regarding categorisation (CAT/NCC/NCO/SPO)).	Procedures
UCA(Ph0.1)-15.2.2-RQ1	Regulator shall be properly trained to be able to correctly review the supplementary documents (TAC (Temp Aerodrome Creation) (e.g., incorrect location, incorrect zone)).	Procedures
UCA(Ph0.1)-15.4.2-RQ3	Regulator shall be properly trained to be able to correctly review the supplementary documents [TAC (Temp Aerodrome Creation)), (e.g. is expired and undetected)].	Procedures
UCA(Ph0.1)-17.1.2-RQ2	Regulator shall be properly trained to be able to correctly review the supplementary documents [Supp. Doc for safety certification].	Procedures
UCA(Ph0.1)-28.1.1-RQ2	Regulator shall be properly trained to be able to correctly review the supplementary documents [Supp. Doc for vertiport / aerodrome licence approval review].	Procedures
UCA(Ph0.1)-17.1.2-RQ1	Regulator shall proactively internally review the correctness of the supplementary documents [Supp. Doc for safety certification] to ensure that it captures the correct information (For example, a misinterpretation that the safety standards have not been met, even though they have been fully complied with).	Procedures

Mitigation ID	Mitigations	Recommendation Type
UCA(Ph0.1)-24.2.1-RQ3	The assessment criteria for Categorisation (CAT/NCC/NCO/SPO) shall be clearly presented to the applicant and shall be consistent both internally within the Regulator and externally with the applicant.	Procedures
UCA(Ph0.1)-16.2.1-RQ2	The communication between Regulator and Licensed Aerodrome shall be efficient, clear, and accurate to ensure that the NOTAM is correctly communicated.	Procedures
UCA(Ph0.1)-14.5.1-RQ3	The tasks related to processing the Temporary Airspace Structure within the Regulator should undergo routine review and be re-prioritised as necessary to guarantee that safety-critical tasks are prioritised above all others.	Procedures
UCA(Ph0.1)-16.5.1-RQ3	The tasks (creation of the NOTAM) within Regulator shall be periodically reviewed and re-prioritised as necessary to guarantee that safety-critical tasks are prioritised above all others.	Procedures

Table 10 Gaps related to Regulator (CAA)

Air Navigation Service Provider (NATS):

Table 11 outlines the gaps associated with the Air Navigation Service Provider, specified as NATS in this study. **It should be noted that these mitigations are widely applicable to all Air Navigation Service Providers and are not exclusively relevant to NATS.**

Mitigation ID	Mitigations	Recommendation Type
UCA(Ph1)-2.1.1-RQ1	ANSPs should ensure that requests for Air Traffic and Flight Information Services from vertiports or other relevant stakeholders are received and responded to in a timely and consistent manner, particularly in uncontrolled airspace.	Procedures
UCA(Ph1)-2.1.1-RQ3		
UCA(Ph1)-18.2.1-RQ1	ANSPs should ensure that surveillance systems are capable of monitoring aircraft performance parameters (e.g., position, heading, speed) to support safe integration, separation and enhanced situational awareness.	Procedures
UCA(Ph1)-18.2.1-RQ7	Procedures should be in place requiring flight crews to notify the relevant ANSP of any deviations from the cleared or planned flight path.	Procedures
UCA(Ph1)-18.2.1-RQ9	ANSPs should implement mechanisms to detect and alert controllers/service providers to deviations in aircraft performance (e.g., altitude, speed, trajectory) from expected parameters.	Procedures
UCA(Ph1)-18.5.1-RQ2	ANSPs should ensure that communication channels with aircraft, including eVTOLs, meet latency and reliability standards appropriate for the operational environment.	Procedures
UCA(Ph1)-21.1.1-RQ2	ANSPs should ensure access to accurate and timely meteorological data to support operational decision-making and flight safety.	Procedures
UCA(Ph1)-22.1.1-RQ3	ANSPs should maintain sufficient numbers of trained and licensed personnel to manage air traffic services and respond to operational demands.	Procedures

Mitigation ID	Mitigations	Recommendation Type
UCA(Ph1)-22.5.1-RQ2	ANSPs should ensure that the recording of flight data, flight plan amendments and clearances are processed and managed in a timely and coordinated manner across relevant sectors.	Procedures

Table 11 Gaps related to Air Navigation Service Provider (NATS)

eVTOL Operator:

Table 12 lists the Mitigations identified as gaps, linked to the eVTOL Operator.

Mitigation ID	Mitigations	Recommendation Type
UCA(Ph0.1)-50.2.1-RQ7	Performance review of the relevant team issuing ‘Aircraft Release to Service’ within the eVTOL Operator shall be conducted periodically to ensure that the team operates properly and safely.	Regulations
UCA(Ph0.1)-50.2.1-RQ8	Process review of the relevant team issuing ‘Aircraft Release to service’ within the eVTOL Operator shall be conducted periodically to ensure that the team operates properly and safely.	Regulations

Table 12 Gaps related to eVTOL Operator

Vertiport Operator:

Table 13 lists the Mitigations identified as gaps, linked to Licensed Vertiports/ Aerodromes.

Mitigation ID	Mitigations	Recommendation Type
UCA(Ph2)-7.1.3-RQ.2	Aerodrome control systems shall incorporate high-resolution airspace monitoring tools to identify critical hotspots.	Procedures
UCA(Ph2)-7.5.2-RQ.4	Aerodrome control systems shall optimise algorithms to assign squawk codes within *to be defined* second of receiving relevant information.	Procedures
UCA(Ph2)-6.1.1-RQ.5	Feedback (to 'Hold outside RA(T)) [Licensed Aerodrome to eVTOL] regarding capacity status shall utilise multiple channels to ensure redundancy in communication pathways.	Regulation
UCA(Ph2)-6.3.1-RQ.5		Regulation
UCA(Ph3)-13.5.1-RQ.1	Ground services must use advanced real-time sensors to ensure provision of continuous Feedback on landing conditions.	Regulation
UCA(Ph2)-6.2.2-RQ.6	Implement conflict detection algorithms to identify discrepancies between manual and automated Feedback concerning 'Hold outside RA(T) (acknowledgement to Hold outside RA(T) command)	Regulation
UCA(Ph2)-6.5.1-RQ.2	Licensed Aerodrome (Silverstone Aerodrome) shall conduct automated self-checks of Feedback about Hold outside RA(T) Ack' systems every *to be defined* sec.	Procedures
UCA(Ph2)-6.5.1-RQ.1	Licensed Aerodrome (Silverstone Aerodrome) shall deploy systems capable of managing the airspace density.	Procedures
UCA(Ph2)-6.1.1-RQ.3	Licensed Aerodrome (Silverstone Aerodrome) shall dynamically update and reflect the accurate capacity status.	Procedures

Mitigation ID	Mitigations	Recommendation Type
UCA(Ph2)-6.1.1-RQ.8	Licensed Aerodrome (Silverstone Aerodrome) shall employ fail-safe communication protocols to ensure the receipt of Hold outside RA(T) acknowledgements.	Procedures
UCA(Ph2)-6.1.1-RQ.6	Licensed Aerodrome (Silverstone Aerodrome) shall establish alerts for any missing or delayed Feedback on Hold outside RA(T) acknowledgements.	Procedures
UCA(Ph2)-6.1.1-RQ.7	Licensed Aerodrome (Silverstone Aerodrome) shall establish communication diagnostic tools to detect errors or interruptions in the reception of Hold outside RA(T) acknowledgements.	Procedures
UCA(Ph2)-6.5.1-RQ.4		Procedures
UCA(Ph2)-6.3.1-RQ.7		Procedures
UCA(Ph2)-6.1.1-RQ.2	Licensed Aerodrome (Silverstone Aerodrome) shall include an algorithm that verifies whether the capacity is exceeded when providing holding instructions.	Procedures
UCA(Ph2)-6.1.1-RQ.1	Licensed Aerodrome (Silverstone Aerodrome) shall include automated monitoring tools that provide holding instructions whenever capacity is exceeded.	Procedures
UCA(Ph2)-6.2.1-RQ.1	Licensed Aerodrome shall incorporate advanced decision-making tools to dynamically update the holding instructions based on severe weather data.	Procedures
UCA(Ph2)-6.2.1-RQ.2	Licensed Aerodrome shall utilise simulations to test the algorithm's efficiency under severe weather conditions to dynamically update the holding instructions.	Procedures
UCA(Ph2)-6.3.1-RQ.3	Licensed Aerodrome shall utilise simulations to test the algorithm's efficiency to avoid unnecessary holding instructions.	Procedures
UCA(Ph2)-6.2.2-RQ.4	Licensed Aerodrome shall implement alerts like amber lights when detecting missing Feedback updating airspace capacity.	Procedures

Mitigation ID	Mitigations	Recommendation Type
UCA(Ph2)-6.2.2-RQ.5	Licensed Aerodrome shall implement automated systems that periodically validate Feedback loop between eVTOL and the aerodrome about airspace capacity.	Procedures
UCA(Ph2)-6.2.2-RQ.3	Licensed Aerodrome shall include Feedback loops to confirm successful execution of commands of holding instructions when the holding area limits its capacity to accommodate additional aircraft due to emergency situations.	Procedures
UCA(Ph2)-7.5.1-RQ.3	Licensed Aerodrome shall measure sensor processing times, to provide RF/Transponder Setting(squawk), to identify inefficiencies.	Procedures
UCA(Ph0.2)-33.7.2-RQ3	Local Authority shall ensure that the proposed Land Approval is properly communicated with Temporary Aerodrome Management.	Unclassified by SME
UCA(Ph0.2)-33.7.2-RQ6	Local Authority shall ensure that the proposed 'No of Movement & Op Hours' are properly communicated with Temporary Aerodrome Management.	Policy
UCA(Ph0.2)-33.7.2-RQ4	Local Authority shall ensure that the provided 'No of Movement & Op Hours' are complete and up to date.	Policy
UCA(Ph0.1)-13.2.2-RQ1	Licensed Aerodrome/Vertiport shall proactively pursue Regulator for Approval if not heard from the Regulator.	Procedure
UCA(Ph0.1)-13.2.2-RQ3	Licensed Aerodrome/Vertiport shall proactively internally review the correctness of the supplementary documents (i.e., the content was not reflecting the actual event) to ensure that it captures the correct information.	Procedure
UCA(Ph0.1)-14.2.1-RQ2	Licensed Aerodrome/Vertiport shall proactively internally review the correctness of the supplementary documents to ensure that it captures the correct information.	Procedure
UCA(Ph0.1)-28.5.1-RQ1	Licensed Vertiport shall actively seek for confirmation of receiving the supplementary documents (compliance with regulatory standards, safety management systems, training and competency of personnel, operational readiness, data integrity and cybersecurity, environmental compliance etc.) after they have been sent to the regulator.	Procedure

Mitigation ID	Mitigations	Recommendation Type
UCA(Ph0.1)-15.2.2-RQ4	The communication between Licensed Aerodrome and Regulator shall be clear, efficient, and accurate to ensure that the supplementary document for TAC application is correctly communicated.	Procedure
UCA(Ph0.1)-14.5.1-RQ5	The process for the creation of supplementary documents for Temporary Airspace Structure within [Licensed Vertiport] / [Licensed Aerodrome] shall be periodically reviewed and prioritised to ensure that the application is submitted promptly (based on the closing date)	Procedures
UCA(Ph0.1)-15.5.1-RQ5	The process for the creation of supplementary documents for TAC (Temp Aerodrome Creation) within [Licensed Vertiport] / [Licensed Aerodrome] shall be periodically reviewed and prioritised to ensure that the application is submitted promptly (based on the closing date)	Procedures

Table 13 Gaps related to Vertiport Operator

Discussion on identified regulatory gaps for eVTOL Operations

Out of these 56 gaps for eVTOL operations (not addressed by current aviation regulations), **27 were identified to be applicable to both eVTOL and current helicopter operations** (Table 14). Thus, making the latter a prioritised area of focus for the CAA to address to ensure safety of current helicopter operations.

Stakeholder	**Number of Mitigations NOT addressed by current aviation regulations (Gaps)**	**Number of Mitigations NOT addressed with current aviation regulations (Gaps) which are applicable to both eVTOL & current helicopter operations**
Regulator (CAA)	17	11
Air Navigation Service provider (NATS)	8	8
eVTOL Operator	2	
Vertiport operator (also considering them as heliport operator)	29	8

Table 14 Summary of Gaps

In this section, we discuss the individual gaps for each of the stakeholders and indicate potential approaches to address these gaps.

Gap Analysis- Regulator (CAA)

From the analysis of the Mitigations related to the Regulator (as illustrated in Table 10), we identified 17 unique Mitigations which are not covered by existing regulations. Based on the analysis of these gap Mitigations with the project stakeholders, a list of procedural implementations was identified to address these Mitigations:

- *Performance and process review*

There is a need to enforce regular performance review and process review within the Regulator to optimise the efficiency of each department. Whilst there have been regular performance and process reviews carried out in most of the departments, from the analysis, we identified three departments that need inclusion of the performance review. These include the teams responsible for:

- ***Vertiport / Aerodrome Licence Approval:***
    - **UCA(Ph0.1)-28.1.1-RQ6 / UCA(Ph0.1)-28.2.1-RQ1:** Performance review of the relevant team issuing vertiport / aerodrome licence approval within Regulator shall be conducted periodically to ensure that the team operates properly and safely.
    - **UCA(Ph0.1)-28.1.1-RQ7:** Review of the vertiport / aerodrome licence approval process within the Regulator shall be conducted periodically to ensure safe operation.
- ***NOTAM:***
    - **UCA(Ph0.1)-16.1.1-RQ3:** Performance review of the relevant team issuing NOTAM within Regulator shall be conducted periodically to ensure that the team operates properly and safely.
    - **UCA(Ph0.1)-16.1.1-RQ4:** Process review of the relevant team issuing NOTAM within Regulator shall be conducted periodically to ensure that the team operates properly and safely.
    - **UCA(Ph0.1)-16.5.1-RQ3):** The tasks (creation of the NOTAM) within Regulator shall be periodically reviewed and re-prioritised as necessary to guarantee that safety-critical tasks are prioritised above all others.
- ***Temporary Aerodrome Creation (TAC):***
    - **UCA(Ph0.1)-15.2.2-RQ5:** Performance review of the relevant team issuing TAC within Regulator shall be conducted periodically to ensure that the team operates properly and safely.
    - **UCA(Ph0.1)-15.2.2-RQ6:** Process review of the relevant team issuing TAC within Regulator shall be conducted periodically to ensure that the team operates properly and safely.

- ***Temporary Airspace Structure:***
- **UCA(Ph0.1)-14.5.1-RQ3:** The tasks related to processing the Temporary Airspace Structure within the Regulator should undergo routine review and be re-prioritised as necessary to guarantee that safety-critical tasks are prioritised above all others.
- ***Aircraft Certification:***

- **UCA(Ph0.1)-17.1.2-RQ1:** Regulator shall proactively internally review the correctness of the supplementary documents [Supp. Doc for safety certification] to ensure that it captures the correct information (For example, a misinterpretation that the safety standards have not been met, even though they have been fully complied with).

In line with the "just-culture" approach, it is important to note here that the reason for enforcing the performance review is not to identify and blame any underperforming department or individual within the Regulator. Instead, the performance review of the individuals who are part of the whole system (e.g., the Regulator for the eVTOL Operation), systematically helps identify any possible causes of underperformance, and provide required support to enhance efficiency. Creating a blame-free working culture has always been one of the primary goals of STPA.

- *Acknowledgement and confirmation*

There is also a need to include acknowledgement as part of the Mitigations. Based on STPA, we identified the missing acknowledgement between Aerodrome and Regulator during various application and approval processes. This includes:

- ***Missing confirmation from Licensed Aerodrome of the received eVTOL approval:***
  - **UCA(Ph0.1)-13.2.2-RQ1:** Licensed Aerodrome/Vertiport shall proactively pursue Regulator for Approval if not heard from the Regulator.
- ***Acknowledgements between Regulator and Licensed Vertiport:***
  - **UCA(Ph0.1)-28.5.1-RQ1:** Licensed Vertiport shall actively seek for confirmation of receiving the supplementary documents (compliance with regulatory standards, safety management systems, training and competency of personnel, operational readiness, data integrity and cybersecurity, environmental compliance etc.) after they have been sent to the regulator.

The confirmation would allow the Regulator to double-check the correctness of the issued approval.

- *Training*

There is also a need to improve the training process within the Regulator. As part of the regulatory preparation for the eVTOL operation, there are many types of supplementary documents that need to be reviewed by the Regulator. Considering eVTOL as a new domain, relevant departments need to be re-trained to ensure that they are capable of review of the supplementary documents. This includes:

- ***Supplementary documents for applications of TAC:***

        - **UCA(Ph0.1)-15.2.2-RQ1:** Regulator shall be properly trained to be able to correctly review the supplementary documents (TAC (Temp Aerodrome Creation) (e.g., incorrect location, incorrect zone)).
        - **UCA(Ph0.1)-15.4.2-RQ3:** Regulator shall be properly trained to be able to correctly review the supplementary documents [TAC (Temp Aerodrome Creation)), (e.g. is expired and undetected)].
    - ***eVTOL aircraft certification:***
        - **UCA(Ph0.1)-17.1.2-RQ2:** Regulator shall be properly trained to be able to correctly review the supplementary documents [Supp. Doc for safety certification].
    - ***Vertiport / Aerodrome Licence Approval:***
        - **UCA(Ph0.1)-28.1.1-RQ2:** Regulator shall be properly trained to be able to correctly review the supplementary documents [Supp. Doc for vertiport / aerodrome licence approval review].
    - ***Aircraft categorisation:***
        - **UCA(Ph0.1)-24.2.1-RQ1:** The assessment criteria for Categorisation (CAT/NCC/NCO/SPO) shall be clearly presented to the applicant and shall be consistent both internally within the Regulator and externally with the applicant.

- *Communication*

The analysis also highlighted a need to improve the communications between Licensed Aerodrome and Regulator when managing different applications especially when handling the applications for:

    - ***TAC:***
        - **UCA(Ph0.1)-15.2.2-RQ4:** The communication between Licensed Aerodrome and Regulator shall be clear, efficient, and accurate to ensure that the supplementary document for TAC application is correctly communicated.
    - ***NOTAM:***
        - **UCA(Ph0.1)-16.2.1-RQ2:** The communication between Regulator and Licensed Aerodrome shall be efficient, clear, and accurate to ensure that the NOTAM is correctly communicated.

These would require enforcement of the digital form-fill system to improve the process for the application, to minimise errors.

- *Assessment Criteria*

There is also a need to ensure that the assessment criteria for the aircraft categorisation are clearly presented to the applicant:

- **UCA(Ph0.1)-24.2.1-RQ3:** The assessment criteria for Categorisation (CAT/NCC/NCO/SPO) shall be clearly presented to the applicant and shall be consistent both internally within the Regulator and externally with the applicant.

As suggested by the stakeholders, there have been existing processes for this, in the aviation domain. During the review process, the first person from the regulator initially reviews and assigns permission. Then the second person, who directly engages with the applicant identifies what the applicant wishes to do within the airspace. Same process can be tailored for the eVTOL application.

Gap Analysis- Air Navigation Service Provider (NATS)

Out of the 16 unique high-priority ANSP(NATS) Mitigations, 8 were identified "gaps" with existing regulation and classified as procedural deficiencies (Table 11) impacting both the Helicopter and eVTOL Operations. These gaps are allocated to:

- ***Air traffic Service (ATS) surveillance systems:***
    - **UCA(Ph1)-18.2.1-RQ1:** ANSPs should ensure that surveillance systems are capable of monitoring aircraft performance parameters (e.g., position, heading, speed) to support safe integration, separation and enhanced situational awareness.
- ***Trajectory Modelling Systems:***
    - **UCA(Ph1)-18.2.1-RQ9:** ANSPs should implement mechanisms to detect and alert controllers/service providers to deviations in aircraft performance (e.g., altitude, speed, trajectory) from expected parameters.
- ***Air Traffic Controllers:***
    - **UCA(Ph1)-22.5.1-RQ2:** ANSPs should ensure that the recording of flight data, flight plan amendments and clearances are processed and managed in a timely and coordinated manner across relevant sectors.
- ***Pilots:***
    - **UCA(Ph1)-18.2.1-RQ7:** Procedures should be in place requiring flight crews to notify the relevant ANSP of any deviations from the cleared or planned flight path.
- ***Weather Monitoring and Prediction Systems:***

- **UCA(Ph1)-21.1.1-RQ2**: ANSPs should ensure access to accurate and timely meteorological data to support operational decision-making and flight safety.

Some of these gaps e.g., **UCA(Ph1)-18.2.1-RQ7**, could be addressed by revising future pilot procedural Mitigations in class G airspace. Mitigations have also been defined to ensure appropriate coordination between these components (e.g., **UCA(Ph1)-18.2.1-RQ7**, **UCA(Ph1)-22.5.1-RQ2**). The gap review highlighted the need to update the NERL license function processes for proper training of Air Traffic Controllers to ensure coordination both within and across sectors and for issuing clearances relative to other clearances in a timely manner (e.g., **UCA(Ph1)-22.5.1-RQ2**).

Gap Analysis- eVTOL Operator

From the analysis of the Mitigations related to the eVTOL Operator (Table 12), 2 unique Mitigations were identified which are not covered by pre-existing eVTOL regulations:

- **UCA(Ph0.1)-50.2.1-RQ7:** Performance review of the relevant team issuing ‘Aircraft Release to Service’ within the eVTOL Operator shall be conducted periodically to ensure that the team operates properly and safely.
- **UCA(Ph0.1)-50.2.1-RQ8:** Process review of the relevant team issuing ‘Aircraft Release to Service’ within the eVTOL Operator shall be conducted periodically to ensure that the team operates properly and safely.

Both Mitigations were needed to enforce the performance and process review of the relevant team responsible for issuing the Aircraft Release to Service. This would ensure that the aircraft release to service for the eVTOL despatch is issued on time and ensure the safe operation of eVTOL.

Gap Analysis- Vertiport Operator

In the vertiport Mitigations gap review (Table 13), 29 unique Mitigations were identified based on the STPA application. Of these, 8 Mitigations are common gaps that apply to both helicopter and eVTOL operations which implies that these issues must be addressed in the procedures and regulations for both platforms.

A detailed analysis of these Mitigations has led to various aviation recommendations:

- *Collision Management*

There is a need to manage airborne conflict risk along designated flight paths. To achieve this, the air traffic management system should incorporate high-resolution airspace monitoring tools that can identify critical hotspots.

- *Energy Management*

Considerations for energy management should be included. This can be mitigated by implementing advanced real-time sensors that provide continuous Feedback on landing conditions, as described in:

- **UCA(Ph3)-13.5.1-RQ1:** Ground services must use advanced real-time sensors to ensure provision of continuous Feedback on landing conditions.

- *Data Link Monitoring*

A gap was identified in both the helicopter and eVTOL procedures for managing data link issues, such as missing or delayed Feedback. An alert system should be implemented to address these issues:

- **UCA(Ph2)- 6.1.1-RQ6:** Licensed Aerodrome (Silverstone Aerodrome) shall establish alerts for any missing or delayed Feedback on 'Hold outside RA(T)' acknowledgements.

- *Diagnostic Tools*

It is essential to integrate diagnostic tools within eVTOL procedures to detect errors or interruptions:

- **UCA(Ph2)- 6.1.1-RQ7:** Licensed Aerodrome (Silverstone Aerodrome) shall establish communication diagnostic tools to detect errors or interruptions in the reception of 'Hold outside RA(T)' acknowledgements.

- *Automation and Simulation*

There is a notable gap regarding the lack of automation in predicting flight paths currently as this process is currently done manually. It is recommended to use simulation tools to test algorithm efficiency and to implement automated systems that periodically validate the feedback loop:

- **UCA(Ph2)- 6.3.1-RQ3:** Licensed Aerodrome shall utilise simulations to test algorithm efficiency to avoid unnecessary holding instructions.

- *Process Improvement*

There is a need to improve the process not only within the Regulator (as an organisation), but also within the Licensed Vertiports / Licensed Aerodromes to prioritise the tasks related to the preparation of the supplementary documents for:

- ***Temporary Aerodrome Creation:***

  - **UCA(Ph0.1)-15.5.1-RQ5:** The process for the creation of supplementary documents for TAC (Temp Aerodrome Creation) within [Licensed Vertiport] / [Licensed Aerodrome] shall be periodically reviewed and prioritised to ensure that the application is submitted promptly (based on the closing date).

- ***Temporary Airspace Structure:***
  - **UCA(Ph0.1)-14.5.1-RQ5:** The process for the creation of supplementary documents for TAS (Temp Airspace Structure) within [Licensed Vertiport] / [Licensed Aerodrome] shall be periodically reviewed and prioritised to ensure that the application is submitted promptly (based on the closing date).
  - **UCA(Ph0.1)-14.2.1-RQ2:** Licensed Aerodrome/Vertiport shall proactively internally review the correctness of the supplementary documents to ensure that it captures the correct information.

Conclusion

The current air navigation system, including airspace structures and Air traffic management procedures, is based on a mature regulatory framework and ruleset. The UK Airspace Modernisation Strategy is focused on integration rather than segregation of different airspace user groups, to facilitate greater capacity and enable aerospace innovation.

Integrating a novel technology like eVTOL into the existing airspace will create emergent behaviours. The existing airspace design and regulations may not be designed to safely react to such emergent behaviours. Thus, posing risk to eVTOL operations and their sharing of the airspace with existing airspace users. With OEMs forecasting eVTOL operations in the near term (2-3 years), there is an urgent need for both identifying and assessing the risk posed by such emergent behaviours.

Traditional hazard analysis and risk management techniques, most of which were created decades ago for the less complex and linear systems of that time, cannot effectively handle the complex systems with multi-stakeholder interactions being developed today. More powerful and a systems thinking based approach to hazard analysis is needed. Systems-Theoretic Process Analysis (STPA) is a relatively new type of hazard analysis technique based on a very different type of paradigm and assumptions about the causes of accidents.

In contrast to traditional safety analysis approaches which focus on component faults and failures driving by reliability assessments, STPA focusses on non-linear, indirect, and feedback relationships among events and actors.

In this project, safety analysis using STPA was conducted for eVTOL operation, identifying loss scenarios, causal factors, unsafe control actions and their corresponding Mitigations to prevent or mitigate them. Many of the scenarios identified in this report include more than just component failures. Therefore, many of the Mitigations identified by the STPA analysis go beyond reliability and relate to the behaviour of system components (both human controllers and automation) and the information that those components receive and exchange. The initial STPA output yielded 434 Mitigations.

Additionally, a novel severity, control impact and expert judgement-based prioritisation method was developed to rank the Mitigations. The resulting output yielded 124 prioritised Mitigations

Comparing the 124 Mitigations with existing aviation regulations, 56 Mitigations were identified as “gaps”, i.e., they were not addressed by current aviation regulations. Out of these 56 gaps, 27 were identified to be impacting both future eVTOL operations and current helicopter operations, making it crucial to address them.

As the next step, the Mitigations which have been identified as gaps by the STPA for eVTOL analysis need to be developed into practical, implementable actions for each relevant stakeholder in the form of regulatory and policy updates, operational instructions, and practical guidance.

Finally, this project has demonstrated that STPA is capable of effectively analysing the advanced features of the next generation aviation technologies and the complexity of the proposed operational improvements. The findings from this project demonstrate that STPA offers a thorough framework to identify shortcomings in existing regulations, policies, and procedures. This approach helps to establish a robust safety management system that proactively addresses risks and evolves in response to the challenges posed by new technologies.

Annexes

Annex A: Overview of various safety analysis approaches including STPA

In today's complex world, it's crucial to make sure systems are both safe and secure. With technology always changing, we need to understand hazards, assess risks, and find ways to make the system safe, secure, and resilient. The imperative to ensure the safety and security of complex systems has become increasingly prominent in various domains, ranging from aviation and healthcare to information technology, smart cities, nuclear power plants to any kind of industry. Safety is a system property simply understood as the lack of accidents, where every industry, company, or enterprise can have specific definitions for what constitutes an accident. According to (Defense, 10 Feb 2000), safety can be defined as "freedom from those conditions that can cause death, injury, occupational illness, damage to or loss of equipment or property, or damage to the environment. An accident is an undesired or unplanned event that causes loss, damage, or injury.

After an accident occurs, accident analysis, especially the analysis of the cause of the accident, is critical for taking effective preventive measures. Accident analysis relies on accident models which are a simplified description of reality. The effective use of accident models can better investigate and analyse accidents and prevent them. Accident models are also the basis for risk analysis and technical assessment. Over time, the ever-changing nature of accidents promotes the evolution of accident models from finding a single direct cause to identifying the system cause. Thus far, two of the most used accident models are: linear chain-of-failure events models and systems accident models.

To remain effective, accident models must adapt to emergent technologies, by integrating various factors, including human, organisational, and environmental, to effectively assess risks, identify novel interactions between stakeholders, and mitigate potential unsafe interactions within systems. These factors could have been overlooked and can be traced back to the existing regulatory gaps.

Traditional Approach to Safety Analysis

The linear chain-of-failure events model is the most basic type of accident model. Historically, complexity has been managed by dividing systems into smaller parts, analysing each part separately, and then combining the findings to understand how the overall system behaves. This traditional method assumes that the physical or functional components interact in direct and predictable ways. For example, an aircraft's functional elements might include propulsion, navigation, attitude control, braking, and cabin environment systems. Similarly, the aircraft can be broken down into physical parts like the fuselage, engines, wings, stabilizers, and nozzles. Behaviour is then modeled as separate events over time (as depicted in Figure 12), where each event is the direct result of the preceding event(s). It represents how accidents are initiated and unfold as a sequence of events, viewing the cause of accidents as a chain of distinct occurrences that happen in a specific chronological order. The typical representatives of linear chain-of-failure events models are the domino model (Heinrich, 1941) and the Swiss cheese model (Reason, 2000). The Swiss Cheese Model, introduced by James Reason in 1990, is one of the most widely adopted models for understanding accidents. In this model, the holes in the slices of cheese symbolize weaknesses, gaps, or failures in safety barriers—points where the barriers are ineffective in preventing the progression of a risk event. The Bow-tie method is another risk management tool based on this model that can be applied to identifying and displaying the barriers in place that aim to prevent the occurrence of unwanted losses in a system (McLeod, 2018). Bow-tie diagrams visually illustrate the pathway of risk within a system, showing how threats can lead to final consequences. This format helps distinguish between preventive barriers, which aim to stop the threat from occurring, and recovery barriers, which are designed to mitigate the impact if the threat materialises.

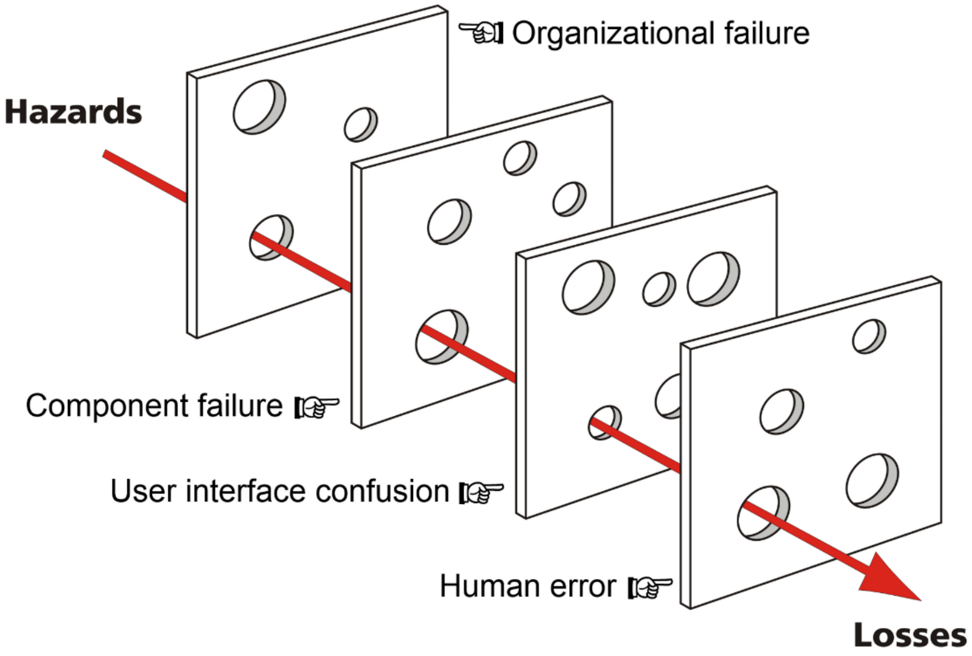

Figure 12 Chain of Events Model [Source- 'Revisiting the Swiss cheese model of accidents', REASON, J., HOLLNAGEL, Erik, et PARIES, Jean].

Several other traditional safety analysis techniques exist which are based on multiple events sequenced as a chain over time such as Failure Mode and Effects Analysis (FMEA), Fault Tree Analysis (FTA), Event tree analysis (ETA) and Hazard and operability study (HAZOP). They have been widely used by many industries to find failure causes and adopt measures to mitigate them. FMEA is an inductive, bottom-up approach, which starts at the component level, where the possible component failure modes are identified, and consequences are examined on a higher level. On the contrary, FTA is a deductive and top-down approach used to map the relationships between a top undesired failure event and the combination of events that lead to its occurrence. HAZOP is a technique used to study the hazards of a system and its operability problems, by exploring the effects of any deviations from design conditions. Event tree analysis is the technique used to define potential accident sequences associated with a particular initiating event or set of initiating events. The event tree model describes the logical connection between the potential successes and failures of defined safety systems or safety functions as they respond to the initiating event and the sequence of events.

The main advantage of Linear chain-of-failure events models is that it can easily graphically show a series of events leading to an accident, which is helpful for understanding and communicating results. Moreover, after an accident occurs, the cause can be quickly found and resolved. However, linear chain-of-failure events model also has some critical drawbacks. For example, choosing one of the many factors as the cause of the accident seems quick and concise, but it often ignores the potential factors that cause the accident; the social and technical characteristics are not fully considered (Leveson N. , 2004). Therefore, linear chain-of-failure events models can cope with relatively simple systems but cannot sufficiently deal with increasingly complex sociotechnical systems (Leveson N. G., 2016).

The assumptions behind the traditional hazard analysis approach—based on system decomposition—were generally valid for older electromechanical systems and still hold for certain aspects of today’s high-tech, software-intensive systems. However, the dramatic increase in complexity, largely due to software, has reduced the effectiveness of this method. It has become far more challenging to predict, understand, plan for, and prevent all possible system behaviours before deployment. Modern complexity introduces “unknowns” that can’t be revealed by simply breaking system behaviour into linear chains of events. Moreover, crucial system properties like safety now depend more on how components interact rather than on the behaviour of individual parts. As a result, accidents can arise from unsafe interactions between components—even when each component is functioning correctly and fulfilling its safety responsibilities.

Systems accident models are the mainstream paradigm of accident models (Rasmussen, 1997). These models take a holistic view of the system, rather than focusing on individual components in isolation. Systems accident models interpret accidents as emergent phenomena that arise from the potential degradation of overall system performance or from complex interactions between components, even when no single component has failed. The representatives of systems accident models are STAMP (System-Theoretic Accident Model and Processes) (Leveson N. , 2004) and AcciMap (Svedung, 2002). AcciMap provides a graphical representation of the accident stakeholders on six levels. The pre-defined six levels of contributing factors in AcciMap make it potentially highly capable of identifying all the contributory factors involved in a particular accident. However, there are also limitations with AcciMap. Firstly, the AcciMap diagram can be very elaborate depending on the complexity of the accident. Summarising the entire accident in the same diagram could make it challenging to understand. Secondly, each of the six levels of stakeholders lack taxonomies or guidewords. Systems accident models aim to describe the dynamic and non-linear risk behaviours in sociotechnical systems.

STAMP (System-Theoretic Accident Model and Processes)

STAMP, which originated from the aviation safety field, provides a new theoretical perspective for system safety. STAMP is a new accident causality model based on systems theory, which provides theoretical foundation for STPA (System-Theoretic Process Analysis).

System Theory

System theory used in engineering was created after World War II to deal with the increased complexity of the systems being built after the war (Stallings, 1976). Systems thinking is an approach used to understand and analyse complex systems by viewing them as interconnected or interdependent entities. It focuses on examining how various parts of a system interact and influence one another. This approach helps identify relationships, patterns, and interactions, leading to a more comprehensive understanding of how a system behaves. By applying systems thinking, one can better grasp complex problems, make more informed decisions, anticipate unintended consequences, and enhance overall system performance. Originally developed to address the complexity of biological systems—where analysing components in isolation led to distorted insights due to tightly coupled interactions—systems thinking was later adopted in engineering, with early applications seen in missile and early warning systems during the 1950s and 1960s (Leveson N. G., 2018) (Leveson N. G., 2016).

Some unique aspects of System Theory are:

- The system is treated as a whole, not merely as the sum of its parts. This reflects a core principle of systems thinking, emphasising that understanding the system requires looking at how components interact and influence each other, rather than analysing each part in isolation.

- A key focus of systems thinking is on *emergent properties*—characteristics of the system that do not exist in any individual component but arise from the interactions among components. These properties cannot be understood by examining parts in isolation; instead, they "emerge" only when the system is viewed as a whole. To fully address emergent properties, it's essential to consider both technical and social dimensions of the system, as these aspects often interact in complex and non-obvious ways.

- Emergent properties come from the relationships between the parts of a system—that is, from how the components interact and connect with each other. These properties are a result of the system's overall structure and the way its parts work together, rather than from any single component alone.

STAMP, grounded in systems theory, broadens the traditional view of causality beyond simple chains of failure events or component malfunctions to encompass complex processes and unsafe interactions among system components. It serves as the foundation for STPA and other related tools. In STAMP, safety is viewed as a dynamic control challenge rather than merely a failure prevention issue. Rather than excluding causes, STAMP includes a wider range of factors, shifting the focus from just preventing failures to enforcing constraints on how the system behaves (Leveson N. G., 2018).

Some advantages of using STAMP are:

- It works on very complex systems because it works top-down rather than bottom-up.

- It includes software, humans, organisations, safety culture, etc. as causal factors in accidents and other types of losses without having to treat them differently or separately.

- It allows creation of more powerful tools, such as STPA, CAST (Causal Analysis based on Systems Theory), identification and management of leading indicators of increasing risk, organisational risk analysis, etc.

These advantages allow the achievement of the following objectives:

- Objective 1: To identify new and amended interactions between stakeholders that already pre-existed in helicopter operation.

- Objective 2: To conduct analysis of unforeseen and unexpected interactions, which may compromise the stability and safety of the ecosystem.

- Objective 3: To capturing Mitigations to prevent these unsafe interactions between stakeholders, thereby mitigating emergent risks.

- Objective 4: To Develop those Mitigations into recommendations for each relevant stakeholder group, resulting in policy updates, operational instructions and practical guidance.

- Objective 5: To communicate the analysis and outcomes with stakeholders and develop momentum for change.

As an approach that is based on system-thinking, STAMP is not just used for accident or hazard analyses. Instead, it is also a model that enables visualisation of systems with complex, non-linear interactions. Although the traditional Chain-of-Failure-Events model (or Dominos or Swiss Cheese Slices illustrated in Figure 12, all of which are essentially equivalent) has been robust in capturing linear causalities, it is not enough to be applied in a complex system with dynamic and non-linear interactions. STAMP has therefore been an alternative to the Chain-of-Failure-Events model. Traditional analysis methods like FTA, ETA, HAZOP, and FMEA are based on the Chain-of-Failure-Events Model assumptions about why accidents happen. In contrast, newer analysis methods can be built on the STAMP framework. The two most used STAMP-based tools today are STPA and CAST. STPA is a proactive approach that identifies potential accident causes during system development to eliminate or control hazards. CAST, on the other hand, is a reactive method that investigates accidents or incidents after they occur to determine the causal factors involved.

STPA is a relatively new hazard analysis technique which assumes that accidents can be caused by unsafe interactions of system components, none of which may have failed. STPA recognises safety as an emergent property of a complex system caused by the interaction of its components. One of the key benefits of STPA is that it allows the analyst to identify hazards and their corresponding Mitigations, that if implemented, would prevent the hazard from occurring. It therefore supports to create the preventive action for a hazard and not just its downstream mitigation (as in other methods). STPA can identify a diverse range of Causal Factors (component failures, component interactions, specification flaw, human error, design flaws, societal issues, organisational issues, etc.) in any technical or socio-technical systems with many diverse components interacting together (Leveson N. G., 2018). Some of the advantages of STPA over traditional hazard/risk analysis techniques are that:

- Very complex systems can be analysed using STPA. "Unknown unknowns" that were previously only found in operations can be identified early in the development process and either eliminated or mitigated. Both intended and unintended functionality are handled.

- Unlike the traditional hazard analysis methods, STPA can be started in early concept analysis to assist in identifying safety mitigations and constraints. These insights guide the design of safety (and security) into the system architecture from the start, reducing costly redesigns later in development or operation. As the design evolves, STPA is continuously refined to support more detailed design decisions, with full traceability from mitigations to all system artifacts, improving maintainability and system evolution.

- STPA explicitly includes software and human operators in the analysis, ensuring that all potential causal factors contributing to losses are considered.

- STPA also provides clear documentation of system functionality, which is often missing or hard to find in large, complex systems.

STPA applied to social technical systems (Chen S. K., 2021) as well as applications in space (Owens, 2008), aviation (Liu), medical (Silvis-Cividjian, 2020) defence (Stanton) marine (Sultana, 2019) and automotive industries (Chen S. a., 2020) (Chen S. a., 2023) (Khastgir, 2021) and have delivered promising results.

Many evaluations and comparisons of STPA to more traditional hazard analysis methods, such as FTA, FMEA, ETA, Bow-Tie and HAZOP have been done (Merrett H. C., 2019) (Sun, 2022) (James Elizebeth, 2023). In all these studies, STPA not only found all the causal scenarios found by the traditional techniques, but also identified many more, often software-related and non-failure scenarios that the traditional methods did not find. In certain cases where analysts were unaware of a past accident, only STPA was able to identify the root cause. Additionally, STPA proved to be significantly more cost-effective, requiring less time and fewer resources compared to traditional methods.

A comparison of FMEA and STPA based on the case study of a forward collision avoidance system case showed that the two methods complemented each other (Sulaman, 2019). A Comparison of STPA and Bow-tie Method Outcomes in the Development and Testing of an Automated Water Quality Management System showed that STPA process was able to identify some hazards which did not visibly relate to the Bow-tie barriers. However, the Bow-tie diagram included a visible distinction between preventative and recovery hazard controls (Merrett H. , 2019). Previous studies have also proposed the complimentary use of the Bow-Tie method and STPA, where a bow-tie diagram can provide the analyst with a prompt of the areas of concern before commencing the STPA process to provide a more robust outcome (Chatzimichailidou, 2018). (Bensaci, 2020) presents an approach that combines aspects of qualitative approach (STPA) and quantitative approach (Bow-tie) for safety assessment purposes. The authors applied this combined approach to multi-robot systems, considering coordination, cooperation, and collaboration aspects. Initially, STPA was used to extract hazardous scenarios related to different types of hierarchical coordination architectures and their causal factors. Subsequently, Bow-tie was used to evaluate these scenarios, aiming to compare different control approaches within multi-agent systems. (Benhamlaoui, 2020) applied both STPA and Bow-tie methods to hazard identification in pipeline transportation, specifically focusing on a condensate pipeline. The study demonstrated that integrating both methods provides a more comprehensive hazard analysis, capturing different aspects of potential risks and their management.

In 2012, Lincoln Laboratory was tasked by the Federal Aviation Administration (FAA) Office of Safety and Technical Training, AJI-312, to conduct a survey of risk-based modeling and analysis techniques to support NextGen concept assessment and validation (Harkleroad, Vela, Kuchar, & Barnett). An operational concept early in its development process presents both great challenge and great opportunity. A less developed concept can often lack rigorous safety and risk analysis, as fewer risk modeling options are available. However, the advantage of early safety evaluation is that systems at this stage have fewer design constraints and should offer greater opportunity for safety-driven design changes; major design changes become less feasible as development progresses (Harkleroad E. a., 2013). The report identified System Theoretic Process Analysis (STPA) as capable of identifying hazards and analysing risk during a system’s initial development process and recommended consideration of applying STPA to NextGen concepts early in their design (Leveson N. G., 2016) (Harkleroad E. a., 2013).

Another report summarising a joint effort by civil aviation authorities to evaluate System-Theoretic Process Analysis (STPA) and its applicability to aviation safety including safety management, aircraft development, safety assessment, and certification involving Subject Matter Experts (SMEs) from FAA, EASA, ANAC, ICAO, and NASA concluded that STPA addresses important gaps that exist in standard approaches to safety that are used today and is more effective for future technologies like increasing autonomy and eVTOLs (Thomas & Van Houdt, 2024).

The Risk Sub-Group of the eVTOL Safety Leadership Group (eVSLG) thus decided to apply STPA to understand and establish a new safety analysis procedure for emerging technologies in the aviation industry. This was undertaken with the recognition for the need for more systems engineering based approaches to be used for both safety analysis and for creating new policy recommendations. As part of the preliminary phase of the project, STPA was applied to helicopter operations - between London Heliport and Silverstone Aerodrome, due to the volume of operations for special events. In the following phase, STPA was applied to eVTOL operations between London Heliport and Silverstone Aerodrome, as an example. The results would however be applicable to eVTOL operations between any two licensed Vertiports/aerodromes.

System-Theoretic Process Analysis (STPA)

The standard STPA methodology developed by Professor Nancy Leveson of Massachusetts Institute of Technology, consists of four steps (Leveson N. G., 2018) as shown in Figure 13:

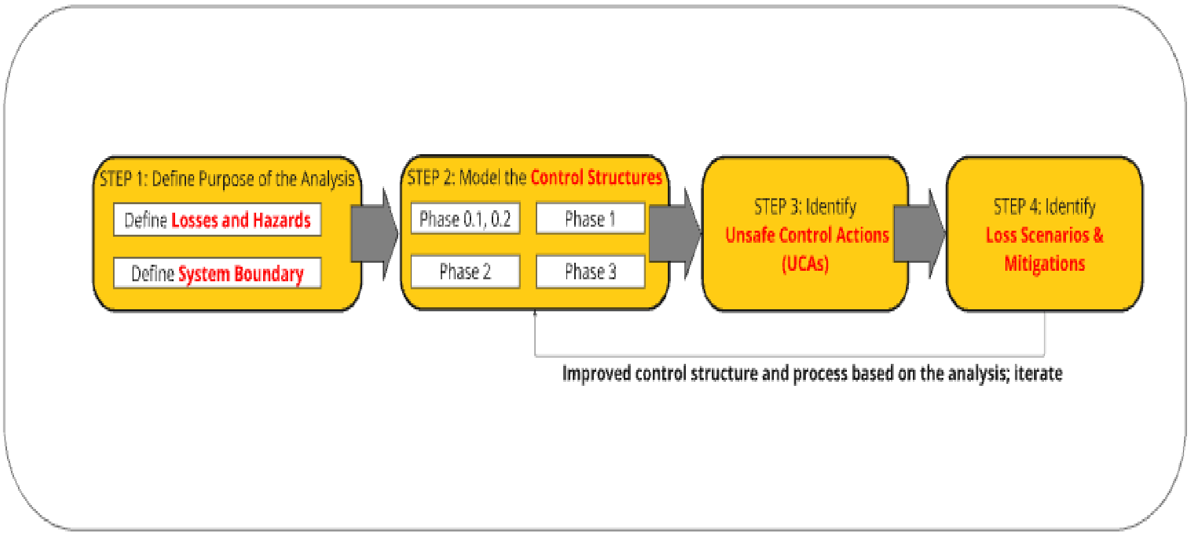
STEP 1: Define Purpose of the Analysis
Define Losses and Hazards
Define System Boundary
STEP 2: Model the Control Structures
Phase 0.1, 0.2
Phase 1
Phase 2
Phase 3
STEP 3: Identify Unsafe Control Actions (UCAs)
STEP 4: Identify Loss Scenarios & Mitigations
Improved control structure and process based on the analysis; iterate

Figure 13 Overview of the STPA methodology

Step 1: Define Purpose of the Analysis

The initial step of the analysis involves identification of the objective of the analysis. Will STPA be limited to traditional safety objectives, such as preventing human fatalities, or will it also be used to address broader concerns like security, privacy, system performance, and other critical properties? Clearly defining the system to be analysed and establishing its boundaries is essential. This foundational step ensures clarity about what is included in the analysis and what lies outside its scope. This phase involves addressing several core questions to ensure a complete understanding of the analysis objectives. A crucial component of this stage is identifying potential losses and hazards, as these elements guide the focus and direction of the analysis.

This part involves carefully identifying any possible negative outcomes or adverse events that might arise due to hazards within the system. A *loss* involves something of value to the stakeholders such as human life or injury, pollution, loss of mission, reputation, or property which are unacceptable to stakeholders (Leveson N. G., 2018).

A basic approach to identifying losses might involve steps such as:

- Identification of stakeholders such as customers, users, operators, etc.

- Identification of stakes in the system such as their value, for example, human life, transportation, aircraft fleets, etc., and their goals, for example, providing medical treatments, maintaining aircraft fleets, providing transportation, etc.

- Finally, convert those values into loss. For example, loss of human life, aircraft, transportation, etc

Some examples of losses that users aim to prevent are:

- L-1: Loss of life or injury.
- L-2: Loss of or damage to system or vehicle.
- L-3: Loss of or damage to others in the environment.
- L-4: Loss of mission such as (transportation, defence, surveillance, etc.).
- L-5: Loss of client satisfaction.
- L-6: Environmental loss

The losses identified in STPA can be safety-critical (e.g. Loss of life or injury) or non-safety-critical or business losses (e.g. Loss of client satisfaction). Losses could also be from the environment level which could be out of the system designer's perspective. There should be documentation where explicitly excluded losses are mentioned and their exclusion justified. After the losses of concern in the analysis are identified, the subsequent step is to define the hazards related to these losses. A hazard is a system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to a loss. Typically, a hazard can result in multiple losses, and it's essential to link each hazard to its corresponding losses. This connection is usually indicated in brackets following the hazard description (Leveson N. G., 2018). Listed below are some examples of hazards.

H-1: Aircraft violates minimum separation requirements in flight [L-1, L-2, L-4, L-5]

H-2: Airframe integrity of the aircraft is lost [L-1, L-2, L-4, L-5]

H-3: Aircraft leaves designated taxiway, runway, or apron on the ground [L-1, L-2, L-5]

Step 2: Model the control structure

The subsequent step involves developing a system model referred to as a control structure. In systems theory, components are organised in hierarchical levels: every level controls the level below. The behaviour in the lower level can be controlled or limited by components at higher levels. The control structure illustrates the functional interactions between the system components by representing the system as a series of feedback control loops.

In general, a hierarchical control structure contains at least five types of elements:

- Controllers
- Control Actions

- Feedback
- Other inputs to and outputs from components (neither control nor Feedback)
- Controlled Processes

Typically, a controller issues Control Actions (CA) to control a process, utilising feedback signals to monitor the Controlled Process, as shown in the generic control loop (Figure 14). The Control Algorithm represents the controller's decision- making process, it determines the CAs to provide. Controllers use Process Models to represent their internal understanding of the system or environment they are regulating—referred to as the Controlled Process. These models help guide decision-making. In the case of humans, this internal representation is typically called a mental model, and the decision-making mechanisms are often known as operating procedures or rules (Leveson N. G., 2018). Despite the different terminology, the fundamental idea remains the same.

Accidents often occur when there's a mismatch between the controller's Process Model and the actual state of the system or environment, highlighting the critical role of accurate system control. Issues can arise anywhere within the control loop, as shown in Figure 14. For instance, if a Process Model is inaccurate—such as when a controller believes a vehicle is in Park when it is actually in Reverse, or assumes an aircraft is descending when it's climbing—this can lead to unsafe Control Actions. Faulty sensors may also provide incorrect Feedback, resulting in dangerous outcomes. Furthermore, a system design might lack necessary Feedback mechanisms or deliver them too late, causing errors in the Process Model and leading to unsafe decisions or behaviour (Leveson N. G., 2018).

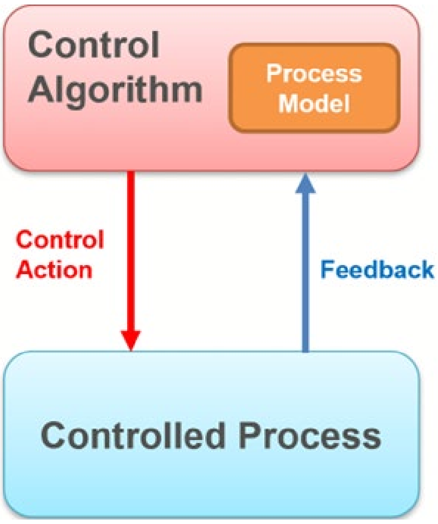

Figure 14 Generic Control Loop

Initially, the control structure is created at a high abstraction level (less detailed) and then, it is gradually refined through various iterations, adding more details about the system. A simple example of a control structure for aviation is shown in Figure 15. To manage system complexity, control structures often apply abstraction. For instance, in a commercial aircraft, there may be two or three pilots operating the flight. Rather than representing each pilot separately in the control model, they can be grouped as a single unit- “flight crew”-that collectively issues Control Actions and receives Feedback.

Similarly, instead of detailing every individual subsystem of the aircraft, the model can begin at a higher level of abstraction, distinguishing between aircraft automation systems and the physical components they manage. The vertical axis in a hierarchical control structure carries significance: it reflects the flow of control and authority. Higher-level controllers are positioned at the top, while lower-level entities appear at the bottom. Each element exercises control over those directly beneath it and, in turn, is governed by those directly above it in the hierarchy (Leveson N. G., 2018). For example, the Automated Controllers in Figure 15 can act as a Controller by sending control actions to the Physical Processes and monitor Feedback. At the same time, the Automated Controllers is also a Controlled Process that receives and executes Control Actions from the Flight Crew and sends Feedback to the crew.

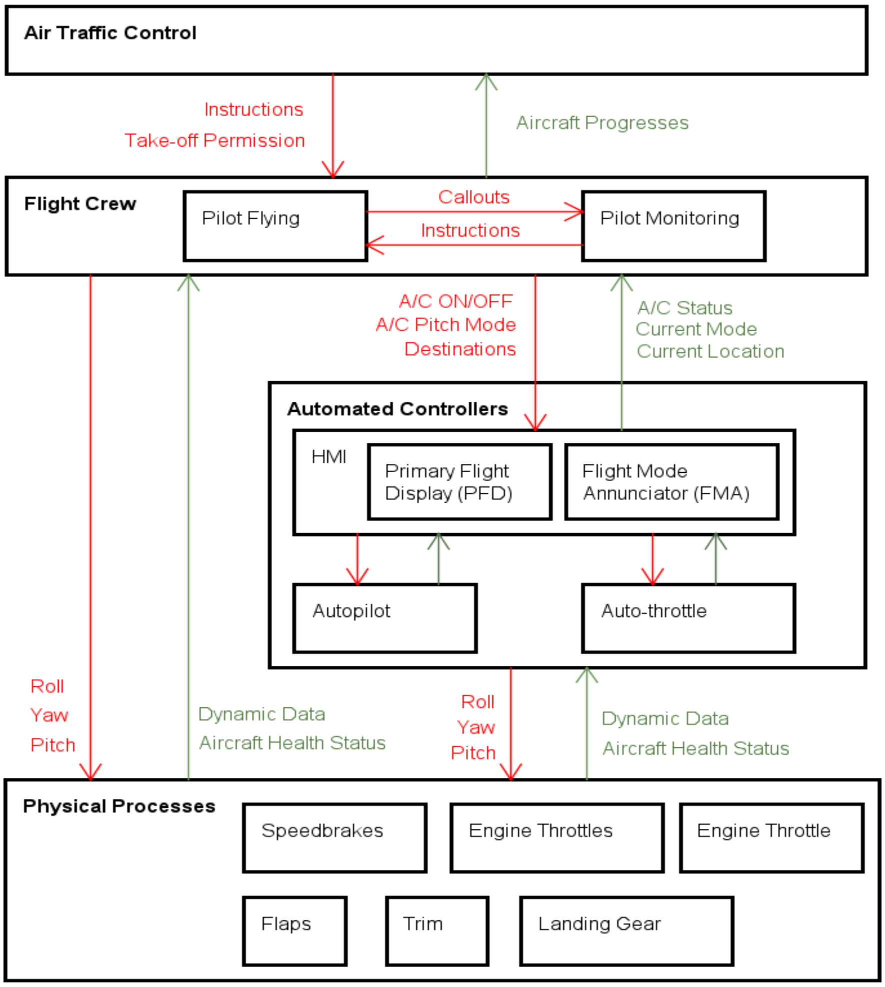

Figure 15 An example of a hierarchical control structure for Aviation

Sometimes, just drawing a simple control structure diagram can reveal flaws that were previously unnoticed. For instance, Control Actions (CA) might be issued by components lacking the essential feedback to choose safe CAs. Additionally, feedback could be offered to those unable to address it, and various controllers might give contradictory commands to the same component without the capability to identify or resolve such conflicts, among other scenarios (Leveson N. G., 2018).

Step 3: Identify Unsafe Control Actions (UCA)

After the control structure has been modelled, UCAs are identified for every CA in the control structure. Each CA is analysed to identify how the CA would manifest into a UCA. UCAs should specify the context in which the CA is unsafe. Context is essential when analysing Unsafe Control Actions (UCAs). If a Control Action (CA) were inherently unsafe in all situations, it likely would not have been incorporated into the system in the first place. Therefore, each UCA must clearly define the specific conditions under which the CA becomes unsafe. Identifying these contexts allows us to either eliminate such scenarios from the system design or develop mitigation strategies. A UCA can reference any context that contributes to its potential hazard, such as environmental conditions, the state of the Controlled Process, the Controller's internal state, previous or repeated actions by the Controller, the behaviour or state of other Controllers, simultaneous or conflicting actions, or specific characteristics of the CA itself (e.g., a certain braking force being applied). Including words such as - “when,” “while” or “during” in the wording of UCAs, can be particularly useful for clearly defining the circumstances in which the CA becomes hazardous (Leveson N. G., 2018).

To identify a UCA, the CA is usually considered together with a particular context and worst-case environment. There are four ways a CA can be unsafe:

- Not providing the CA leads to a loss.
- Providing the CA incorrectly or when not needed leads to a loss.
- Providing a CA too early or too late or in the wrong order leads to a loss.
- Providing the CA too long or stopping the CA too soon leads to a loss (for continuous CAs, not discrete ones).

A UCA contains five parts, as shown in Figure 16.

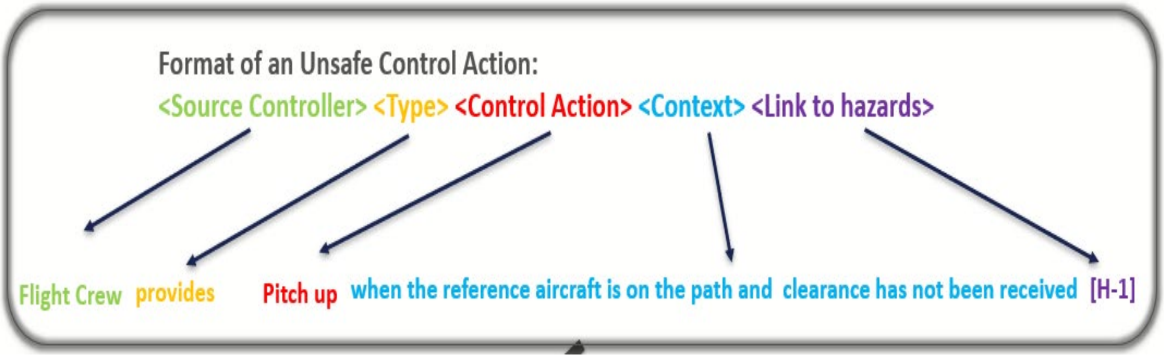
Format of an Unsafe Control Action:
<Source Controller> <Type> <Control Action> <Context> <Link to hazards>
Flight Crew
provides
Pitch up
when the reference aircraft is on the path and clearance has not been received
[H-1]

Figure 16 Structure of a UCA

The first part is the controller that can provide the CA. The second part is the type of unsafe CA (provided, not provided, too early or too late, stopped too soon or applied too long). It is worth noting that there may be multiple UCAs identified for the same type. The third part is the CA or command itself (from the control structure). The fourth part is the context discussed above, and the last part is the link to hazards (identified in Step-1). Some example UCAs linked to the CA – 'Pitch-Up' (issued by the Flight Crew) are shown in Table 15.

UCA Type	UCA Descriptions
Not Provide	UCA 1.1: Flight Crew does not provide Pitch up when it has received clearance [H-3]
Provide incorrectly or when not needed	UCA 1.2: Flight Crew provides Pitch up when the ref aircraft is on the path and clearance has not been received. [H-1,2]
Provide too early or too late	UCA 1.3: Flight Crew provides Pitch up too early before clearance has been received[H-1,2]
Provide too long or too short	UCA 1.4: Flight Crew stops providing Pitch up too soon when the aircraft has not reached the designated altitude [H-1]

Table 15 A selection of UCAs for the CA- Pitch Up

Step 4: Identify Loss Scenarios

Once the UCAs are identified for all the CAs in the control structure, possible loss scenarios, which describe the Causal Factors (CFs) or causes that can lead to the UCAs, are identified by analysing the specific control loops of the CAs. Following this, Mitigations can be defined to prevent or mitigate these CFs.

A loss scenario describes the CFs that can lead to the UCAs and to losses. Two types of loss scenarios must be considered:

a) Why would unsafe or inadequate CAs occur?

b) If the CA was originally safe or adequate, why would it be improperly executed or not executed, leading to an UCA?

Until now, the analysis has focused on identifying potential Control Actions (CAs) and Feedback within the system, but it has not addressed how Feedback is obtained (e.g., through sensors) or how Control Actions are carried out (e.g., via actuators). To understand the specific causes of unsafe control and Feedback in real-world scenarios, it's beneficial to refine the control structure by explicitly incorporating sensors and actuators. This additional detail provides greater insight into how unsafe situations can arise and supports the development of more effective safety measures.

a) Why would unsafe or inadequate CAs occur?

This type of loss scenario can be generated by starting with an Unsafe Control Action (UCA) and working backward to determine what could lead the Controller to issue (or fail to issue) that Control Action (CA). To identify type A loss scenarios, we must consider various factors, starting with the unsafe Controller behaviour that caused the UCA (Leveson N. G., 2018).

Scenarios that lead to UCAs are in general caused due to **1) unsafe Controller behaviour** and **2) inadequate Feedback or other inputs received**.

- **Unsafe Controller behaviour**

There are four general reasons why a Controller might provide (or not provide) a CA that is unsafe:

1. Failures involving the Controller (for physical Controllers)
2. Inadequate Control Algorithm (flawed algorithm, flawed implementation or degradation over time)
3. Unsafe control input (from another Controller)
4. Inadequate Process Model

Process model flaws happen when the Controller’s understanding of the process doesn’t align with what’s actually happening. These flaws can arise if the Controller gets wrong feedback or information, if it receives correct feedback but misinterprets or disregards it, if the feedback is delayed or never received when needed, or if the necessary feedback simply doesn’t exist (Leveson N. G., 2018).

The loss scenarios can be captured in a structured and efficient way by asking:

1. What was the Process Model’s belief of the Controller?
2. What was the reason for this belief?
3. What was the cause (loss scenario) that triggered this reason?

Example:

UCA-1.4: The Pilot stops providing pitch up too soon when the aircraft has not reached the designated altitude [H-1]

Process Model (belief) of the Controller that could cause the UCA: The pilot believes that the aircraft has reached the designated altitude.

The reason for the Process Model Belief: The Pilot believes so because they received no Feedback confirming that the target altitude had been reached.

The CF that triggered this reason: The Feedback confirming whether the target altitude has been reached or not, is missing in the system design (*inadequate/missing Feedback*).

Loss Scenario 1 for UCA-2: The Pilot stops providing pitch up too soon when the aircraft has not reached the designated altitude because the pilot incorrectly believes that the aircraft has reached the designated altitude. This is due to the lack of a Feedback in the design providing confirmation to the Pilot on whether the designated altitude has been reached or not.

A Mitigation that can be proposed to address this loss scenario would be:

Mitigation to prevent the cause/CF: Feedback confirming that the target altitude has been reached, shall be included in the system design.

- **Causes of inadequate Feedback and information**

Scenarios involving insufficient feedback or information typically include:

1. Feedback or information not received
2. Inadequate Feedback is received

When a scenario reveals that Feedback or information (or the absence of it) could lead to an Unsafe Control Action (UCA), it’s important to investigate the source of that information to understand what might contribute to the issue. Feedback typically originates from the Controlled Process, often through sensors, while other types of information may come from additional processes, other Controllers, or various components within the system or its environment. Identifying these sources helps uncover potential failure points and supports more effective risk mitigation.

b) Why would the CA (that was originally safe or adequate) be improperly executed or not executed, leading to an UCA?

Hazards may arise from Unsafe Control Actions (UCAs), but they can also occur even without a UCA if control actions are executed incorrectly or not executed at all. To identify such scenarios, it is important to examine **3) factors that affect the control path** as well as **4) factors that affect the Controlled Process** (Leveson N. G., 2018).

- **Factors involving the Control Path**

The control path illustrates how Control Actions (CAs) are transmitted from the Controller to the Controlled Process. It's important to analyse this path to identify how issues may prevent CAs from being delivered correctly—or at all. Such problems are often linked to communication delays or errors between the Controller and the Controlled Process, as well as failures or performance degradation in the Actuators responsible for executing those actions.

- **Factors related to the Controlled Process**

Although CAs might be transferred or implemented within the Controlled Process, their efficacy is not guaranteed, and they could potentially be superseded by other Controllers. Typically, scenarios involving the Controlled Process might encompass:

1. The CA being not executed (i.e., the CA is applied or received by the Controlled Process, but the Controlled Process does not respond) due to the received CA from other controllers.
2. The CA is improperly executed (i.e., the CA is applied or received by the Controlled Process, but the Controlled Process responds improperly) due to failure or degradations of the Controlled Process, and disturbances from other inputs.

Further guidance and examples of application of STPA can be found in (Leveson N. G., 2018).

Annex B: Detailed Process for Prioritisation of UCAs and Mitigations

Prioritisation of UCAs

Pre-Mitigation Severity (PMS):

PMS defines the severity of a risk before any mitigation is implemented. In this case, it defines the severity of each UCA. Based on the traditional process of STPA, each UCA should lead to at least one system-level hazard or loss that is identified in Step 1, as otherwise, the control action would be safe. To enable the identification of the PMS of each UCA, the Step 1 results are extended by refining each Loss based on Design Assurance Levels (DAL): 1) Catastrophic; 2) Hazardous; 3) Major; 4) Minor; and 5) No Effect). These guidewords define the severity levels, with 'Catastrophic' representing the highest severity and incrementally 'No Effect' representing the lowest severity (i.e., zero severity). They have been commonly used in many standards such as DO-178C (Software Considerations in Airborne Systems and Equipment Certification). In this work, 'No Effect' is not considered.

Table 16 illustrates the refined sub-losses of the five Losses identified in Step 1. It also summarises the PMS values assigned to each sub-loss. There are in total twenty sub-losses, each of which has a unique PMS value assigned, ranging from 20 (most severe) to 1 (least severe).

ID		Description	PMS
L1 **(Human Loss)**	**L1.1**	**Catastrophic:** Total fatalities (loss of life)	**20**
	L1.2	**Hazardous:** Multiple Fatalities and/or serious injuries that include mental health losses (e.g., trauma).	**19**
	L1.3	**Major:** Multiple serious injuries and/or multiple injuries	**18**
	L1.4	**Minor:** Minor/non-serious injuries.	**10**
L2 **(Material Loss)**	**L2.1**	**Catastrophic:** Complete loss of the aircraft (loss of up to 100% of cost).	**17**
	L2.2	**Hazardous:** Serious or fatal damage to the material (loss of up to 75% of cost).	**13**
	L2.3	**Major:** Major damage to the material (loss of up to 50% of cost).	**8**
	L2.4	**Minor:** Minor damage to the material (loss of up to 25% of cost).	**5**
L3 **(Mission Loss)**	**L3.1**	**Catastrophic:** Complete of the tactical mission that significantly affects strategic mission.	**15**
	L3.2	**Hazardous:** Complete loss of the tactical mission.	**9**
	L3.3	**Major:** Partial loss of the tactical mission.	**4**
	L3.4	**Minor:** Minor degradations of the tactical mission.	**1**
L4 **(Consumer Demands Loss)**	**L4.1**	**Catastrophic:** Complete loss of customer satisfactions / consumer demands (up to 100%).	**16**
	L4.2	**Hazardous:** Serious loss of customer satisfactions / consumer demands (up to 75%).	**12**

ID		Description	PMS
	L4.3	**Major:** Major loss of customer satisfactions / consumer demands (up to 50%).	7
	L4.4	**Minor:** Minor loss of customer satisfactions / consumer demands (up to 25%).	2
L5 (Business Goal Loss)	L5.1	**Catastrophic:** Complete loss of business goals (up to 100% of total business goals).	14
	L5.2	**Hazardous:** Serious loss of business goals (up to 75% of total business goals).	11
	L5.3	**Major:** Major loss of business goals (up to 50% of total business goals).	6
	L5.4	**Minor:** Minor loss of business goals (up to 25% of total business goals).	3

Table 16 Summary of Sub-losses and PMS assigned

Controller Impact Factor (CIF)

CIF is a parameter that quantifies the impact of a controller. To rank the impact of each controller of the control structure, i.e., their CIF value, it is important to understand how many blocks are affected by the decisions (i.e., the CAs) made by that controller. In STPA, a control structure is created in such a way that functional blocks are located hierarchically - i.e., controllers are above the controlled processes. A mechanism was proposed to rank the CIF based on the hierarchy of the blocks. In this project, the block [Regulator (CAA)] (as in Figure 5) has the highest CIF value because it is located at the top level of the control structure. The behaviours of and decisions made by the other blocks, can directly or indirectly be affected by the CAs from [Regulator (CAA)]. The next highest CIF value is assigned to [NATS (LHR RADAR)], which is located at the second highest level of the Control Structure. The [Commander] block, which directly engages with the passengers and aircraft, has the lowest CIF in this control structure. While it may sound atypical that a commander has the lowest impact factor here, it is important to note that the ranking of CIF is closely linked to the system being analysed.

In this work, the scope of the analysis is to understand potential issues of the whole eVTOL operation, which involves regulatory, organisational, and operational management. A UCA from a high CIF controller (like the Regulator) could potentially affect many other stakeholders simultaneously such as the operation of all the vertiports, eVTOL operators, and commanders of different eVTOL aircraft. It is therefore arguable that the commander as part of this system would have a much lower CIF value compared to the regulator. Table 17 summarises the CIF values for each Controller.

Phase of Control Structure	Controller	CIF (Range)
0.1, 2	Regulator (CAA)	8
0.1, 1	NATS (LHR RADAR)	7
0.1	Local Authority (Battersea)	6
0.1	Local Authority (Silverstone)	5

Phase of Control Structure	Controller	CIF (Range)
0.1, 0.2, 1	Licensed Vertiport (Battersea)	4
2, 3	Licensed Aerodrome (Silverstone)	3
0.1, 0.2, 1	eVTOL Operator	2
0.2, 1, 2, 3	Commander	1

Table 17 Summary of CIF values for each Controller

Expert Judgement Score (EJ)

To calculate the EJ, stakeholders were asked to provide inputs for each EJ parameters for every UCA identified. There are in total five parameters that need to be considered, each parameter has its own scoring system with two levels (e.g., for Likelihood of Occurrence) or three levels (e.g., for the other four parameters), as summarised in Table 18.

Domain experts first assign each parameter a score. Each UCA would then have five scores (one for each parameter). These scores are then calculated to identify the EJ value of each UCA. To minimise bias, an objective approach called Monte Carlo Simulation (MCS) is then used to calculate the final EJ value. In the context of decision analysis, in scenarios where expert judgements are subject to uncertainty, MCS enables the visualisation of the distributions after running random simulations to identify sensitivity to changes (Rose, 2023). MCS can help identify which expert inputs most significantly influence the overall ranking or outputs, as well as determine which criteria remain stable under variations.

Parameters	Descriptions
Operational Disruption	**Severe:** The UCA leads to severe disruptions, including system-wide airspace management breakdowns, multiple flight cancellations, or long-term restrictions. **Moderate:** The UCA results in localized disruptions that impact only a subset of operations (e.g., temporary rerouting of eVTOLs or limited delays in specific areas). **Minor:** The UCA causes very limited disruptions with manageable consequences (e.g., slight changes in airspace allocation or route adjustments).
Criticality	**Severe:** The UCA causes an immediate risk to eVTOL operational safety, leading to catastrophic consequences. **Moderate:** The UCA causes operational delays or significant safety concerns but allows time for corrective action. **Minor:** The UCA has minimal impact, such as causing minor delays or requiring rerouting, without posing a significant risk to eVTOL operations or safety.
Detectability	**Low Detectability:** The UCA is inherently difficult to detect due to limited monitoring capabilities or delayed Feedback, leading to potential long-term risks before discovery. **Moderate Detectability:** The UCA can be identified but requires significant effort, manual intervention, or time to detect and correct, often delaying the response. **High Detectability:** The UCA is easily and promptly detected, either through

Parameters	Descriptions
	automated systems or real-time monitoring, allowing for rapid intervention with minimal disruption.
Effect on Other Stakeholder	**Severe:** The UCA affects multiple stakeholders, causing a breakdown in communication, coordination, or responsibilities. **Moderate:** The UCA affects only some stakeholders and can be managed through coordination. **Minor:** The UCA has little to no impact on stakeholders or causes minimal inconvenience.
Likelihood of Occurrence	**1**: The UCA has not been mitigated by pre-existing regulations and is likely to occur. **0**: The UCA has been mitigated by pre-existing regulations and is unlikely to occur.

Table 18 Factors considered for Expert Judgement for prioritisation of UCAs

EJ Score Calculation Procedure

The process for calculation of EJ score is illustrated in Figure 17.

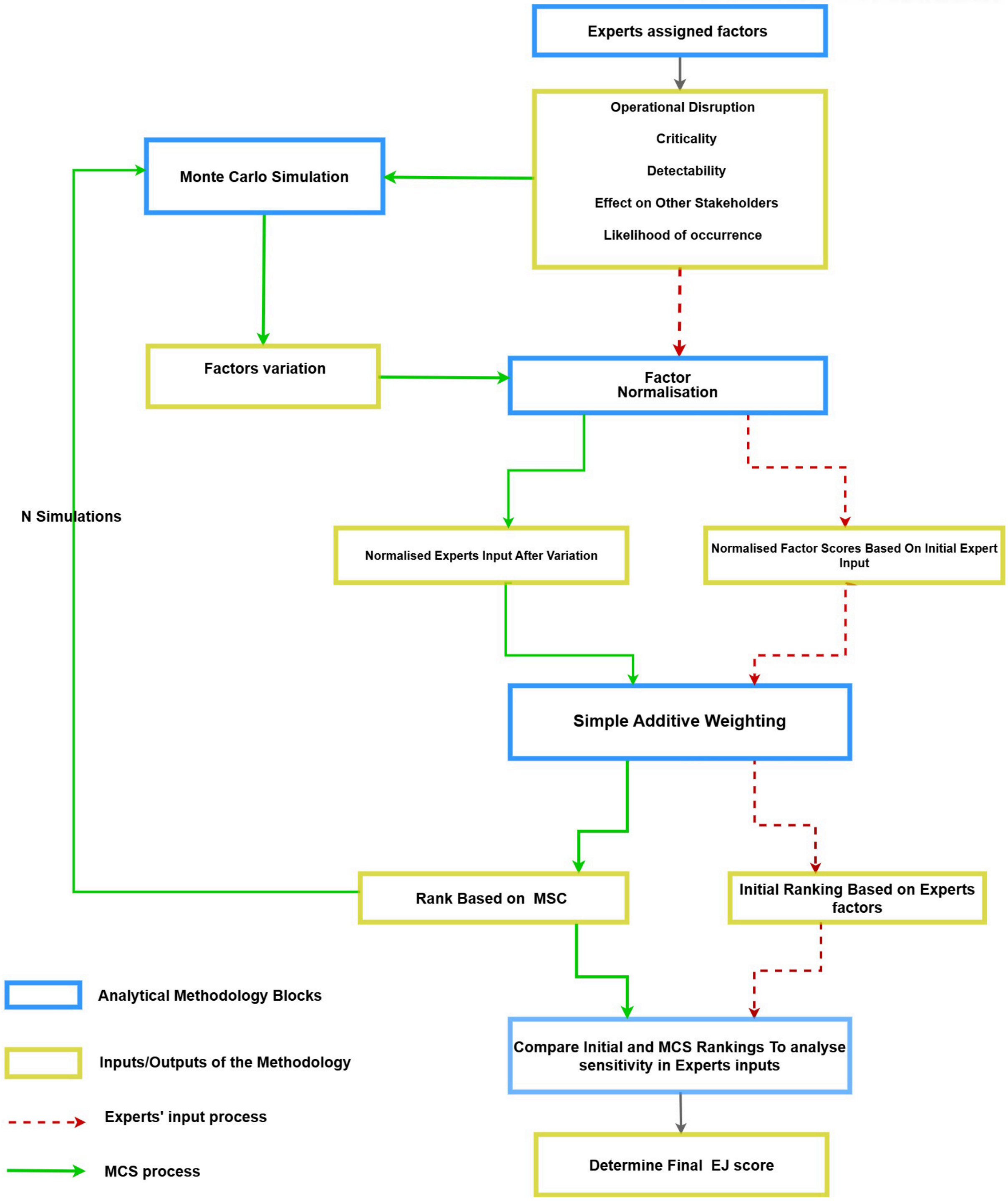
Experts assigned factors
Operational Disruption
Criticality
Detectability
Effect on Other Stakeholders
Likelihood of occurrence
Monte Carlo Simulation
Factors variation
Factor Normalisation
N Simulations
Normalised Experts Input After Variation
Normalised Factor Scores Based On Initial Expert Input
Simple Additive Weighting
Rank Based on MSC
Initial Ranking Based on Experts factors
Compare Initial and MCS Rankings To analyse sensitivity in Experts inputs
Determine Final EJ score
Analytical Methodology Blocks
Inputs/Outputs of the Methodology
Experts' input process
MCS process

Figure 17 Overview of the EJ score calculation Process

1. Expert Judgment Factors

The first step in applying this methodology is to collect experts' input from various stakeholders. These inputs are then translated into numerical scores to enable objective analysis. For example, experts assessing impact levels assigned a score of:

- 3 for high impact
- 1 for low impact

Note: Since lower detectability increases risk, it is scored inversely:

- 3 for low detectability
- 1 for high detectability

2. Factor Normalisation:

Initially, each factor is normalised, meaning it is adjusted so that all factors have the same impact on the final rankings, regardless of their original scales (e.g., Detectability is assessed on a three-point scale, while Likelihood of Occurrence uses only a two-point scale).

3. Simple Additive Weighting (SAW):

After normalisation, an initial score for each UCA is calculated using Simple Additive Weighting (SAW). This means adding together scores given by experts to form an initial ranking.

4. Monte Carlo Simulation (MCS):

The main goal of using MCS is to test how sensitive or stable the initial rankings are to small changes in experts' scoring. This is done through the following process:

- Each factor's original score is adjusted slightly (by, e.g., ±10%, ±30%...) many times (typically 1,000 repetitions).
- For every small adjustment, the SAW score is recalculated.
- After repeating this procedure multiple times, the stability or variability of each UCA's ranking is measured.
- Finally, an overall stable (average) score is calculated for each UCA.

Practical Example:

1. Expert Assigned Factors

The first step is to collect the factor scores from the experts. Then, finalise the process by assigning a score to each intensity, ranging from 1 to 3, based on its priority. Table 9Table 19presents an example of UCAs and their respective scores for each factor. This example will be used to demonstrate the application of the methodology for calculating the EJ score.

UCA-ID	Operational Disruption	Criticality	Detectability	Effect on Other Stakeholders	Likelihood of occurrence
UCA-1.1.1	3	3	2	3	0

UCA-ID	Operational Disruption	Criticality	Detectability	Effect on Other Stakeholders	Likelihood of occurrence
UCA-1.2.1	2	2	3	3	1
UCA-2.1.1	1	2	1	2	1

Table 19 Example of scores allocated to UCAs by experts

2. Factor Normalisation

Table 20 presents the output of the second step- Factors normalisation.

UCA-ID	Operational Disruption	Criticality	Detectability	Effect on Other Stakeholders	Likelihood of Occurrence
UCA-1.1.1	1.00	1.00	0.5	1.00	0
UCA-1.2.1	0.5	0	1.00	1.00	1.00
UCA-2.1.1	0	0	0	0	1.00

Table 20 Factor Min-Max Normalisation.

3. Simple Additive Weighting

Table 21 presents the output of the application of SAW to the normalised factors assigned by the domain experts, and an initial ranking is generated.

UCA-ID	Initial SAW Score	Initial Rank
UCA-1.1.1	3.5	1
UCA-1.2.1	3.5	1
UCA-2.1.1	1.0	3

Table 21 Simple Additive Weighting Outputs

4. Monte Carlo Simulation (MCS):

This paragraph presents the algorithm used to implement the MCS and to assess how initial ranking is sensitive to changes.

Simulation 1:

Assume random variations are as follows (one for each factor of each UCA):

Operational Disruption: Originally scored as 2, is increased by 10% (0.10):

- $Operational\ Disruption^1 = 2 \times (1 + 0.10) = 2.20$

Criticality: Originally scored as 1, increased by 50% (0.50):

- $Criticality^1 = 1 \times (1 + 0.50) = 1.50$

Detectability: Originally scored as 1, decreased by 10% (0.10):

- $Detectability^1 = 1 \times (1 - 0.10) = 0.90$

The same approach is applied to the remaining factors. After adjusting these values, the SAW score is recalculated for each UCA. This process is repeated for all UCAs (e.g., UCA-1.2.1 and UCA-2.1.1).

Results of Simulation 1, the normalisation of these factors and the recalculation of the SAW scores is presented in Table 22.

UCA-ID	Operational Disruption	Criticality	Detectability	Effect on Other Stakeholders	Likelihood of Occurrence	SAW Score	Rank
UCA-1.2.1	0.50	0.50	1.00	1.00	1.00	4.00	1
UCA-1.1.1	0.85	1.08	0.40	1.00	0.00	3.33	2
UCA-2.1.1	0.00	0.50	0.00	0.50	1.00	2.00	3

Table 22 Results of Simulation 1

The simulation process described above is then repeated many times (Simulation 2, Simulation 3, etc.), as presented in Table 23.

UCA ID	SAW Score (Sim 2)	Rank (Sim 2)	SAW Score (Sim 3)	Rank (Sim 3)
UCA-1.2.1	3.53	2	4.04	1
UCA-1.1.1	3.90	1	3.76	2
UCA-2.1.1	2.10	3	1.94	3

Table 23 Results of Simulation 2, Simulation 3

5. Compare Initial and MCS Rankings To analyse sensitivity in Experts inputs

After completing multiple simulations, results from each simulation are combined. The final rank for each UCA is decided based on the stability of rankings. An example of the final aggregated rankings in Table 24.

UCA ID	Rank (Sim. 1)	Rank (Sim. 2)	Rank (Sim. 3)
UCA-1.1.1	1	2	1
UCA-1.2.1	2	1	2
UCA-2.1.1	3	3	3

Table 24 Final aggregated rankings based on the example

Calculating the Average Rank:

Calculating the *Average Rank* $_{UCA}$ across multiple simulations provides a measure of central tendency, indicating the position of each UCA in terms of risk priority.

$$\text{Average Rank}_{\text{UCA}} = \frac{1}{\text{num sim}} * \sum_{i=1}^{num\ sim} Rank_{sim} \quad \textbf{(1)}$$

Calculating the Standard Deviation:

For each alternative (UCA), the mean rank across all simulations is calculated using the standard deviation $\boldsymbol{\sigma_i}$ of ranks per UCA and computed as the equation below. The standard deviation $\boldsymbol{\sigma_i}$ measures the variability or dispersion of ranks across simulations, reflecting the stability of each UCA's ranking.

$$\sigma_i = \sqrt{\frac{1}{\text{num sim}} * \sum_{i=1}^{num\ sim} \left(Rank_{sim} - \text{Average Rank}_{\text{UCA}}\ \right)^2} \quad \textbf{(2)}$$

By combining the *Average Rank* $_{UCA}$ and its standard deviation σ_i the *EJ Score* $_{UCAi}$ incorporates both the central tendency and the variability of each UCA's ranking Table 25.

$$\text{EJ Score}_{\text{UCAi}} = \text{Average Rank} + \sigma_i \quad \textbf{(3)}$$

UCA ID	$\textbf{Average Rank}_{\textbf{UCA}}$	$\boldsymbol{\sigma_i}$	$\textbf{EJ Score}_{\textbf{UCAi}}$
UCA-1.1.1	1.33	0.47	1.80
UCA-1.2.1	1.67	0.47	2.14
UCA-2.1.1	3.00	0.00	3.00

Table 25 Generation of EJ score

A lower *EJ Score* $_{UCAi}$ indicates more stable and higher ranked UCAs. The MCS

simulates a ranking of the UCAs based on the evaluation of experts' factors. A tool was developed at WMG to execute this algorithm and generate the Expert Judgement (EJ), for each UCA identified in STPA step 3.

Final Rank

Following the execution of the Monte Carlo Simulation (MCS), a revised ranking of UCAs is obtained. At this stage, a comparative analysis is conducted between the initial expert-based rankings and the MCS-derived rankings. This comparison serves to evaluate the sensitivity of each UCA to changes in the contributing factors and to derive a final, robust Expert Judgement (EJ) score.

- In some cases, UCAs maintained their initial rank despite minor variations in input values. This consistency indicates that the EJ score assigned to these UCAs is stable, and their priority is robust against uncertainty.

- In contrast, some UCAs showed clear changes in their rankings when the input factors were slightly adjusted. The EJ score of these UCAs is considered sensitive, as their priority is strongly influenced by the specific values given to certain factors (the initial Experts' input). This indicates that the input data for these cases may require further refinement, and there's a need for another layer (using PMS and CIF) to define their priorities.

Incorporating both the initial expert inputs and the variability analysis from MCS, guarantee a more objective inputs to the Prioritisation matrix along with PMS and CIF.

UCAs Prioritisation Matrix

The Severity Impact Factor (SIF) -the product of PMS and CIF was plotted against the EJ to enable a granular risk assessment beyond a single-number approach. The UCA prioritisation Matrix maps SIF and EJ score to the corresponding risk priority level. Each cell has a colour that refers to a level of criticality – 'Very Low'(green, P5), 'Low' (yellow, P4), 'Moderate' (orange, P3), 'High' (red, P2) or 'Very High' (dark red, P1), as illustrated in the UCA Prioritisation Matrix in Figure 18.

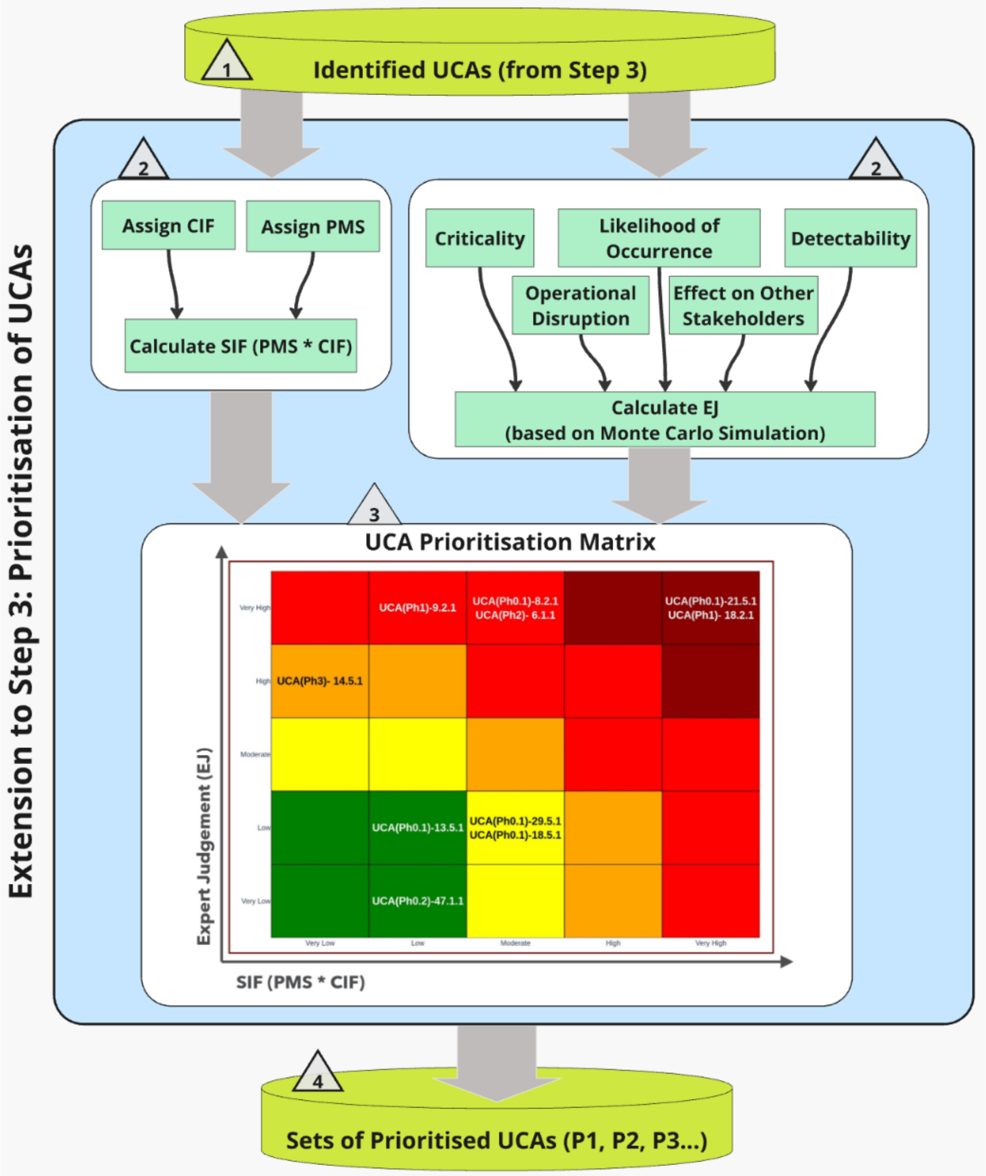

Figure 18 Overview of the concept of prioritisation of UCAs

Prioritisation of Mitigations

Mitigations Score

To reduce subjectivity, Monte Carlo simulation (MCS) method, which is a technique that uses repeated random sampling to estimate the properties of complex systems, was used to compute the Mitigation score, based on the values assigned to the expert judgement factors by the domain experts. Values were assigned for each Mitigation for the following key parameters/factors – 1) Time 2) Cost 3) Type of Mitigation (based on Safety Order of Precedence in (MIL-STD-882E, 2012)) and 4) Likelihood of Occurrence of the CF (Table 26).

Parameters	Descriptions
Time	**Significant:** Implementing the Mitigation would require significant effort

Parameters	Descriptions
	Moderate: Implementing the Mitigation would require moderate effort **Minor:** Implementing the Mitigation would require minor effort
Cost	**High:** The cost involved in implementing the Mitigation would be high **Medium:** The cost involved in implementing the Mitigation would be medium **Low:** The cost involved in implementing the Mitigation would be low
Type of Mitigation	**Type A:** The Mitigation is implemented by selecting a major design or material alternative to eliminate the CF. **Type B:** The Mitigation is implemented by minor design change that reduce the severity and/or the probability of the CF. **Type C:** The Mitigation is implemented by using engineered features or devices to actively interrupt the mishap sequence and reduce the risk of the mishap. **Type D:** The Mitigation is implemented by including detection and warning systems to alert personnel to the CF. **Type E:** The Mitigation is implemented by incorporating signage, procedures, training, and PPE to the personnel.
Likelihood of Occurrence	**1:** The Mitigation has not been covered by pre-existing regulations and the CF is likely to occur. **0:** The Mitigation has already been covered by pre-existing regulations and the CF is unlikely to occur.

Table 26 Factors considered for Mitigation Prioritisation

The weights assigned to the parameters were as follows – Type of Mitigation (0.4), Likelihood of Occurrence (0.3), Time (0.15), and Cost (0.15). The ‘Type of

Mitigation' and 'Likelihood of occurrence' were assigned the highest weights due to their impact on safety. Those Mitigations assigned 1 for the 'likelihood of occurrence' was prioritised over those assigned 0 for the same parameter. A Mitigation assigned Type - 'A' was ranked higher than those assigned other types due to its capability in terms of prevention or mitigation of the CF.

Mitigation Score determination for prioritisation of Mitigations:

The process for generation of the Mitigation Score is illustrated in Figure 19, following the same steps used for the prioritisation of UCAs (section "Extension to Step 3: Prioritisation of UCAs"). The only key difference in this stage is the use of weighted factors in the calculation of the SAW score as follows:

$$SAW_{UCA} = w_{Type} \times Type + w_{Timee} \times Time + w_{Cost} \times Cost + w_{Likelihood} \times Likelihood\ of\ Occurrence$$

Where:

$w_{Type} = 0.4,\ w_{Likelihood} = 0.3\ ,\ w_{Timee} = 0.15,\ w_{Cost} = 0.15$

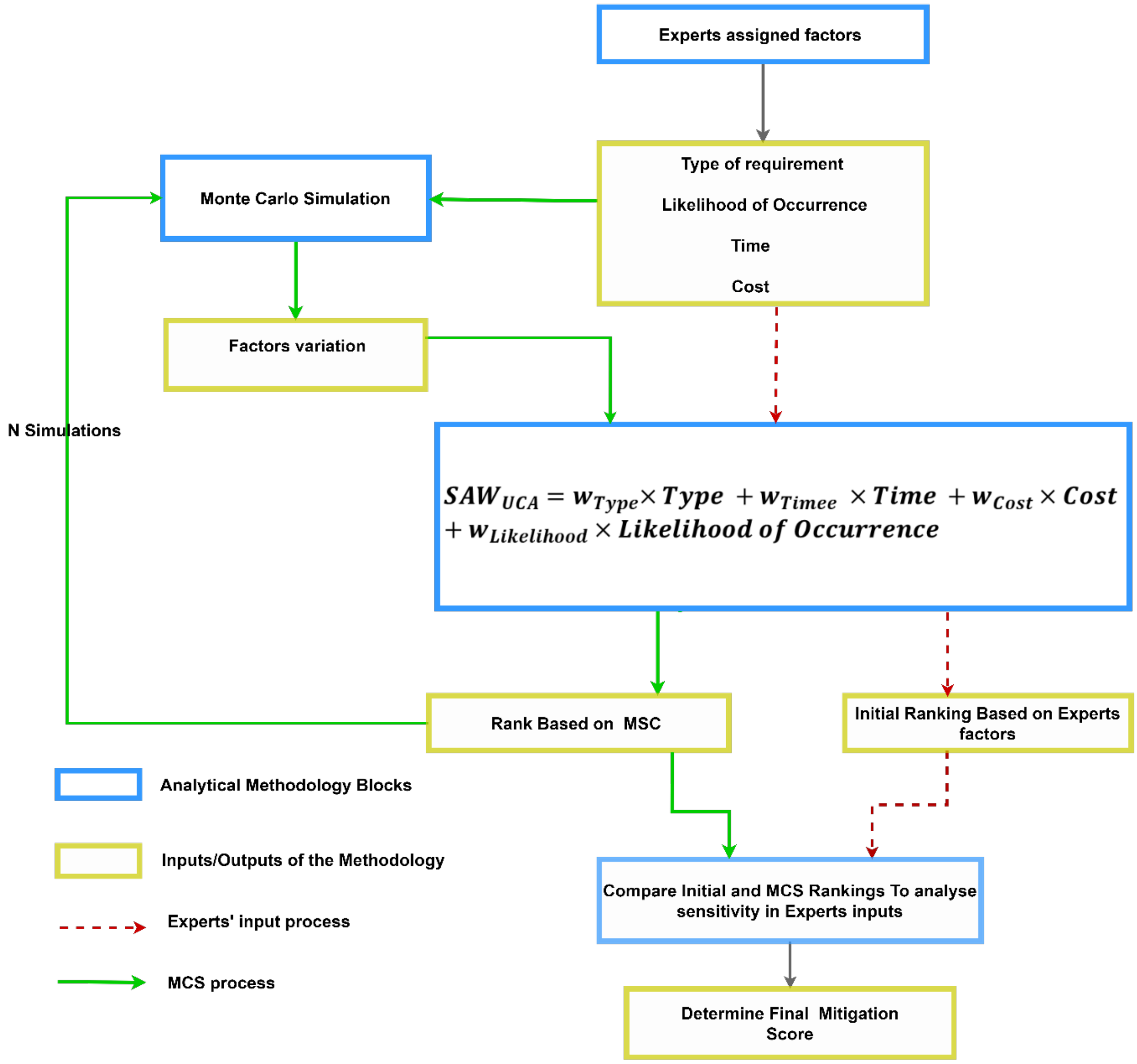
Experts assigned factors
Type of requirement
Likelihood of Occurrence
Time
Cost
Monte Carlo Simulation
Factors variation
N Simulations
$SAW_{UCA} = w_{Type} \times Type + w_{Timee} \times Time + w_{Cost} \times Cost + w_{Likelihood} \times Likelihood\ of\ Occurrence$
Rank Based on MSC
Initial Ranking Based on Experts factors
Analytical Methodology Blocks
Inputs/Outputs of the Methodology
Experts' input process
MCS process
Compare Initial and MCS Rankings To analyse sensitivity in Experts inputs
Determine Final Mitigation Score

Figure 19 Overview of the Mitigations Score calculation Process

Mitigation Prioritisation Matrix

The UCA Priority (along the Y axis) and Mitigation Score (along the X axis) were plotted to create a Mitigation Prioritisation Matrix (Matrix 3 in Figure 20). Mitigations were ranked P1 (highest priority) to P5 (lowest priority). Each cell in the matrix includes a color-coded scheme that refers to its priority – ‘P5'(green), 'P4’(yellow), ‘P3’(orange), ‘P2’(red) or ‘P1’ (dark red). The prioritisation of Mitigations is a phased approach with the SIF Matrix (Matrix 1 in Figure 20) and the UCA Prioritisation Matrix (Matrix 2 in Figure 20) from the UCA prioritisation concept, forming the basis for the creation of Mitigation Prioritisation Matrix(Matrix 3 in Figure 20). Each prioritised Mitigation inherits the priority of the UCA (based on the product of SIF and EJ) that it links to.

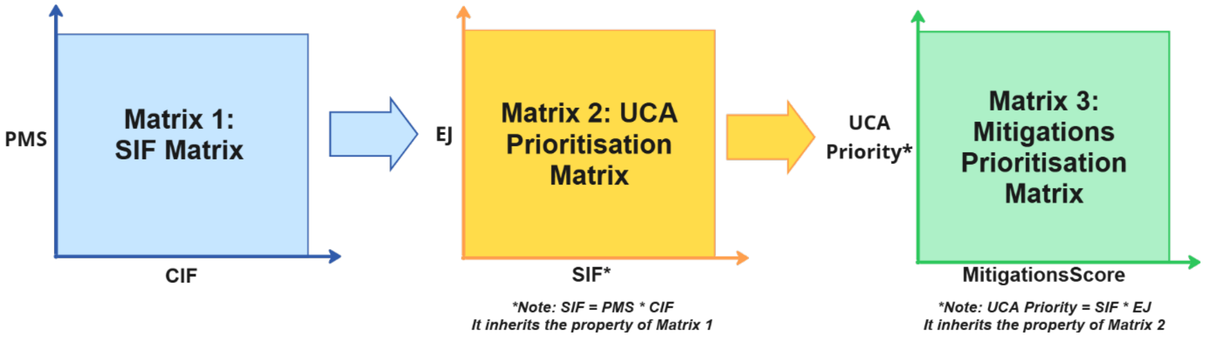

Figure 20 Overview of the concept of prioritisation of UCAs and Mitigations

Annex C: Comparison between Safety Analysis Methods

Traditional safety analysis methods such as Fault Tree Analysis (FTA), Event Tree Analysis (ETA), Failure Mode and Effects Analysis (FMEA), Hazard and Operability Study (HAZOP), and Bow-Tie Analysis (which are based on the Linear Chain of Events model, where accidents can be modeled as linear chains of events), have been widely used in aviation domain for decades. These methods provide a structured approach to identifying, assessing, and mitigating risks. However, when applying the same methods to complex systems with novel technologies like eVTOLs, the unsafe interactions between the stakeholders of the system may be overlooked.

As each stakeholder of the eVTOL operation is fulfilling their duties to achieve a common goal, which is to ensure the safe operation of eVTOL, these stakeholders can be treated as the ‘components’ of the system. A system-thinking approach can therefore be applied to objectively understand how these components can better interact with each other to achieve the system-level goal. To more effectively manage the Mitigations so that the most critical sets of Mitigations are prioritised, a prioritisation framework is also needed.

Comparison of various Safety Analysis Methods

A comparison of various safety analysis methods along with their advantages and disadvantages is presented in Table 27.

Method	Description	Pros	Cons
FMEA (Failure Mode and Effect Analysis)	FMEA identifies failure modes in system components and evaluates their effects and severity.	▪ It has systematic breakdown of potential failures at the component level ▪ It provides quantitative analyses for severity and probability	▪ It only focuses on component-level analyses, not system-level. ▪ It does not account for external influences ▪ It generates excessive results for complex systems.
FTA (Fault Tree Analysis)	It is a deductive method that models failure logic and identify causes of the system failure.	▪ It provides a clear graphical representation of failure logic. ▪ It supports quantitative analyses by assigning probabilities to failure modes.	▪ It only models failures, not unsafe interactions. ▪ It cannot handle emergent behaviours or feedback loops. ▪ It requires a well-defined failure scenario (not effective for new or unknown system).

Method	Description	Pros	Cons
ETA (Event Tree Analysis)	It is an inductive approach that starts from an initiating event and explores possible outcomes.	▪ It captures multiple failure paths. ▪ It is useful for emergency response planning	▪ It only models predefined scenarios and cannot predict emergent risks. ▪ It fails to capture system-level dependencies. ▪ The process is too complex when applying to large systems.
HAZOP (Hazard and Operability Study)	HAZOP uses guidewords to systematically identify hazards in system operations.	▪ It is great for process-based systems (chemical, nuclear, and industrial applications). ▪ It is flexible and can identify deviations that lead to hazards	▪ Quality of analysis varies based on participants' experience. ▪ It requires extensive effort for large-scale systems. ▪ It does not support quantitative analysis.
STPA (System-Theoretic Process Analysis)	STPA is a modern, systems-thinking approach to safety that analyses unsafe interactions on top of failures.	▪ It captures complex interactions and emergent behaviours. ▪ It is applicable for human and organisational factors. ▪ It can analyse novel systems where past failure data is unavailable. ▪ It covers functional safety and cyber-physical risks, making it useful for autonomous systems, eVTOLs, and digital aviation;	▪ It lacks standardised quantification.

Table 27 Comparison of various safety analysis methods

Appendices

Appendix A: Deliverables

1. Ranked List of Unsafe Control Actions: ranked_list_of_unsafe_control_actions.xlsx
2. List of Loss Scenarios: list_of_loss_scenarios.xlsx
3. Ranked list of Mitigations: ranked_list_of_mitigations.xlsx
4. Gap Review of Mitigations: gap_review_highprioritymitigations.xlsx

Appendix B: Abbreviations

Abbreviation	Description
AAM	Advanced Air Mobility
ANAC	National Civil Aviation Agency of Brazil
ANSP	Air Navigation Service Provider
AOC	Air Operator Certificate
ATC	Air Traffic Control
CA	Control Action
CAA	Civil Aviation Authority
CAP	Civil Aviation Publication
CAST	Causal Analysis based on Systems Theory
CAT	Commercial Air Transport
CF	Causal Factor
CIF	Controller Impact Factor
CPL	Commercial Pilot Licence
DAL	Design Assurance Level
EASA	European Union Aviation Safety Agency
EC	Electronic Conspicuity
EJ	Expert Judgement
ETA	Event Tree Analysis
eVSLG	eVTOL Safety Leadership Group
eVTOL	electric vertical take-off and landing
FAA	Federal Aviation Administration
FMEA	Failure Mode and Effects Analysis
FTA	Fault Tree Analysis
HAZOP	Hazard and operability study
ICAO	International Civil Aviation Organisation
MCS	Monte Carlo Simulation

NASA	National Aeronautics and Space Administration
NCC	Non-commercial operations with complex motor-powered aircraft
NCO	Non-Commercial Operations with other than complex motor-powered aircraft
NOTAM	Notice to Aviation
OEM	Original Equipment Manufacturer
PED	Portable electronic devices
PMS	Pre-mitigation Severity
RA(T)	Restricted Area (Temporary)
RF	Radio Frequency
RPM	Revolutions per minute
SAW	Simple Additive Weighting
SIF	Severity Impact Factor
SME	Subject Matter Expert
SoC	State of Charge
SPO	Specialised Operations
STAMP	System-Theoretic Accident Model and Processes
STPA	Systems- Theoretic Process Analysis
TAC	Temporary Aerodrome Creation
UCA	Unsafe Control Action
VMC	Visual Meteorological Conditions

List of Figures

List of Tables

References

Benhamlaoui, W. (2020). Comparative Study of STPA and Bowtie Methods: Case of Hazard Identification for Pipeline Transportation. Springer Nature.

Bensaci, C. (2020). STPA and Bowtie Risk Analysis Study for Centralized and Hierarchical Control Architectures Comparison. *Alexandria Engineering Journal*, 18.

(2023). *CAP 2576 - Understanding the downwash/outwash characteristics of eVTOL aircraft.* Civil Aviation Authority.

(2025). *CAP 3075 - Protecting the Future: Trials and Simulation of Downwash and Outwash for Helicopters and Powered Lift Aircraft.* Civil Aviation Authority.

Chatzimichailidou, M. M. (2018). A comparison of the Bow-Tie and STAMP approaches to reduce the risk of surgical instrument retention. *Risk Analysis*.

Chen, S. a. (2020). Identifying accident causes of driver-vehicle interactions using system theoretic process analysis (stpa). *IEEE International Conference on Systems, Man, and Cybernetics (SMC)*.

Chen, S. a. (2023). A System-Based Safety Assurance Framework for Human-Vehicle Interactions. *SAE Technical Paper*.

Chen, S. K. (2021). Analyzing national responses to COVID-19 pandemic using STPA. *Safety Science*.

Chen, S., Khastgir, S., & Jennings, P. (n.d.). A System-Based Safety Assurance Framework for Human-Vehicle Interactions. *WCX SAE World Congress Experience.* SAE.

Defense, U. D. (10 Feb 2000). *MIL-STD-882D Standard Practice for System Safety.*

Harkleroad, E. a. (2013). *Review of systems-theoretic process analysis (STPA) method and results to support NextGen concept assessment and validation.* ATC-427 MIT.

Harkleroad, E., Vela, A., Kuchar, J., & Barnett, B. a.-B. (n.d.). *Risk-based modeling to support nextgen concept assessment and validation.* Lincoln Laboratory, Lexington, MA, Project Report ATC-405.

Heinrich, H. W. (1941). Industrial Accident Prevention. A Scientific Approach.

Ishikawa, K. a. (1990). *Introduction to quality control.* Springer.

James Elizebeth, M. a. (2023). *Comparison of FTA and Stpa approaches: a brake-by-wire case study.*

Khastgir, S. a. (2021). Systems approach to creating test scenarios for automated driving systems. *Reliability engineering & system safety*.

Leveson, N. (2004). A new accident model for engineering safer systems. *Safety science*.

Leveson, N. G. (2016). *Engineering a safer world: Systems thinking applied to safety.* MIT Press.

Leveson, N. G. (2018). *STPA Handbook.* MIT press.

Liu, T. a. (n.d.). Safety analysis of Civil aviation Flight and UAV Operation based on STAMP/STPA. *E3S Web of Conferences.*

McLeod, R. W. (2018). Bowtie Analysis as a prospective risk assessment technique in primary healthcare. *Policy and Practice in Health and Safety*.

Merrett, H. (2019). Comparison of STPA and Bow-tie Method Outcomes in the Development and Testing of an Automated Water Quality Management System. *MATEC Web of Conferences.*

Merrett, H. C. (2019). Comparison of STPA and bow-tie method outcomes in the development and testing of an automated water quality management system. MATEC Web of Conferences.

Merrett, H. C. (2019). Comparison of STPA and bow-tie method outcomes in the development and testing of an automated water quality management system. *MATEC Web of Conferences* (p. 18). MATEC Web of Conferences.

Natarajan, D. (2017). *ISO 9001 Quality management systems.* Springer.

Owens, B. D. (2008). Application of a safety-driven design methodology to an outer planet exploration mission. *IEEE aerospace conference*.

Qi, Y. a. (2025). Safety analysis in the era of large language models: a case study of STPA using ChatGPT. *Machine Learning with Applications*.

Rasmussen, J. (1997). Risk management in a dynamic society: a modelling problem. *Safety Science*.

Reason, J. (2000). Human error: models and management. *Bmj*.

Rose, E. J. (2023). Monte Carlo sensitivity analysis for unmeasured confounding in dynamic treatment regimes. *Biometrical Journal*.

Silvis-Cividjian, N. a. (2020). Using a systems-theoretic approach to analyze safety in radiation therapy-first steps and lessons learned. *Safety science*.

smith2012mil. (2012). *MIL-STD-882E.* Department of Defence.

Stallings, W. (1976). *Gerald M. Weinberg. An introduction to general systems thinking. New York: Wiley, 1975, 279 pp.*

Stanton, N. A. (2019). Systems Theoretic Accident Model and Process (STAMP) applied to a Royal Navy Hawk jet missile simulation exercise. *Safety science*.

Sulaman, S. M. (2019). Comparison of the FMEA and STPA safety analysis methods-a case study. *Software quality journal*.

Sultana, S. a. (2019). Hazard analysis: Application of STPA to ship-to-ship transfer of LNG. *Journal of Loss Prevention in the Process Industries*.

Sun, L. a.-F. (2022). Comparison of the HAZOP, FMEA, FRAM, and STPA methods for the hazard analysis of automatic emergency brake systems. *ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems, Part B: Mechanical Engineering*.

Svedung, I. a. (2002). Graphic representation of accidentscenarios: mapping system structure and the causation of accidents. *Safety science*.

Thomas, J. P., & Van Houdt, J. G. (2024). *Evaluation of System-Theoretic Process Analysis (STPA) for Improving Aviation Safety -DOT/FAA/TC-24/16.* Center for Aviation Safety, Advanced Engineering Services.