Safety Assurance Report on Draft EUROCONTROL Specifications for Military UAV as OAT Outside Segregated Airspace

Functional Hazard Assessment/Preliminary System Safety Assessment (FHA/PSSA) Report for Military UAV as OAT Outside Segregated Airspace

Reference	P05005.10.4
Date:	23 August 2005
Issue:	v1.0

Prepared by:

Joanne Stoker
Alan Simpson

Checked by:

Jason Denness

Authorised by:

Mike Sotirakos

Distribution:	EUROCONTROL	Ebeni
	Mike Strong	Joanne Stoker
	Trond Bakken	Alan Simpson
	Bernd Tiemeyer	Project File

Derek Fowler

© Copyright

Configuration Control

Issue	Date	Comments
v0.1	27 July 2005	Draft Issue
v0.2	29 July 2005	Provisional Issue following internal Ebeni review for LM Stasys review and visibility to EUROCONTROL
v1.0	23 August 2005	Updated issue incorporating LM Stasys and EUROCNTROL comments

Table of Contents

TABLE OF FIGURES

TABLE OF TABLES

1 Introduction

1.1 Background

To exploit fully the unique operational capabilities of current and future Unmanned Aerial Vehicles (UAV), and to undertake training necessary for the safe conduct of UAV operations, European military authorities require UAVs to be able to access all classes of airspace and to be able to operate across national borders and FIR/UIR boundaries. At the moment most military UAVs are restricted to segregated airspace or they are flown under special arrangements over the sea. On some occasions, operations in an extremely limiting environment are permitted outside segregated airspace.

To address this, the UAV Operational Air Traffic (OAT) Task Force (TF), reporting to the Military Team (MILT) has started to develop a specification for the use of UAVs outside of segregated airspace, with an emphasis on OAT. The TF therefore considered those specifications it felt were necessary to safely integrate UAVs with other airspace users, without seeking to address related technical issues. The TF is approaching UAV System operations from the ATM viewpoint rather than being constrained by possible limitations in current UAV System capability which is for industry to address. Notwithstanding, particular attention has been paid to collision avoidance, sense and avoid, and separation minima.

The TF has identified 26 draft EUROCONTROL specifications [1]. One of the key principles followed by the TF was that UAV operations should not increase the risk to other airspace users. Verification of this principle for the Draft Specification is the primary purpose of this safety assurance, which together provides support to the States in developing their own national regulations.

The EUROCONTROL Safety Assessment Methodology (SAM) [2] identifies specific techniques for the identification of hazards and assessment of their significance. SAM also highlight the process to be followed to document the safety analysis, hence a Functional Hazard Assessment and

Preliminary System Safety Assessment (FHA /PSSA) process, as outlined within SAM, has been adopted to validate the UAV specifications.

1.2 Aim

This FHA/PSSA provides an independent assessment of the hazards related to operating Military UAVs as OAT in non-segregated airspace in support of the derivation of high level safety requirements for incorporation in the Draft UAV-OAT Specification [1].

The aim of this FHA/PSSA is derived from the top level safety argument, which implies a relative safety argument based on the following top-level claim:

- Military UAV-OAT operations in non-segregated airspace will be ***acceptably safe***;
- where ***acceptably safe*** is defined as ‘risks’ to other airspace users are:
  - no greater than for military manned OAT in non-segregated airspace; and
  - reduced to As Far As Reasonably Practicable (AFARP), as required by ESARR 3 [10] and EATMP Safety Policy [11].

The initial step in addressing the above claim is to specify safety requirements such that, subject to complete and correct implementation, Military UAV operations in non-segregated airspace are acceptably safe.

The aim of the FHA/PSSA is therefore to derive a set of high level safety requirements such that, if satisfied, an ***acceptable level of safety*** can be demonstrated.

1.3 Scope

This report presents the FHA/PSSA for Military UAV-OAT operations in non-segregated airspace, up to the derivation of high level safety requirements, for incorporation into the Draft UAV-OAT Specification [1].

The Military UAV-OAT safety argument and safety requirements will also be documented within a summary report.

This FHA/PSSA incorporates the results of the safety analysis work to document the high level safety requirements to support the on-going work of the UAV-OAT Task Force.

1.4 Structure

This FHA/PSSA Report is structured as follows:

Section 1 Introduction – presents the scope and purpose of the report.

Section 2 Functional Hazard Assessment/Preliminary System Safety Assessment Overview – documents the objectives of the FHA/PSSA along with the process and the hazard and risk assessment methodology.

Section 3 System Definition – provides an overview of the system under consideration and the scope of the analysis.

Section 4 FHA/PSSA Results – documents the results of the hazard identification, causal and consequence analysis for Military UAV as OAT in non-segregated airspace.

Section 5 Safety Requirements – presents the safety requirements for Military UAV as OAT in non-segregated airspace.

Section 6 Conclusions and Identified Safety Issues – presents the conclusions and identified safety issues of the FHA/PSSA.

A table of abbreviations and acronyms used throughout this report is provided in Appendix G.

This document should be read in colour for ease of reading.

2 Functional Hazard Assessment/Preliminary System Safety Assessment Overview

2.1 Introduction

The EUROCONTROL ANS Safety Assessment Methodology [2] defines the objectives of a FHA as:

> *"a top-down iterative process, initiated at the beginning of the development or modification of an Air Navigation System. The objective of the FHA process is to determine: how safe does the system need to be?*
>
> *The process identifies potential functional failures modes and hazards. It assesses the consequences of their occurrences on the safety of operations, including aircraft operations, within a specified operational environment.*
>
> *The FHA process specifies overall Safety Objectives of the system, i.e. specifies the safety level to be achieved by the system."*

The PSSA extends the hazard assessment to derive safety requirements for the system that are necessary and sufficient to satisfy the acceptance criteria for safety. Given that the Military UAV-OAT operations safety argument requires a relative demonstration of risk improvement, the specification of absolute Safety Objectives is not performed for existing hazards, i.e. requirements have been expressed qualitatively in terms of 'at least as good as for manned aircraft' rather than quantitatively in terms of achievement of a 'probability of occurrence of less than 1 x 10^{-6} per UAV flight hour'.

2.2 FHA/PSSA Objectives

The overall objectives[1] for the FHA/PSSA as defined in sections 1.2 and 2.1 are further refined to specific task objectives as discussed in the following list. Some of the objectives were addressed as part of the pre-

[1] The input objectives of the FHA/PSSA have been repeated here for traceability and completeness.

workshop and workshop activities and others as part of the post-workshop FHA/PSSA activities. The results of these activities are captured in this report. The detailed objectives were to:

- review and agree the overarching UAV Safety Argument Strategy;
- verify the scope and boundaries of the analysis being undertaken;
- validate the Functional and Logical Architecture Models and identify the variations (if needed) to the models under different situations, e.g. IFR/VFR, Night/Day and differing levels of Air Traffic Services (ATS);
- identify the hazards as applicable to the current Military Manned OAT operations in non-segregated airspace (without-UAV) and proposed Military UAV OAT operations in non-segregated airspace (with-UAV);
- identify, for both without-UAV and with-UAV situations, the possible consequences of each hazard, taking into account the available mitigations, using Event Tree Analysis;
- identify the possible causes of each hazard, using Fault Tree Analysis;
- discuss the potential safety issues with the implementation of Draft UAV-OAT Specifications and Safety Requirements.

All of the objectives stated above have been satisfied.

2.3 FHA/PSSA Process

This FHA/PSSA was performed in order to support a relative safety argument. This analysis aimed to derive a necessary and sufficient set of safety requirements for Military UAV-OAT operations in non-segregated airspace.

The diagram presented in Appendix J shows the relationship between the essential components of the FHA/PSSA process. The diagram also provides reference to the appropriate section within this report that describes the components.

The first step in performing the FHA/PSSA was to establish the scope and boundary of the system, understanding that the system covers all aspects of the ATM environment including people, procedures and equipment. In the context of the defined scope and system boundary, the analysis has focused specifically on the identification of:

- potential accidents and incidents;
- hazards that could lead to those accidents;
- the potential causes and consequences of those hazards;
- necessary risk reduction measures and resultant safety requirements.

The FHA/PSSA process began with the construction of a number of models. Given the requirement to present a relative safety argument, it was important to fully appreciate the current situation with no UAVs (referred to as 'without-UAV') as compared to the proposed situation with UAVs flying in non-segregated airspace (referred to as 'with-UAV'), as well as all transition states from 'without-UAV' to 'with-UAV'. Thus a number of models were constructed to describe the essential differences between the situations and to aid identification of potential hazards that required mitigation. See section 3.2.2 for more detail. These models were defined in sufficient detail to support the objectives of the FHA/PSSA; mainly, the derivation of safety requirements commensurate with the level of detail in the Draft UAV-OAT Specifications.

The models along with the proposed scope, boundary and assumptions for the analysis were presented at a FHA/PSSA Workshop for validation and verification by domain experts. A hazard identification activity was also carried out as part of the FHA/PSSA Workshop.

A number of issues, statements and discussion points were raised at the FHA/PSSA Workshop which were minuted and documented in [3]. A number of these points have been used to justify or substantiate analysis decisions; these are referred to specifically throughout this document as originating from the workshop participants.

The output from the FHA/PSSA Workshop was then taken and used to perform a more detailed analysis which included the construction of causal models using Fault Trees and consequence models using Event Trees. These hazard models were subsequently used to derive the safety requirements for Military UAV-OAT operations in non-segregated airspace.

2.4 FHA/PSSA Workshop

A UAV FHA/PSSA Workshop was held at the Crowne Plaza, Brussels Airport Hotel on Wednesday 01 June and Thursday 02 June 2005. Notes from the workshop are recorded in [3]. The Agenda for the FHA/PSSA Workshop and a list of participants is provided in Appendix A.

With respect to the above objectives, the FHA/PSSA Workshop achieved the following:

- Reviewed and agreed the overarching UAV Safety Argument Strategy.
- Verified the scope and boundaries of the analysis being undertaken.
- Validated the Scenario, Functional, Logical Architecture, and Detailed Logical Models and identified the variations to the models under each operational perspective for both “with-UAV” and “without-UAV” situations.

The remaining objectives are all captured as part of the FHA/PSSA results in section 4.

3 System Definition and Scope of Analysis

3.1 Overview

The concept of operating Military UAVs as OAT in non-segregated airspace is primarily expected to be transparent to the ATM environment. There are obvious differences between manned and unmanned Air Vehicles but in principle UAVs should operate to the same rules of the air and procedures that apply to manned OAT. The safety of other airspace users depends on UAV system operations achieving at least an equivalent level of safety to manned OAT. Assessing the safety of the without-UAVs and the with-UAV situations as defined in section 2.3. For the purpose of this analysis the level of detail used to define these concepts is sufficient only to support the derivation of safety requirements for inclusion in the Draft UAV-OAT Specifications. Note that in the current without-UAV situation there are no European-wide rules and procedures for OAT operations, although this is being addressed by the Harmonisation of OAT Rules and its GAT Interface (HORGI) as discussed in section 3.1.4.

There are three main components of ATM, defined within the Draft ATM Operational Concept Document [7] endorsed at ANC/11 in September 2003;

- Strategic Conflict Management,
- Separation Provision, and
- Collision Avoidance.

Strategic Conflict Management encapsulates all pre-flight planning activities that take place to ensure demand, capacity and conflicts are managed prior to the real time situation. The Strategic Conflict Management component is not considered within this safety assurance activity. Figure 1 below shows the principle interactions between the Separation Provision, Collision Avoidance components and the Airspace. Note that [7] also states that any Collision Avoidance System should be separate from but compatible with the Separation Provision component.

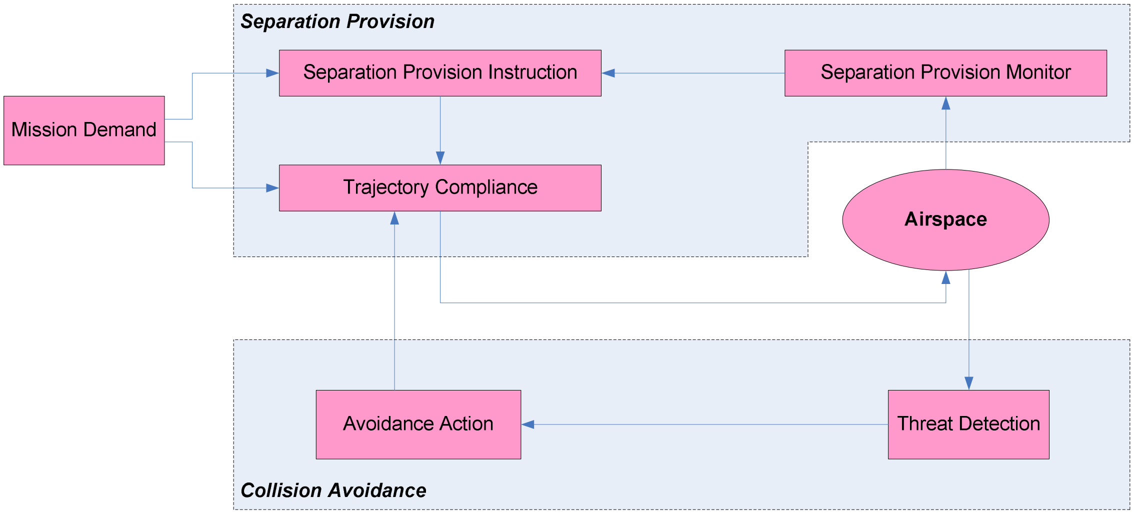


Figure 1 – High Level Functional Model

The use of these terms is important within this analysis and has thus been defined in the following sections.

3.1.1 Separation Provision Component

Separation provision is the tactical process of keeping aircraft away from other airspace users and obstacles by at least the appropriate separation minimum. Depending upon the type of airspace and, where applicable the ATC service being provided, separation provision can be performed by ATC or by the Pilot In Command. Where ATC is responsible for providing Separation Provision, the Separation Provision Monitoring and Demand for an aircraft are provided by an Air Traffic Controller and the pilot is responsible for Trajectory Compliance. Where the pilot is responsible for Separation Provision, all these functions are performed by the pilot.

Under VFR in certain types of airspace, there is no specified minimum separation distance and the pilot of, for example a manned OAT aircraft arranges his trajectory using airborne radar and/or visual means to separate his flight path from other air platforms. In these scenarios for UAV OAT operations the UAV OAT Task Force defined in the Draft UAV OAT Specifications [1] a minimum separation distance of 500ft has been included in the Military UAV OAT Specifications. The term Separation Provision should therefore be taken to include the actions necessary to provide physical separation between a UAV and other air users of at least 500ft, where no separation minima is currently defined for manned OAT operations.

3.1.2 Collision Avoidance Component

For the purpose of this analysis the Collision Avoidance component is separated into Pilot and Collision Avoidance systems. Current Military OAT aircraft may be fitted with Collision Avoidance systems such as TCAS II or elements thereof such as Secondary Surveillance Radar Transponders. Collision Avoidance systems are designed to activate when separation provision has been compromised, although ATC can instigate Collision Avoidance action from a pilot, this mechanism would not be available to an autonomous UAV.

SRC Policy Document 2 [8] states that Collision Avoidance systems (referred to as Safety Nets[2]) are not part of Separation Provision so must not be included in determining the acceptable level of safety required for Separation Provision. However, the Collision Avoidance performed by a pilot of a manned aircraft must be performed to an equivalent level of safety by the UAV whether piloted or autonomous.

The SRC Policy Document statement implies that UAVs must provide an equivalent level of interaction with the Separation Provision function as provided by pilots. Furthermore the UAV Separation Provision System must maintain the level of safety (with respect to the scope of ESARR 4) without the need for a Safety Net. This implies that UAVs will need to provide independence between Separation Provision and Collision Avoidance systems. This issue is captured by Safety Requirement MSF-03, but further consideration should be given to reviewing SRC Policy Document 2 in light of UAV operations, especially when operating autonomously (**Safety Issue 8**).

[2] Safety nets are engineered systems, either airborne or ground-based, which are designed and operated for the purpose of collision avoidance. This can apply to collisions between aircraft, or between aircraft and other objects, including the ground.

Accordingly it is not within the scope of this report to consider the effectiveness of the Pilot's Visual Acquisition process although it is recognised that replicating this process within a UAVs Sense and Avoid capability is an open implementation issue. See **Safety Issue 6**.

COMMENT

Yet, in controlled airspace when you consider that the Pilot in Command is responsible for Separation Provision Compliance and Collision avoidance (which could be supported by TCAS for example) there is a clear common component. In uncontrolled airspace the Pilot is performing BOTH Separation Provision (SP) and Collision Avoidance (CA). Does the pilot really distinguish between the two functions? The Draft Specifications refer to separation minima for collision avoidance and there does not seem to be any distinction made between SP and CA in this respect.

However, it seems that a distinction (level of independence) between SP and CA for UAVs would provide a safety benefit. This issue requires further discussion with EUROCONTROL.

3.1.3 Operation of UAV Systems

UAV Systems encapsulate not only the UAV itself, but the entirety of systems, people and procedures involved in the launch, control and recovery of UAVs. To establish the potential differences in manned and unmanned operations, it is important to understand the specific characteristics of UAV Systems that are potentially applicable to operations in non-segregated airspace. The UAV System characteristics model shown in Figure 2 captures a representation of key UAV System characteristics considered during the FHA/PSSA Workshop, as relevant to this safety analysis:

- A principle characteristic, as illustrated in the diagram below, is that the means of Air Vehicle Control is functionally separate from the UAV. The Pilot in Command (PIC) of the UAV will be remote from the UAV either on the ground, on another aircraft or on a ship. The PIC maintains control of the UAV through a UAV Control System (UCS) and a UAV Control Link (UCL). The details of the UCS and UCL are not considered further in this analysis.

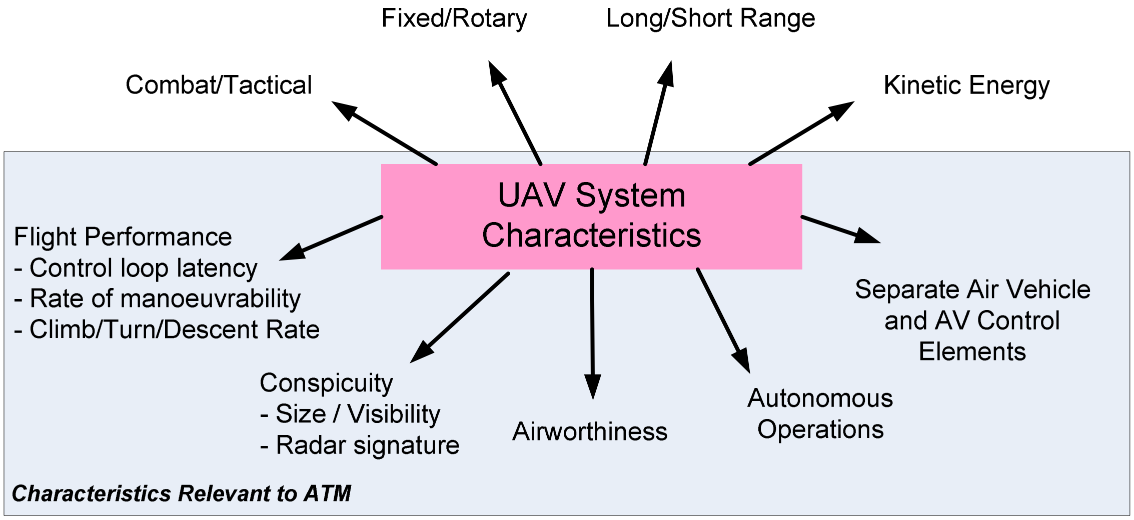


Figure 2 – UAV System Characteristics Model

- Conspicuity – the visibility of the UAV to other airspace users is an important component in the Collision Avoidance component as well as when Separation Provision is the responsibility of the PIC. This could be an issue for UAVs that are smaller than Manned OAT, or UAVs that present a poor signature for Primary Surveillance Radar.

- Autonomous Operations – emergency operations whereby a UAV is operating autonomously from any human control is a fundamental consideration throughout this analysis as it is a key difference between Manned and Unmanned operations. Autonomous UAV operations that are planned or deliberate e.g. for covert mission reasons, are not considered in this assessment except where the action is part of an emergency operation. In all cases, appropriate emergency procedures need to be in place for safe recovery of the UAV itself.

- Airworthiness – the Airworthiness Certification of a UAV is outside scope of this analysis. However, it is assumed within the analysis that UAVs will be fitted with certified equipment equivalent to that required for manned operation in the intended non-segregated airspace, unless otherwise specifically stated.

- Flight Performance – the manoeuvrability of a UAV is important to understand. Currently, Air Traffic Controllers are required to understand flight performance characteristics of the types of aircraft that come under their control and provide separation provision instructions based on this understanding. This requirement for understanding will also need to apply to unmanned operations to ensure ATC instructions can be implemented.

3.1.4 Harmonisation of OAT Rules and GAT Interface

Within Europe today for current MIL OAT operations, there is no harmonisation of OAT rules. OAT structures, rules and handling, are currently still strictly national. To maintain and enhance facilitation of military requirements and operational flexibility for military and civil airspace users within the Single European Sky, EUROCONTROL has identified that the design of a pan-European OAT System is essential.

The following three work packages have been identified within EUROCONTROL to move OAT harmonisation forward, these include:

- Harmonisation of OAT Rules and its GAT Interface (HORGI);

- development of pan-European OAT Route Systems;

- development of Options and Requirements for Cross-Border Operations (CBO) and Cross-Border Areas (CBA), including Temporary Segregated Airspace/Temporary Reserved Airspace (TSA/TRA) sharing.

The HORGI task will facilitate harmonisation and standardisation of all ATM-relevant OAT rules, regulations and procedures within the EUROCONTROL Member States for OAT-IFR Flights and all related ANSP

OAT-handling, with particular emphasis on OAT border crossing. The HORGI work is currently in progress and is being conducted by the HORGI Task Force.

A Draft set of EUROCONTROL Region Rules for OAT has been compiled [6] and is currently under review by the HORGI Task Force and the Military Unit. As such, the requirements derived for the UAV Specification must agree with the Draft OAT Rules.

3.2 Defining the System for the FHA/PSSA Activity

Prior to beginning the FHA/PSSA activity it was important to understand and describe the differences between the "without-UAV" and "with-UAV" situations, to structure the analysis and support the relative assessment of risk. The current "without-UAV" situation and the differences from the "with-UAV" situation were captured and defined in a series of functional and logical models and a scenario model for typical OAT operations.

The scope of the safety assessment is thus determined by the following:

- the Draft UAV-OAT Specification [1], see section 3.2.1;
- a number of operational perspectives, see section 3.2.2;
- a series of identified scoping assumptions, see section 3.2.3.

The scenario, functional and logical models are described in section 3.3.

3.2.1 Draft UAV Specifications

The Draft UAV Specifications provide the basis for the safety assessment activity and were compiled by the UAV-OAT Task Force which comprises EUROCONTROL Staff, national military experts and representatives from other interested organisations. The Task Force agreed that EUROCONTROL Specifications were the most appropriate category, rather than Rules, which would be considered binding. The Specifications have voluntary status and may be developed by other organisations other than EUROCONTROL. Individual States are therefore free to decide whether or not to incorporate the EUROCONTROL UAV Specifications into their own national regulations.

The Draft UAV Specifications contain 26 requirements relating to the following topics:

- ATM Categorisation of UAV Operations;
- Flights across International Borders and across FIR/UIR Boundaries;
- Chase Aircraft;
- Modes of Operation;
- Flight Rules;
- Right-of-way;
- Separation from other airspace users;
- Sense and avoid;
- Separation minima;
- Airfield Operations;
- Emergency Procedures;
- Interface with ATC;
- Meteorology;
- OAT CNS Equipment Requirements.

The paper itself briefly considers non-related ATM matters, however does not aim to address aspects of UAV operations that are outside the EUROCONTROL sphere of control e.g. airworthiness, certification, system security, licensing of personnel, legal liabilities etc.

3.2.2 Operational Perspectives

Consideration of Military UAV-OAT operations in non-segregated airspace can be understood from a number of operational perspectives. The perspectives help identify all the changes between the "without-UAV" situation compared to the "with-UAV" situation. At the highest level as discussed in the overview in section 3.1 the operational perspectives are dictated by who has responsibility for performing the ATM concept functions, mainly:

- Who has responsibility for Separation Provision;
  - PIC or ATCO (dependent on Airspace Class, IFR or VFR);
  - UAV or ATCO during emergency situations (e.g. loss of the UAV Control Link);
- Who has responsibility for Collision Avoidance;
  - PIC or UAV or shared between the PIC and UAV.

3.2.3 Scoping Statements

The following scoping statements have been made to further support the safety assurance activity:

1. Only Military OAT in non-segregated airspace is considered in this safety assessment.
2. Current Manned Military OAT operations in non-segregated airspace are acceptably safe.
3. UAV Specifications will accord with the work of the Harmonisation of OAT Rules and GAT Interface (HORGI), see **Safety Issue 3**.
4. UAV Systems will be operating without Chase Aircraft[3].

[3] Although the Draft Specifications include reference to Chase aircraft, this is in the specific context of military ATC procedures relating to the separation of aircraft formations from other traffic and is not relevant for the purposes of this study.

5. The following are outside the scope of this assessment:

    a. Airworthiness of the UAV system (air and ground element);

    b. Operations other than peace time[4] or those in designated areas of military armed conflict delineated through the use of military Airspace Control Means (ACM) rather than national ATM procedures.

    c. Training qualifications of personnel;

    d. Availability and integrity of aeronautical data.

6. The safety assurance process excludes consideration of legal liabilities.

7. The safety assurance process excludes model aircraft, i.e. only considers ATM relevant UAVs.

8. The safety assurance process excludes UAV planned data link loss activities.

9. The safety assurance process does not consider security issues.

10. Mission aspects of a UAV flight undertaken in segregated airspace are considered outside the scope of the safety assurance activity.

3.2.4 Assumptions

The following assumptions have also been made to further scope and support the safety assurance activity:

1. The ICAO Strategic Conflict Function is common to both the “without” and “with” UAV situations.

2. The analysis assumes that a PIC is only responsible for one UAV[5].

[4] Excludes transit areas.

[5] If the PIC is responsible for more than one UAV, consideration needs to be given to the impact on the likelihood or effectiveness of any PIC mitigating action

3.3 Manned and Unmanned OAT System Models

The following models have been constructed based on the defined scope of the analysis for each of the operational perspectives and for the “without-UAV” and “with-UAV” situations as applicable:

- Scenario Model – captures all likely ATM environments and situations in which Military UAV-OAT aircraft may be required to operate;
- Functional Models – the functional models are a further decomposition of the high level functional model presented in Figure 1 and are derived from the components defined within the ICAO Strategic Conflict Model;
- Logical Architecture Models – derived from understanding the interactions between key stakeholders and logical entities of the system;
- Next Level Logical Models – decomposition of the logical architecture models, specifically for the PIC and Autonomous UAV situations.

The analysis has not considered the changes at the detailed Physical Architecture Level as this would introduce implementation requirements which go beyond the level of the Draft UAV Specification.

3.3.1 Scenario Model

The scenario model is presented in two parts as shown in Appendix B.1 and aims to capture all likely ATM environments in which Military UAV-OAT aircraft may be required to operate. The model encapsulates pre-flight planning, launch of the UAV, VFR operations, crossing FIR and UIR boundaries, emergency operations, approach, landing and any post landing actions.

All the scenarios identified within this model have been considered throughout the safety analysis activity documented in section 4.

3.3.2 Functional Models

The high level functional model presented in section 3.1 presents a very high level view of operations in airspace both with and without ATC responsible for separation provision. This model has been decomposed into two further detailed functional models to capture the following states:

- Functional Model with ATC Responsible for Separation Provision is shown in Appendix B.2;
- Functional Model with PIC Responsible for Separation Provision is shown in Appendix B.3.

The functions within the models are defined below:

- Separation Provision – see section 3.1.1;
- Collision Avoidance – see section 3.1.2;
- Co-ordination and Transfer – is the process by which flights which are being provided with an ATC service are transferred from one ATC unit (transferring unit) to the next (receiving unit) in a manner designed to ensure complete safety. It is a standard procedure that the passage of each flight across the boundary of the areas of responsibility of the two units is **co-ordinated** between them beforehand and that the control of the flight is **transferred** when it is at, or adjacent to, the boundary. Additionally, co-ordination between ATS Units or individual controllers may be necessary to agree a course of action to achieve deconfliction or make use of reduced separation standards.
- Information Services – e.g. Information Services are services provided for the collection and dissemination of information needed to ensure the safety, regularity and efficiency of air navigation. Such information includes, but is not limited to, the following:
    - Meteorological data;

- Aeronautical Information Services (such as Charts and Notice To Airmen (NOTAM);
- Other Flight Information Services.

The key difference between the two models is the shift in responsibility for the separation provision function between ATC for certain types of airspace when flying under Instrument Flight Rules (IFR) and the PIC for certain types of airspace when flying under Visual Flight Rules (VFR). The functional models are the same for both the without-UAV situation and the with-UAV situation.

There are also a number of transition states between the two situations that require consideration throughout the safety analysis, specifically:

- ATC Unit to adjacent ATC Unit (known as Co-ordination and Transfer);
- Change in responsibility for Separation Provision between ATC Unit and PIC.

3.3.3 Logical Architecture Models

The logical architecture models for the without-UAV and with-UAV situations are shown in Appendix B.4 and B.5.

The logical architecture models identify generic entities considered part of Military OAT operations in non-segregated airspace. The diagrams show, for both manned and unmanned operations, the relevant communication points and data flows.

Figure 10 within Appendix B presents the diagram for Military OAT Manned Operations in non-segregated airspace. The diagram shows the communication paths between two manned aircraft and the link to ground ATM systems, including ATC navigational and communication equipment.

Figure 11 within Appendix B presents the diagram for Military UAV-OAT Operations in non-segregated airspace. This diagram highlights the different communication paths between a UAV, the PIC and ATC. All other communications paths remain as for manned operations.

3.3.4 Next Level Logical Models

Two further more detailed logical models are presented within Appendix B as follows:

- Next Level Logical Model – PIC, see Appendix B.6;
- Next Level Logical Model – Autonomous UAV, see Appendix B.7.

These models have been constructed to highlight the differences between a Piloted UAV and a UAV flying autonomously. These models have been constructed due to the need to consider autonomous UAV operations, which may be required due to UAV control link loss and thus appropriate safety requirements need to be adequately defined.

4 FHA/PSSA Results

4.1 Overview

In order to establish the relative change in risk as a result of introducing Military UAV-OAT operations in non-segregated airspace, the initial step in the analysis was to identify the hazards at a common boundary point for the "without-UAV" and "with-UAV" scenarios. It was then necessary to establish if these hazards were common to both situations and whether there were any new hazards in the "with UAV" situation.

The hazards were initially identified during the FHA/PSSA by examining potential failure scenarios associated with the functions depicted in the functional models as described in section 4.2. During the workshop it was noted that the Collision Avoidance component should be given further consideration as part of the Post Workshop FHA/PSSA activities. This resulted in the production of Figure 1 to help clarify the relationship between them, as discussed in section 4.4.

The next step in the analysis was to assess the consequences and causes associated with each hazard for both the without-UAV and with-UAV situations. The relative impact of the change was then assessed with respect to risk. The causes and consequences of each of the identified hazards were initially assessed during the Workshop and the results were used to construct the Consequence and Causal models (which form each side of the Bow-tie model) for each of the hazards as described in sections 4.5 and 4.6, respectively.

The resultant cause and consequence models were then used to derive the safety requirements for Military UAV-OAT operations in non-segregated airspace which are necessary to ensure that the relevant risks are reduced as far as reasonably practicable (see section 5).

4.2 Hazard Identification Approach

To identify the hazards related to each of the functions a series of functional failure guidewords was applied to each function and considered in more detail, as follows:

- **Loss** – complete negation of an intention. No part of the intention is achieved and nothing else happens, i.e. ATC inability to provide separation provision.

- **Error** – any action that is undesirable regardless of cause, e.g. incorrect response to ATC instruction, partial response to ATC instruction or unintentional actions.

- **Intentional deviation** – a different action than that intended occurs as a result of an external input i.e. ATC instruction ignored (e.g. due to Traffic Collision Avoidance System (TCAS) Resolution Advisory (RA)).

- **Too early** – an action occurs earlier than expected either relative to UTC, order or sequence.

- **Too late** – an action occurs later than expected whether relative to UTC, order or sequence.

- **Other** (completeness check).

The potential hazards were thus derived by assessing each of these in turn and determining what sort of loss, error etc. could potentially lead to unsafe consequences. Based on application of the functional failure guidewords to the high level functional model in Figure 1, the following high level hazards were identified:

- Loss of Separation Provision;

- Error in Separation Provision;

- Delayed Separation Provision;

- Intentional Deviation from Separation Provision Instruction.

The preliminary hazards identified during the initial “brainstorm” activity at the UAV FHA/PSSA Workshop are presented in Table 1 below, and were identified using the functional models presented in Appendix B.2 and B.3. During the workshop cause/consequence analysis, the hazards were discussed in more detail and rationalised, resulting in a number of "hazards" being re-defined.

Each of the hazards identified at the UAV FHA/PSSA Workshop has been grouped with one of the high-level hazards listed above. This is discussed in more detail in the causal analysis section, 4.6.

UAV Workshop Hazard No.	UAV Workshop Hazard Title	Discussion
Loss of Separation Provision		
HAZ001	Inability to comply with separation provision instruction from ATC	
HAZ006	Loss of separation provision from ATC	
HAZ008	Loss of separation provision from Pilot in Command	
Separation Provision error		
HAZ002	Incorrect response to separation provision instruction from ATC	
HAZ007	ATC separation provision error	
HAZ009	Pilot in Command separation provision error	
Delayed Separation Provision		
HAZ004	Delayed response to separation provision instruction from ATC	
HAZ010	Pilot in Command separation provision too late	
Intentional Deviation from Separation Provision Instruction		
HAZ003	Intentional deviation from separation provision instruction from ATC	
Additional UAV Workshop Hazards		
HAZ005	Collision avoidance manoeuvre when not required	Hazard 5 was considered a cause of Hazard 3 during the UAV Workshop, and is therefore considered within the causal analysis of HAZ003

UAV Workshop Hazard No.	UAV Workshop Hazard Title	Discussion
HAZ011	Loss of co-ordination and transfer	Hazard 11 was considered a cause of Hazard 6 during the UAV Workshop, and is therefore considered within the causal analysis of HAZ006
HAZ012	Error in co-ordination and transfer	The Co-ordination and transfer process will not be any different for "without" or "with" UAVs, however loss of this function is considered under HAZ011
HAZ013	Co-ordination and transfer too late	Co-ordination and transfer process will not be any different for "without" or "with" UAVs, however loss of this function is considered under HAZ011
HAZ014	Loss of information provision	Hazard 14 was considered a cause of other hazards during the UAV Workshop e.g. Hazard 1, Hazard 2 etc. and would lead to a reduction in situational awareness. Hazard 14 is therefore not considered further
HAZ015	Incorrect information provided	Hazard 15 was considered a cause of other hazards during the UAV Workshop e.g. Hazard 1, Hazard 2 etc. and would lead to a reduction in situational awareness. Hazard 15 is therefore not considered further

Table 1 – Hazard Identification

4.3 Hazard Identification Results

This is explained in more detail in section 4.6. Based on the discussions within 4.2, although five high level hazards were identified, the pivotal point at which the cause/consequence analysis was carried out was taken at a lower level due to the fact the ATC is complicit in the consequential mitigations.

The resultant set of hazards for Military UAV-OAT operations in non-segregated airspace is therefore as follows and is common to both the without-UAV and with-UAV scenarios.

- **HAZ001** – Inability to comply with separation provision instruction from ATC;
- **HAZ002** – Incorrect response to separation provision instruction from ATC;
- **HAZ003** – Intentional deviation from separation provision instruction from ATC;
- **HAZ004** – Delayed response to separation provision instruction from ATC;
- **HAZ005** (was HAZ006) – Loss of separation provision from ATC;
- **HAZ006** (was HAZ007) – ATC separation provision error;
- **HAZ007** (was HAZ008) – Loss of separation provision from Pilot in Command;
- **HAZ008** (was HAZ009) – Pilot in Command separation provision error;
- **HAZ009** (was HAZ010) – Pilot in Command separation provision instruction too late.

4.4 Separation Provision and Collision Avoidance

The high level functional model presented in Figure 1 represents a closed loop control system with the airspace as the element under control. By breaking the control loop at the point where the separation provision compliance function interfaces with the airspace it can be observed that:

- The primary control function is Separation Provision;
- Collision Avoidance can mitigate Separation Provision failure (although the Trajectory Compliance function is a potential for common cause failure);
- Collision Avoidance actions can interfere with Separation Provision.

As such the analysis of hazards rightly focuses on the Separation Provision Function, and models the Collision Avoidance functional failure scenarios either as mitigations in the consequence of the hazards or as potential causes of the hazards. No specific hazards have been identified for Collision Avoidance.

However, it should be noted that:

- current regulatory policy [8] dictates that Separation Provision has to be acceptably safe without collision avoidance. UAVs therefore have to be fully compliant with all separation provision requirements without taking into account the effectiveness of collision avoidance systems.

  This implies that whilst operating in non-segregated airspace UAVs must be able to comply with Separation Instructions from ATCOs or the PICs must manage the UAV separation provision. As such the UAV Control Link must be operational at all times and failure of the UCL must be considered as an emergency situation (captured as Safety Requirement [**FSR-04**]);
- notwithstanding the above, where the UAV is solely or jointly responsible for collision avoidance and given the potential risks in OAT operations from stray airspace users (e.g. balloons), a UAV

flight should be terminated as soon as safely practicable following failure of the UAV Collision Avoidance System (captured as Safety Requirement [**FSR-09**]).

4.5 Consequence Analyses

The FHA/PSSA considered the consequence of hazards without-UAV and with-UAV to establish if Military UAV-OAT operations in non-segregated airspace could alter or influence the consequence chain for the identified hazards. The consequence analysis was conducted to the point where there is the potential for an accident. The columns in the event tree are defined as follows:

- First Column – Initiating Hazard;
- Middle Columns – potential mitigations that would prevent the hazard resulting in an end consequence;
- Last Column – the end consequence.

A number of mitigations within the event trees are generic to all hazards; these are highlighted in the appropriate place.

Given the requirement to present a relative qualitative safety argument for Military UAV-OAT operations in non-segregated airspace and the justification for an improved level of risk reduction than the current 'without-UAV' situation, the table in Appendix D presents a qualitative severity classification scheme applicable for this safety analysis. The scheme is based on ESARR 4 [4] for ATM and JAR25-1309 [5] for aircraft related consequences.

Event trees have not been developed for Autonomous UAV operations; however these would result in the PIC and in most cases the ATC mitigations from the existing event trees being removed. From an ATC perspective consideration needs to be given to the situation where a UAV operating autonomously fails to follow its contingency plan, see **Safety Issue 8**.

4.5.1 Consequences for HAZ001 – Inability to comply with Separation Provision Instruction from ATC

The Event Tree for hazard HAZ001 is presented in Appendix E, E.1 for the without-UAV and with-UAV situation. The mitigations for this hazard are explained in Table 2 below. Note that whilst the mitigations are the same for the without-UAV and with-UAV situation the likelihood of success for some varies between the two situations as discussed below.

The descriptions provided within the following tables are based on the output from the FHA/PSSA Workshop.

Event Tree Mitigation	Description
Pilot in Command	In either the without-UAV or with-UAV situation, if a Pilot in Command is unable to comply with an ATC instruction it is likely that he will communicate this to ATC as soon as possible. However, it was considered potentially more likely that a UAV Pilot in Command could be aware of and inform ATC due to potential situational awareness tools[6] in the UAV.
Air Traffic Control awareness	The likelihood in the ability of an Air Traffic Controller to identify that an aircraft has failed to comply with a separation provision instruction will remain the same for without-UAV and with-UAV situations. Although Air Traffic Controllers in the future may be provided with information to enable them to distinguish between manned and unmanned aircraft, this should not change their ability to provide separation provision.

[6] Not all current UAVs have detailed situational awareness tools that provide information on other traffic, especially smaller, tactical UAVs.

Event Tree Mitigation	Description
Revised ATC Instruction	If the Air Traffic Controller is made aware, or notices, the Pilot in Command's inability to comply with a separation provision instruction, it was considered very likely that ATC would provide an amended instruction to either that specific aircraft, or dependent upon the circumstances, i.e. an inability to control the aircraft, provide appropriate instructions to surrounding aircraft.
Generic Mitigations applicable to all hazards without-UAV and with-UAV	
Other Aircraft	Once all the mitigations listed above have failed, and assuming worst case that there is another aircraft in close vicinity, the immediate mitigation is that the other aircraft takes avoiding action. It was considered that there will be little or no change in the likelihood of another aircraft taking avoiding action for the without-UAV to the with-UAV situation, however, this may depend on the conspicuity of the UAV itself in the with-UAV situation.
Collision Avoidance Systems	See discussion in section 4.4.

Table 2 - HAZ001 Event Tree Mitigations

4.5.2 Consequences for HAZ002 - Incorrect response to Separation Provision Instruction from ATC

The Event Tree for hazard HAZ002 is presented in Appendix E, E.2 for the without-UAV and with-UAV situation. The mitigations for this hazard are explained in Table 3. Note that whilst the mitigations are the same for the without-UAV and with-UAV situation the likelihood of success for some varies between the two situations as discussed below.

Event Tree Mitigation	Description
Pilot in Command	In either the without-UAV or with-UAV situation, if a Pilot in Command realises that he has followed a separation provision instructions incorrectly it is likely that he will communicate this to ATC as soon as possible. However, this mitigation was considered to have a very small likelihood given that a Pilot in Command is only likely to respond incorrectly to a separation provision instruction due to a misinterpretation or misunderstanding of that instruction.
Air Traffic Control awareness	The likelihood in the ability of an Air Traffic Controller to identify that an aircraft has incorrectly complied with a separation provision instruction will remain the same for without-UAV and with-UAV situations. Although Air Traffic Controllers in the future may be provided with information to enable them to distinguish between manned and unmanned aircraft, this should not change their ability to provide separation provision.
Revised ATC Instruction	If the Air Traffic Controller is made aware, or notices, the Pilot in Command's incorrect compliance with a separation provision instruction, it was very likely that ATC would query the Pilot in Commands response and provide an amended instruction.
Other Aircraft and Collision Avoidance mitigations as per HAZ001	

Table 3 – HAZ002 Event Tree Mitigations

4.5.3 Consequences for HAZ003 – Intentional deviation from Separation Provision Instruction from ATC

The Event Tree for hazard HAZ003 is presented in Appendix E, E.3 for the without-UAV and with-UAV situation.

Event Tree Mitigation	Description
Pilot in Command	In either the without-UAV or with-UAV situation, if a Pilot in Command intentionally deviated from a separation provision instruction it was considered highly likely that he will communicate this to ATC as soon as possible. This mitigation was thought to have a very high likelihood given that procedures state, specifically for collision avoidance manoeuvres that are contradictory to an ATC separation provision instructions, that a Pilot informs ATC as soon as possible. It was considered potentially more likely that a UAV Pilot in Command would communicate an intentional deviation from an instruction quicker than for a manned aircraft.
Air Traffic Control awareness	The likelihood in the ability of an Air Traffic Controller to identify that an aircraft has intentionally deviated from a separation provision instruction will remain the same for the without-UAV and with-UAV situation. An Air Traffic Controller may query the deviation from an instruction, but may also assume that the instruction will be followed and focus attention elsewhere.
ATC verifies situation	If the Air Traffic Controller is made aware, or notices, the intentional deviation from a separation provision instruction, it is very likely that ATC would query the Pilot in Command's response and provide an amended instruction. There is no change in the likelihood for either without-UAV or with-UAV situations for this mitigation.
Other Aircraft and Collision Avoidance mitigations as per HAZ001	

Table 4 - HAZ003 Event Tree Mitigations

4.5.4 Consequences for HAZ004 – Delayed response to Separation Provision Instruction from ATC

The Event Tree for hazard HAZ004 is presented in Appendix E, E.4 for the without-UAV and with-UAV situation.

Event Tree Mitigation	Description
Pilot in Command	In either the without-UAV or with-UAV situation, if a Pilot in Command cannot immediately follow a separation provision instruction it was considered highly likely that he will inform ATC as soon as possible. It was considered potentially more likely that a UAV Pilot in Command would communicate a delayed response to an instruction quicker than for a manned aircraft.
Air Traffic Control awareness	The likelihood in the ability of an Air Traffic Controller to identify that an aircraft has a delayed response to a separation provision instruction will remain the same for the without-UAV and with-UAV situation. An Air Traffic Controller may query that there is no initial response to his instruction.
Revised ATC Instruction	If the Air Traffic Controller is made aware, or notices, the Pilot in Command's delayed response and understands the reasons for it, it was considered very likely that ATC would either provide an amended instruction or manoeuvre other aircraft accordingly. There is no change in the likelihood for either without-UAV or with-UAV situations for this mitigation
Other Aircraft and Collision Avoidance mitigations as per HAZ001	

Table 5 – HAZ004 Event Tree Mitigations

4.5.5 Consequences for HAZ005 – Loss of Separation Provision from ATC

The Event Tree for hazard HAZ005 is presented in Appendix E, E.5 for the without-UAV and with-UAV situation.

In either the without-UAV or with-UAV situation, if a Pilot in Command notices a loss in separation provision from ATC, he will initially attempt to contact ATC and if this is not possible will instigate lost communications procedures.

The only mitigation that is considered more likely to occur in the with-UAV situation is that of the Pilot in Command and his attempt to contact ATC due to additional communication systems potentially available to a pilot of a UAV.

The Other Aircraft and Collision Avoidance mitigations are as per HAZ001.

4.5.6 Consequences for HAZ006 – ATC Separation Provision Error

The Event Tree for hazard HAZ006 is presented in Appendix E, E.6 for the without-UAV and with-UAV situation.

Event Tree Mitigation	Description
Air Traffic Control awareness	The likelihood of the ability of an Air Traffic Controller to notice an error in a separation provision instruction provided to a Pilot in Command was considered to be no different for the without-UAV to with-UAV situation.
Air Traffic Control Revised Instruction	The likelihood in the ability of an Air Traffic Controller to identify an error in the separation provision instruction provided to a Pilot in Command is considered to be no different for the without-UAV to with-UAV situation.
Other Aircraft and Collision Avoidance mitigations as per HAZ001	

Table 6 – HAZ006 Event Tree Mitigations

4.5.7 Consequences for HAZ007 – Loss of Separation Provision from Pilot in Command

The Event Tree for hazard HAZ007 is presented in Appendix E, E.7 for the without-UAV and with-UAV situation.

Event Tree Mitigation	Description
Pilot in Command	Where a Pilot in Command is responsible for providing his own separation provision, the likelihood of him realising an action has resulted in a loss of separation was considered no different in the without-UAV situation to the with-UAV situation.
Revised Instruction	Once the Pilot in Command notices a loss in separation provision, it is was considered very likely that he would revise and execute a new instruction as soon as possible. The likelihood for this mitigation was considered no different for the without-UAV to the with-UAV situation.
Other Aircraft and Collision Avoidance mitigations as per HAZ001	

Table 7 – HAZ007 Event Tree Mitigations

4.5.8 Consequences for HAZ008 – Pilot in Command Separation Provision Error

The Event Tree for hazard HAZ008 is presented in Appendix E, E.8 for the without-UAV and with-UAV situation.

Event Tree Mitigation	Description
Pilot in Command	Where a Pilot in Command is responsible for providing his own separation provision, the likelihood of him noticing an error in a separation provision instruction was considered no different in the without-UAV situation to the with-UAV situation.
Revised Instruction	Once the Pilot in Command notices an error in a separation provision instruction, it was considered very likely that he would rectify this through a revised instruction and execute this as soon as possible. The likelihood for this mitigation was considered no different for the without-UAV to the with-UAV situation.

Event Tree Mitigation	Description
Other Aircraft and Collision Avoidance mitigations as per HAZ001	

Table 8 – HAZ008 Event Tree Mitigations

4.5.9 Consequences for HAZ009 – Pilot in Command Separation Provision Instruction too late

The Event Tree for hazard HAZ009 is presented in Appendix E, E.8 for the without-UAV and with-UAV situation.

Where the Pilot in Command is responsible for providing his own separation provision instructions, and one of these is implemented too late, the first mitigation will be if there is an aircraft in the vicinity, followed by initiation of collision avoidance systems.

4.6 Causal Analyses

The FHA/PSSA considered the causes of each hazard for each of the following situations:

- Manned Aerial Vehicles (MAV);
- Piloted Unmanned Aerial Vehicles (PUAV);
- Autonomous Unmanned Aerial Vehicles (AUAV).

Each of the top level hazards identified in section 4.2 has been taken and decomposed down to the hazards identified at the UAV FHA/PSSA Workshop, and then developed for each of the situations listed above.

Transition into the Autonomous UAV situation must always involve detectable loss of the UAVs control link, as planned control link loss are considered outside the scope of the analysis (see section 3.2.3, Statement 8). This can be seen by the AND gate at the top of each AUAV hazard fault tree within Appendix F and is shaded grey.

4.6.1 Loss of Separation Provision

The separation provision function, as identified in section 3.1.1, can be the responsibility of either ATC or a PIC. Figure 3 below shows the decomposition of the high level hazard loss of separation provision.

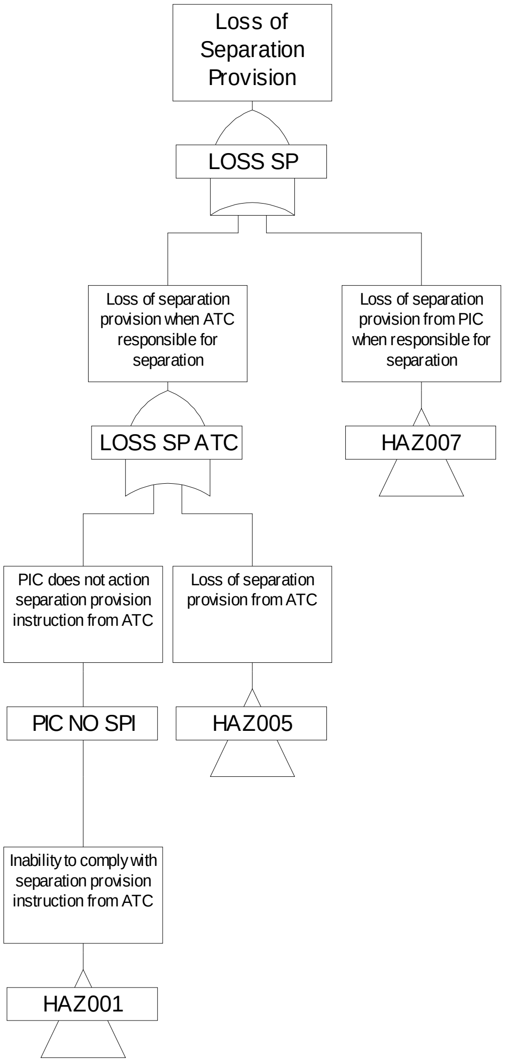

Loss of Separation Provision
LOSS SP
Loss of separation provision when ATC responsible for separation
Loss of separation provision from PIC when responsible for separation
LOSS SP ATC
HAZ007
PIC does not action separation provision instruction from ATC
Loss of separation provision from ATC
PIC NO SPI
HAZ005
Inability to comply with separation provision instruction from ATC
HAZ001

Figure 3 – Loss of Separation Fault Tree

Each of the hazard pivot points is discussed in the following sections.

4.6.1.1 Causes of HAZ001

This hazard covers the situation where a Pilot in Command is unable to comply with a separation provision instruction from ATC.

The causal analysis for this hazard has been considered for each of the situations listed in section 4.6 and is presented in Appendix F.1.1 for the Manned Aerial Vehicle (MAV) situation, F.1.2 for the Piloted UAV (PUAV) situation and F.1.3 for the Autonomous UAV (AUAV) situation.

For HAZ001 the areas of comparison are shown through the shading for each of the trees presented in Appendix F as follows:

- Blue Shading – AV OVER COM[7] is a common event to all three situations.
- Yellow Shading – SPI NOT IMP is a similar event covering air vehicle performance and system failures.
- Green Shading – NO SPI PIC is common to both the MAV and PUAV situations and relates to pilot incapacitation. For the AUAV situation, the events IN UAV CP and NO UAV CP are equivalent and cover the contingency planning aspects of autonomous UAV operations.

4.6.1.2 Causes of HAZ005

This hazard covers the situation where separation provision from ATC is lost.

The causal analysis for this hazard has been considered for each of the situations listed in section 4.6 and is presented in Appendix F.1.4 for the Manned Aerial Vehicle (MAV) situation, F.1.5 for the Piloted UAV (PUAV) situation and F.1.6 for the Autonomous UAV (AUAV) situation.

[7] Specific gates/events within the fault trees have been identified and referred to throughout this report using their gate/event names, which given the limited number of characters available, have been derived from the gate/event description.

For HAZ005 the areas of comparison are shown through the shading for each of the trees presented in Appendix F as follows:

- Blue Shading – NO SP ATC is a common event to the MAV and PUAV situations and covers the situation where ATC is unable to provide separation provision. For the AUAV situation there is no concept of no separation provision from ATC to an autonomous UAV, rather if ATC is unaware of the AUAV contingency plan, then he will potentially no longer be able to assure separation provision to other aircraft as he will not only not know the intentions of the AUAV, but be unable to contact the AUAV.. This is covered by an additional gate NO SP ATC to those in the MAV and PUAV situation.

- Green Shading – NO COTR is a common event to all three situations. If no co-ordination and transfer takes place, this could directly result in a loss of separation provision from ATC.

- Yellow Shading – ATC UNAWARE AV/UAV/AUAV are equivalent and deal with a situation where ATC either forgets an aircraft, or is unaware of the presence of an aircraft due to a failure of the detection capability provided by surveillance systems.

4.6.1.3 Causes of HAZ007

This hazard covers the situation where separation provision from the Pilot in Command is lost.

The causal analysis for this hazard has been considered for each of the situations listed in section 4.6 and is presented in Appendix F.1.7 for the Manned Aerial Vehicle (MAV) situation, F.1.8 for the Piloted UAV (PUAV) situation and F.1.9 for the Autonomous UAV (AUAV) situation.

For HAZ007 the areas of comparison are shown through the shading for each of the trees presented in Appendix F as follows:

- Blue Shading – NO SIT AWARE/PIC DIS are common events to the MAV and PUAV situations and cover the situation where the Pilot in Command is unable to provide his own separation provision based on losing his situational awareness. In the case of PUAV, an additional cause is malfunction of the UAV to provide the PIC with adequate representation of the airspace situation.

- Yellow Shading – NO AV/UAV/AUAV FC/CP are equivalent events covering the aircraft's inability to support separation provision instructions. In the case of an AUAV this is failure of the AUAV to implement its contingency plan.

- Green Shading – For the MAV and PUAV situations pilot incapacitation (PIC INACP) is also a cause of Pilot in Command loss of separation provision.

4.6.2 Separation Provision Error

Figure 4 below shows the decomposition of the high level hazard separation provision error.

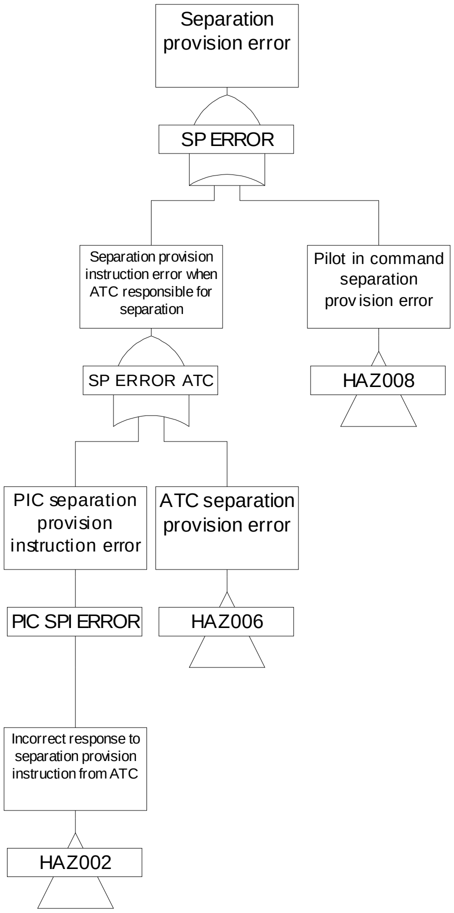

Separation provision error
SP ERROR
Separation provision instruction error when ATC responsible for separation
Pilot in command separation provision error
SP ERROR ATC
HAZ008
PIC separation provision instruction error
ATC separation provision error
PIC SPI ERROR
HAZ006
Incorrect response to separation provision instruction from ATC
HAZ002

Figure 4 – Separation Provision Error Fault Tree

Each of the hazard pivot points is discussed in the following sections.

4.6.2.1 Causes of HAZ002

This hazard covers the situation where a Pilot in Command incorrectly responds to a separation provision instruction from ATC.

The causal analysis for this hazard has been considered for each of the situations listed in section 4.6 and is presented in Appendix F.2.1 for the Manned Aerial Vehicle (MAV) situation, F.2.2 for the Piloted UAV (PUAV) situation and F.2.3 for the Autonomous UAV (AUAV) situation.

For HAZ002 the areas of comparison are shown through the shading for each of the trees presented in Appendix F as follows:

- Blue Shading – SPI FALSE ALERT is a common event to the MAV and PUAV situations, and covers false collision avoidance, terrain avoidance or other alerts. For the AUAV situation, the gate CP OR is equivalent and covers the same alerts that falsely override the AUAV contingency plan.

- Yellow Shading – SPI WRONG PIC/CP WRONG EXEC are equivalent events covering Pilot in Command, or in the case of AUAV the UAV itself, incorrectly executing a separation provision instruction, or in the case of the AUAV wrongly executing its contingency plan.

- Green Shading – SPI MIS PIC is common to both the MAV and PUAV situations and relates to the pilot misunderstanding the separation provision instruction. For the AUAV situation, the event COR CP is equivalent and covers contingency plan corruption.

4.6.2.2 Causes of HAZ006

This hazard covers the situation where ATC provides an incorrect separation provision instruction.

The causal analysis for this hazard has been considered for each of the situations listed in section 4.6 and is presented in Appendix F.2.4 for the

Manned Aerial Vehicle (MAV) situation, F.2.5 for the Piloted UAV (PUAV) situation and F.2.6 for the Autonomous UAV (AUAV) situation.

For HAZ006 the areas of comparison are shown through the shading for each of the trees presented in Appendix F as follows:

- Blue Shading – ATC ERR is a common event to all three situations, and covers all ATCO human errors.
- Yellow Shading – ATC PROV ERR is similar and covers where the ATCO is provided with the incorrect information either via equipment or through incorrect procedures.
- Green Shading – For the AUAV situation, there is an additional event under ATC PROV ERR whereby if ATC has been provided an incorrect contingency plan for AUAV operations, then ATC will provide information to other aircraft based on this incorrect information.

4.6.2.3 Causes of HAZ008

This hazard covers the situation where the Pilot in Command implements an incorrect separation provision instruction when he is responsible for separation provision.

The causal analysis for this hazard has been considered for each of the situations listed in section 4.6 and is presented in Appendix F.2.7 for the Manned Aerial Vehicle (MAV) situation, F.2.8 for the Piloted UAV (PUAV) situation and F.2.9 for the Autonomous UAV (AUAV) situation.

For HAZ008 the areas of comparison are shown through the shading for each of the trees presented in Appendix F as follows:

- Blue Shading – PIC INC SA is a common event for both the MAV and PUAV situations, whereby the pilot has incorrect understanding of his situational awareness. This event does not apply to the AUAV situation.

- Yellow Shading – PIC INC SI/PIC UAV INC SI is common to both the MAV and PUAV and includes situations where the air vehicle itself is providing incorrect situational indication to the pilot, resulting in a separation provision instruction error. Again, this branch of the FTA does not apply to the AUAV situation.

- Green Shading – For the AUAV situation, the only cause of a separation provision error (AUAV CP INC) will be if the AUAV contingency plan is corrupted or incorrect as this is the means by which the AUAV will implement its operations.

4.6.3 Delayed Separation Provision

Figure 5 below shows the decomposition of the high level hazard delayed separation provision.

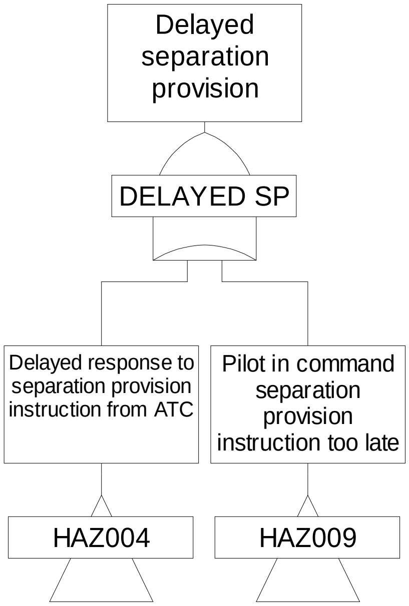

Delayed separation provision
DELAYED SP
Delayed response to separation provision instruction from ATC
Pilot in command separation provision instruction too late
HAZ004
HAZ009

Figure 5 – Delayed Separation Provision Fault Tree

Each of the hazard pivot points is discussed in the following sections.

4.6.3.1 Causes of HAZ004

This hazard covers the situation where a Pilot in Command has a delayed response to a separation provision instruction from ATC.

The causal analysis for this hazard has been considered for each of the situations listed in section 4.6 and is presented in Appendix F.3.1 for the Manned Aerial Vehicle (MAV) situation, F.3.2 for the Piloted UAV (PUAV) situation and F.3.3 for the Autonomous UAV (AUAV) situation.

For HAZ004 the areas of comparison are shown through the shading for each of the trees presented in Appendix F as follows:

- Blue Shading – AV/UAV PERF/CL DELAY is equivalent to all three situations and covers the aircrafts inability to timely respond to separation provision instructions, due to performance limitations. In the case of the PUAV situation, this also includes latency in the control link between the UAV and the Pilot in Command.

- Yellow Shading – SPI DELAY PIC are the same events for the MAV and PUAV situations, and cover where the Pilot in Command delays execution of a separation provision instruction due to either an incorrect situational picture or by simply responding too slowly.

- Green Shading – SPI MIS PIC is common to both the MAV and PUAV situations and relates to the pilot misunderstanding the separation provision instruction provided from ATC. For the AUAV situation, the event COR CP is equivalent and covers contingency plan corruption.

4.6.3.2 Causes of HAZ009

This hazard covers the situation where a Pilot in Command implements his own separation provision instruction too late.

The causal analysis for this hazard has been considered for each of the situations listed in section 4.6 and is presented in Appendix F.3.4 for the Manned Aerial Vehicle (MAV) situation, F.3.5 for the Piloted UAV (PUAV) situation and F.3.6 for the Autonomous UAV (AUAV) situation.

For HAZ009 the areas of comparison are shown through the shading for each of the trees presented in Appendix F as follows:

- Blue Shading – AV/UAV PERF/CL DELAY is a common event to all three situations and covers the aircrafts inability to timely respond to separation provision instructions, due to performance limitations. In the case of the PUAV situation, this also includes latency in the control link between the UAV and the PIC.

- Yellow Shading – PIC SLOW are the same events for the MAV and PUAV situations, and cover where the PIC action is too slow and hence execution of his own separation provision instruction is late.

- Green Shading – PIC INC SA is common to both the MAV and PUAV situations and relates to the pilot having an incorrect situational picture. For the AUAV situation, the event COR CP is equivalent and covers contingency plan corruption.

4.6.4 Intentional Deviation from Separation Provision Instruction (Causes of HAZ003)

This hazard covers the situation where a Pilot in Command intentionally deviates from a separation provision instruction from ATC.

The causal analysis for this hazard has been considered for each of the situations listed in section 4.6 and is presented in Appendix F.4.1 for the Manned Aerial Vehicle (MAV) situation, F.4.2 for the Piloted UAV (PUAV) situation and F.4.3 for the Autonomous UAV (AUAV) situation.

For HAZ003 the areas of comparison are shown through the shading for each of the trees presented in Appendix F as follows:

- Blue Shading – CA ALERT is a common event to all three situations. One of the causes for a Pilot in Command or AUAV to intentionally deviate from an instruction, or from information provided within a contingency plan in the case of AUAV, would be due to a collision avoidance alert.

- Yellow Shading - OTHER ALERT is also a common event to all three situations. There are additional alerts other than collision avoidance alerts e.g. terrain avoidance alerts which may also result in an intentional deviation from a separation provision instruction.

4.7 Analysis Conclusions

The consequence analysis undertaken for Military UAV-OAT operations in non-segregated airspace has shown that the identified mitigations for the without-UAV and with-UAV situations are logically the same. However, the workshop identified that there are specific areas where the with-UAV situation has the potential to reduce the likelihood of failure of specific mitigations. Those areas of significant relevance will need to be considered as part of the implementation of MIL UAV-OAT operations and include:

- UAV Pilots in Command identify situational awareness issues more easily or quickly based on the additional potential range of information sources available.

- UAV Pilots in Command may have more communication equipment at hand to verify potential issues with ATC.

The causal analysis further decomposed the with-UAV situation to include PIC controlled UAVs (PUAV) and Autonomous UAVs (AUAV) to highlight the different causes for each situation. The causal analysis has identified specific areas within the fault tree analysis (highlighted by coloured shading) where the causes are either:

- identical for all three situations, without-UAV (MAV), PUAV and AUAV;

- need to achieve an equivalent or reduced frequency of occurrence in the PUAV situation;

- equivalent for the MAV and PUAV situations, but there is a difference for the AUAV situation.

Thus the causal analysis has identified that a reduction in the likelihood of hazard occurrence rates for UAV-OAT operations could only be achieved within the implementation of UAV Systems and thus cannot be achieved via changes to ATC.

Overall, from a risk reduction point of view there are clearly areas where there is no difference between the without-UAV and with-UAV situations. However, where there is equivalence the implementation of the UAV System should consider further risk reduction As Far As Reasonably Practicable (AFARP).

5 Safety Requirements

5.1 Introduction

The FHA/PSSA set out to provide evidence in support of the safety argument for Military UAV-OAT operations in non-segregated airspace. The proceeding hazard analysis has identified the hazards that fall within the scope and boundary and has performed cause/ consequence analyses for the without-UAV and with-UAV situations. As a result of this analysis a number of requirements have been identified that need to be satisfied in order to support the argument further. These are derived and discussed in the following section.

5.2 Risk Assessment Overview

The purpose of the FHA/PSSA was to derive a set of high level safety requirements such that, if satisfied, an acceptable level of safety can be demonstrated. In order for this to be established, appropriate risk mitigation related to each hazard needs to be specified in the form of Safety Requirements.

Given that the analysis has not identified any unique hazards for UAV-OAT operations, the safety requirements set out below are derived from the risk mitigation necessary in order to ensure that the safety criteria (as stated in section 1.2) are achieved, i.e. the risk from Military UAV-OAT operations is:

- no greater than for Military Manned OAT in non-segregated airspace; and
- reduced As Far As Reasonably Practicable (AFARP).

The safety requirements consider all of the hazards that relate to Military UAV-OAT operations in non-segregated airspace, referred to throughout this report as the “with-UAV” situation. The requirements are allocated against the mitigations in the event trees and the events in the fault trees, which have been developed down to the level of the logical models defined in Appendix B.

Traceability between the identified Safety Requirements and the Draft Specification is presented in Appendix G, the Draft Specification has also been traced back to the Safety Requirements Appendix I to ensure completeness.

5.3 Safety Requirements Sources

Safety Requirements are derived from the following sources and are subject to resolution of any identified outstanding safety issues:

a. Functional Safety Requirements – derived from the functional models and causal analysis.

b. Mitigating Safety Functions – derived from the consequence analyses.

c. Safety Integrity Requirements – derived from the cause and consequence analyses and based on output from the FHA/PSSA Workshop.

The derivation of each requirement is recorded in the following requirements tables. Where the requirement wording within the Draft Specification is adequate for the safety analysis requirement, then that wording has been used. This is shown by the requirement being in *italic* text.

5.4 Functional Safety Requirements

The following safety requirements have been identified from the functional models and the hazard analysis.

Each of the functional requirements in the following table should be read in the context of the Scenario Model presented in Appendix B.1, excluding the mission aspects of the scenario which is considered outside the scope of the analysis, see section 3.2.3, statement 10. For example, FSR-01 applies to all scenarios so the requirement applies to taxi, departure, en-route, approach, landing, etc.

ID	Requirement	Derivation and Traceability	Applicable Scenarios
FSR-01	*The air traffic service provided to UAVs should accord with that provided to manned aircraft*	Figure 8 and Figure 9 FTA HAZ005, Appendices F.1.4, F.1.5 and F.1.6 FTA HAZ006, Appendices F.2.4, F.2.5 and F.2.6	Applicable to all scenarios
FSR-02	When ATC are responsible for separation provision, the separation minima between UAVs and other traffic should be the same as for manned aircraft flying OAT in the same class of airspace	Figure 8 and Figure 9	Applicable to all scenarios
FSR-03	The Pilot in Command is responsible for ensuring that the UAV trajectory is compliant with any ATC clearance	Figure 8	Applicable to all scenarios excluding MSA, VFR and Sea operations
FSR-04	*While in receipt of an air traffic service, UAVs should be monitored continuously by the UAV Pilot in Command for adherence to the approved flight plan*	Figure 12	Applicable to all scenarios
FSR-05	*The weather minima for UAV flight should be determined by the equipment and capabilities of each UAV System*	Figure 8 and Figure 9	Applicable to Pre-flight Planning
FSR-06	UAVs shall be pre-programmed with an appropriate contingency plan in the event that the Pilot in Command is no longer in control of the UAV	Section 4.4	Applicable to Pre-flight Planning

ID	Requirement	Derivation and Traceability	Applicable Scenarios
FSR-07	Following the above event, UAVs should continue flight autonomously and in accordance with the pre-programmed contingency plan	Figure 8	Applicable to Pre-flight Planning and Emergency Operations
FSR-08	UAVs flying in controlled airspace shall notify ATC of contingency plans for emergency AUAV operations prior to operations	Figure 8 FTA HAZ005, See Appendix F.1.6, Event ATC NO AUAV CP (AUAV)	Applicable to Pre-flight Planning
FSR-09	*Where a UAV Pilot in Command has primary responsibility for separation provision, he should maintain a minimum distance of 500ft between his UAV and other airspace users, regardless of how the conflicting traffic was detected and irrespective of whether or not he was prompted by a collision avoidance system*	Figure 9	Applicable to VFR operations
FSR-10	UAV collision avoidance systems should enable a UAV Pilot in Command to perform collision avoidance functions at least as well as, and preferably better, than a pilot in a manned aircraft	Figure 8 and Figure 9	Applicable to all scenarios
FSR-11	Autonomous UAV collision avoidance systems should have equivalent efficacy to a pilot performing threat detection and collision avoidance actions	Figure 8 and Figure 9	Applicable to all scenarios

ID	Requirement	Derivation and Traceability	Applicable Scenarios
FSR-12	UAV equipment carriage shall render it compatible with mandated collision avoidance systems fitted to other aircraft	FTA HAZ001, Appendices F.1.1, F.1.2 and F.1.3, Gate CA ALERT (MAV, PUAV and AUAV) FTA HAZ003, Appendices F.4.1, F.4.2 and F.4.3, Event CA ALERT (MAV, PUAV and AUAV)	Applicable to all scenarios
FSR-13	UAVs should have limited alerting systems equivalent to those on a manned aircraft, to minimise the potential alerts that can interrupt compliance with separation provision instructions	FTA HAZ001, Appendices F.1.1, F.1.2 and F.1.3, Gate OTHER ALERT (MAV, PUAV and AUAV) FTA HAZ003, Appendices F.4.1, F.4.2 and F.4.3, Event OTHER ALERT (MAV, PUAV, AUAV)	Applicable to all scenarios

ID	Requirement	Derivation and Traceability	Applicable Scenarios
FSR-14	Pilots in Command of UAVs and ATC shall be familiar with individual UAV performance characteristics	FTA HAZ001, Appendices F.1.1, F.1.2 and F.1.3, Gate NO SPI PERF LIM (MAV, PUAV and AUAV) FTA HAZ004, Appendices F.3.1, F.3.2 and F.3.3, Event AV PERF (MAV), UAV PERF (PUAV and AUAV) FTA HAZ009, Appendices F.3.4, F.3.5 and F.3.6, Event AV PERF (MAV), UAV PERF (PAUV and AUAV)	Applicable to Pre-flight Planning
FSR-15	*UAVs should carry similar equipment for flight, navigation and communication as required for manned aircraft, as mandated for the airspace in which the UAV is operating, with the exception of ACAS*	FTA HAZ005, Appendices F.1.4, F.1.5 and F.1.6, Gate ATC NO RADAR (MAV, PUAV and AUAV)	Applicable to all scenarios
FSR-16	UAVs should carry appropriate equipment to ensure UAV Pilots in Command are provided with an accurate situational indication equivalent to that provided to a pilot of a manned aircraft	FTA HAZ002, Appendices F.2.1, F.2.2 and F.2.3, Gate SPI INC SI (MAV, PUAV and AUAV) FTA HAZ008, Appendices F.2.7 and F.2.8, Gate PIC INC SI (MAV and PUAV)	Applicable to all scenarios

ID	Requirement	Derivation and Traceability	Applicable Scenarios
FSR-17	*While in receipt of an air traffic service, the UAV Pilot in Command should maintain two-way communications with ATC, using standard phraseology when communicating via RTF. The word "unmanned" should be included on first contact with an ATC agency*	FTA HAZ002, Appendices F.2.1 and F.2.2, Event SPI MIS PIC (MAV and PUAV)	Applicable to all scenarios excluding MSA, VFR and Sea operations
FSR-18	*Where UAV emergency procedures necessarily differ from those for manned aircraft e.g. UAV control link hijacking, security breaches etc., they should be designed to ensure the safety of other airspace users and people on the ground, and they should be coordinated with ATC as appropriate*	FTA HAZ002, Appendix, F.2.2, Event UAV CL HIJACK (PUAV)	Applicable to Pre-flight Planning and Emergency operations
FSR-19	UAV Pilots in Command shall be able to respond to separation provision instructions and manoeuvre UAVs via a control link at least as quickly as a pilot can receive an instruction and manoeuvre a manned aircraft	FTA HAZ004, Appendix F.3.2, Event UAV CL DELAY (PUAV) FTA HAZ009, Appendix F.3.5, Event UAV CL DELAY (PUAV)	Applicable to all scenarios

ID	Requirement	Derivation and Traceability	Applicable Scenarios
FSR-20	*With regard to cross-border operations, state UAVs should be bound by the same international conventions as manned state aircraft. In addition, flights by state UAVs into the FIR/UIR of other states should be pre-notified to the relevant FIR/UIR authorities, normally by submission of a contingency plan. ATC transfers between adjacent states should accord with those for manned aircraft*	Section 3.3.2 FTA HAZ005, Appendices F.1.4, F.1.5 and F.1.6, Event NO COTR (MAV, PUAV and AUAV)	Applicable to FIR/UIR, State Boundary operations
FSR-21	UAV Pilots in Command shall have equivalent piloting skills to pilots of conventional aircraft, enabling them to monitor, control and operate the air vehicle in a manner comparable to manned aircraft	FTA HAZ002, Appendices F.2.1 and F.2.2, Event PIC ERROR (MAV and PUAV)	Applicable to all scenarios
FSR-22	UAV Systems shall provide an indication to Pilots in Command when the UAV Control Link has been lost and the UAV is operating autonomously	All hazards for AUAV, Event DET LOSS CL (AUAV)	Applicable to all scenarios
FSR-23	Autonomous UAV separation provision systems should have equivalent efficacy to a pilot performing separation provision actions	Figure 8 and Figure 9	Applicable to MSA, VFR and Sea operations
FSR-24	Where a UAV is unable to continue to comply with any of the requirements for operations in non-segregated airspace then the UAV should be segregated from all other airspace users as soon as practicable.	Figure 6 and Figure 7	Applicable to all scenarios

ID	Requirement	Derivation and Traceability	Applicable Scenarios
FSR-25	When the UAV Control Link has been lost Pilots in Command shall inform ATC as soon as possible	FSR-22	Applicable to all scenarios
FSR-26	UAV Systems shall provide an indication to ATC when the UAV is operating autonomously	All hazards for AUAV, Event DET LOSS CL (AUAV)	Applicable to all scenarios

Table 9 – Functional Safety Requirements

5.5 Mitigating Safety Functions

The following external requirements are derived from the consequence analyses. Some of the Mitigating Safety Requirements are derived from examining the dependence between the hazard and each of the mitigations, and the mitigations themselves.

Given that there are no changes envisaged in ATC operations with or without-UAVs, it is assumed that ATC will apply the same procedures for Manned and Unmanned operations. Thus no specific mitigating safety functions are identified for ATC other than a general requirement to apply the same procedures [**FSR-01**].

ID	Requirement	Derivation and Traceability
MSF-01	The PIC must inform ATC when unable to comply with any ATC instruction	HAZ001 ETA, Appendix E.1
MSF-02	UAVs shall be fitted with suitable conspicuity devices to aid visual acquisition by other airspace users.	HAZ001 ETA, Appendix E.1
MSF-03	Whilst for manned and unmanned operations the PIC is a common factor to both the Separation Provision and Collision Avoidance functions, to reduce the risk to AFARP then implementation of these functions should be as independent as far as is reasonably practicable	Inferred from dependence between HAZ001 and Collision Avoidance mitigation See **Safety Issue 8**

ID	Requirement	Derivation and Traceability
MSF-04	Following failure of the UAV Collision Avoidance System, the UAV flight should be terminated as soon as safely practicable	Section 4.4 and FSR-10
MSF-05	The PIC must inform ATC as soon as he becomes aware that the UAV is responding incorrectly to any ATC instruction	HAZ002 ETA, Appendix E.2
MSF-06	The PIC must inform ATC of any intentional deviation from an ATC instruction	HAZ003 ETA, Appendix E.3
MSF-07	The PIC must inform ATC of any delayed response to an ATC instruction	HAZ004 ETA, Appendix E.4
MSF-08	In the event of loss of communications with ATC the PIC shall attempt to contact ATC, if the attempt fails the PIC should follow lost communications procedures as per manned operations	HAZ005 ETA, Appendix E.5
MSF-09	*UAVs should comply with VFR and IFR as they affect manned aircraft flying OAT*	HAZ007, HAZ008 and HAZ009 ETAs, Appendices E.7, E.8 and E.9
MSF-10	*UAVs should comply with the right-of-way rules as they apply to other airspace users*	HAZ007, HAZ008 and HAZ009 ETAs, Appendices E.7, E.8 and E.9

Table 10 – Mitigating Safety Functions

5.6 Safety Integrity Requirements

The following safety requirements are derived from the event trees and fault tree analysis. Where the FHA/PSSA Workshop identified that UAV could reduce the likelihood associated with an event or mitigation, this is reflected in the requirements below. Where ATC operations remain unchanged no SIRs have been identified.

ID	Requirement	Derivation and Traceability
SIR-01	The probability that a Pilot in Command of a UAV does not inform ATC of an inability to comply with ATC instructions shall be equivalent, and preferably lower, than for manned operations	MSF-01
SIR-02	The probability of failure of UAV visual conspicuity devices shall be equivalent to those used on Manned AV	MSF-02
SIR-03	The probability that the UAV Collision Avoidance system (with or without PIC) fails to avoid a collision shall be equivalent to an aircraft with a pilot on board	MSF-03 and MSF-04
SIR-04	The probability that a Pilot in Command of a UAV does not inform ATC of a recognised incorrect response to an ATC instruction shall be equivalent to Manned operations	MSF-05
SIR-05	The probability that a Pilot in Command of a UAV does not inform ATC of an intentional deviation from an ATC instruction shall be equivalent, and preferably lower, than for manned operations	MSF-06

ID	Requirement	Derivation and Traceability
SIR-06	The probability that a Pilot in Command of a UAV does not inform ATC of a delayed response to an ATC instruction shall be equivalent, and preferably lower, than for Manned operations	MSF-07
SIR-07	The probability that a Pilot in Command of a UAV fails to notice loss of Separation Provision and contact ATC shall be equivalent, and preferably lower, than Manned operations[8]	MSF-08
SIR-08	The probability that a Pilot in Command of a UAV fails to follow lost communications procedures in the event of loss of Separation Provision from ATC shall be equivalent to manned operations	MSF-08
SIR-09	The frequency of occurrence of UAVs being unable to implement a separation provision instruction due to a UAV System failure shall be equivalent to that of manned aircraft	FTA HAZ001, Appendices F.1.1, F.1.2 and F.1.3, Event AV SYS FAIL (MAV), UAV SYS FAIL (PUAV and AUAV) and UAV CS FAIL (PUAV) FTA HAZ007, Appendices F.1.7 and F.1.8, Gate NO AV/UAV FC (MAV and PUAV)

[8] Consideration should be given to provision of independent means of communication with ATC such as telephone etc.

ID	Requirement	Derivation and Traceability
SIR-10	The frequency of occurrence with which a UAV pre-programmed flight path is corrupted or incorrect shall be equivalent to that of a Pilot in Command of a manned aircraft being unable to or incorrectly responding to a separation provision instruction	FTA HAZ001, Appendix F.1.3, Event INC UAV CP (AUAV), NO UAV CP (AUAV) FTA HAZ002, Appendix F.2.3, Event COR CP (AUAV) FTA HAZ006, Appendix F.2.6, Event AUAV CP INC (AUAV) FTA HAZ008, Appendix F.2.9, Event AUAV CP INC (AUAV) FTA HAZ004, Appendix F.3.3, Event COR CP (AUAV) FTA HAZ009, Appendix F.3.6, Event COR CP (AUAV)
SIR-11	The frequency of occurrence with which a UAV Pilot in Command loses situational awareness shall be equivalent, and preferably lower, to that of manned aircraft	FTA HAZ007, Appendices F.1.7 and F.1.8, Gate NO SIT AWARE (MAV and PUAV) FTA HAZ008, Appendices F.2.7 and F.2.8, Event PIC INC SA (MAV and PUAV) FTA HAZ004, Appendices F.3.1 and F.3.2, Event PIC INC SA (MAV and PUAV) FTA HAZ009, Appendices F.3.4 and F.3.5, Event PIC INC SA (MAV and PUAV)
SIR-12	The frequency of occurrence with which an Autonomous UAV fails to implement its pre-programmed contingency plan shall be equivalent, and preferably lower, to that of a Pilot in Command being unable to comply with a separation provision instruction	FTA HAZ007, Appendix F.1.9, Event NO AUAV CP (AUAV)

ID	Requirement	Derivation and Traceability
SIR-13	The frequency of occurrence with which a UAV PIC does not recognise a missed co-ordination and transfer shall be equivalent, and preferably lower, than that for a pilot of a manned aircraft	FTA HAZ005, Appendices F.1.4, F.1.5 and F.1.6, Event NO COTR (MAV, PUAV and AUAV)
SIR-14	The probability of a UAV false collision avoidance or other false alerts shall be equivalent to that for Manned aircraft	FTA HAZ002, Appendices F.2.1, F.2.2 and F.2.3, Gate SPI FALSE ALERT (MAV and PUAV) and CP OR (AUAV)
SIR-15	The frequency of occurrence of a UAV flight control error shall be equivalent to that for Manned aircraft	FTA HAZ002, Appendices F.2.1, F.2.2 and F.2.3, Event AV FC ERROR (MAV), UAV FC ERROR (PUAV and AUAV)
SIR-16	The frequency of occurrence of a UAV Pilot in Command human error shall be equivalent to that for a Pilot of a Manned aircraft	FTA HAZ002, Appendices F.2.1 and F.2.2, Event PIC ERROR (MAV and PUAV) FTA HAZ004, Appendices F.3.1 and F.3.2, Event PIC SLOW (MAV and PUAV) FTA HAZ009, Appendices F.3.4 and F.3.5, Event PIC SLOW (MAV and PUAV)
SIR-17	The frequency of occurrence of corruption of UAV flight control commands shall be equivalent to that of Manned aircraft	FTA HAZ002, Appendices F.2.1, F.2.2 and F.2.3, Gate VAL COR FC (MAV, PUAV and AUAV)

Table 11 – Safety Integrity Requirements

6 Conclusions and Identified Safety Issues

6.1 Conclusions

The safety assurance activity undertaken for Military UAV-OAT operations in non-segregated airspace has involved a number of safety activities, outlined in Appendix J, culminating in construction of this FHA/PSSA Report.

The safety assurance activity has identified nine hazards that fall within the defined scope of the safety analysis. All nine hazards are common to the without-UAV and with-UAV situations:

- HAZ001 – Inability to comply with separation provision instruction from ATC;
- HAZ002 – Incorrect response to separation provision instruction from ATC;
- HAZ003 – Intentional deviation from separation provision instruction from ATC;
- HAZ004 – Delayed response to separation provision instruction from ATC;
- HAZ005 – Loss of separation provision from ATC;
- HAZ006 – ATC separation provision error;
- HAZ007 – Loss of separation provision from Pilot in Command;
- HAZ008 – Pilot-in-command separation provision error;
- HAZ009 – Pilot-in-command separation provision instruction too late.

A causal and consequence analysis has been undertaken for each of the identified hazards to the level of detail commensurate with the Draft Specifications.

Based on this assessment, 53 safety requirements have been derived and traced to the Draft Specification in Appendix G and Appendix I.

These requirements include the following eight functional safety requirements that are not currently covered by the Draft Specification:

- **FSR-06**: UAVs shall be pre-programmed with an appropriate contingency plan in the event that the Pilot in Command is no longer in control of the UAV;

- **FSR-13**: UAVs should have limited alerting systems equivalent to those on a manned aircraft, to minimise the potential alerts that can interrupt compliance with separation provision instructions;

- **FSR-14**: Pilots in Command of UAVs and ATC shall be familiar with UAV performance characteristics;

- **FSR-19**: UAV Pilots in Command should be able to respond to separation provision instructions and manoeuvre UAVs via a control link at least as quickly as a pilot can receive an instruction and manoeuvre a manned aircraft;

- **FSR-22**: UAV Systems shall provide indication to Pilots in Command when the UAV Control Link has been lost and the UAVs is operating autonomously;

- **FSR-25**: When the UAV Control Link has been lost Pilots in Command shall inform ATC as soon as possible;

- **FSR-26**: UAV Systems shall provide an indication to ATC when the UAV is operating autonomously;

- **MSF-03**: Whilst for manned and unmanned operations the PIC is a common factor to both the Separation Provision and Collision Avoidance functions, to reduce the risk to AFARP then implementation of these functions should be as independent as is reasonably practicable. See **Safety Issue 8**.

The safety analysis has shown that the Draft Specifications adequately address, either explicitly (shown in italic text) or implicitly, the safety recommendations derived from the independent safety assurance activity. The documented safety assurance activity is provided to support the Draft Specifications from a safety perspective; consequently the eight functional requirements that are not currently addressed by the Draft Specification should be included. It is also recommended that the safety requirements documented in Appendix G be included as an Annex to the Draft Specifications.

The Draft Specifications are primarily functional in nature and thus a trace to the safety integrity requirements was not expected. However, consideration should be given to the inclusion of summary safety integrity requirements within the Draft Specifications which capture the potential for:

- reduction in probability of some of the hazard mitigations failing;
- improvements in UAV System integrity over manned aircraft.

6.2 Safety Issues

The following safety issues were identified during the safety analysis activities. Safety Issues 1 to 5 were identified during the FHA/PSSA Workshop. Some of these issues were closed during the post workshop activity are included here for traceability.

No	Safety Issue	Resolution	Status
1	During discussions relating to the use of UAVs as Military OAT in non-segregated airspace, it was identified that there is the potential for an increase in military air traffic. The point was raised that certain UAVs e.g. Global Hawk, climb to FL450 and remain there for 10 hours or longer, this replaces the need for current successive missions by 2 or more manned surveillance aircraft all of whom climb and descend to/from operating areas contributing to congestion and ATC workload	It was agreed that any increase in Military OAT traffic did not need to be considered within the Safety Assessment.	**Closed**

No	Safety Issue	Resolution	Status
2	During the review of the functional and logical models it was noted that consideration should be given to the mix of VFR/IFR traffic and mixed responsibilities for separation, depending on the airspace class. It was agreed that this would be considered within the post workshop safety assessment	The FHA/PSSA Report has considered the shift in responsibility for separation provision throughout the safety analysis, see section 3.2.2. This is also reflected in the hazard analysis, which in some cases specifically identifies who is responsible.	**Closed**
3	It was agreed that ATM provisions e.g. airspace regulations etc. and their impact on UAVs as Military OAT in non-segregated airspace will be considered on the analysis is complete against the Harmonisation of Operational Air Traffic and its General Air Traffic Interface (HORGI) work.	This analysis will need to be reviewed by EUROCONTROL for its harmonisation with the HORGI work already carried out.	**Open**
4	During discussions of UAVs themselves it was identified that the integrity of UAV aircraft systems with respect to ATM hazards could be an issue. It was agreed that any UAV system requirements with respect to the identified ATM hazards would be considered during the post workshop safety assessment	See Safety Integrity Requirements, section 5.6	**Closed**
5	During review of the functional models, the collision avoidance function created much debate. It was agreed that the collision avoidance function itself would be assessed separately within the safety analysis activity, and any safety requirements, e.g. collision avoidance failure contingency procedures identified as appropriate	See Collision Avoidance discussion in sections 3.1 and 4.4 and Safety Requirements, section 5	**Closed**
6	It is recognised that replicating the	Outside the scope	**Closed**

No	Safety Issue	Resolution	Status
	effectiveness of the Pilot's Visual Acquisition process within a UAV's Sense and Avoid capability is an open implementation issue	of this Safety Assurance activity	
7	Paragraph 8.1 of the Draft Specification states that "Within controlled airspace where primary collision avoidance is provided by ATC"	It is recommended that this requirement is re-worded as follows "Within controlled airspace where primary separation provision is provided by ATC", given that ATC is never responsible for the Collision Avoidance function	**Closed**
8	EUROCONTROL need to consider the implications of UAV operations on SRC Policy Document 2 [8] with respect to the independence of separation provision and collision avoidance systems on UAVs	Feedback provided to SRC via DAP/SAF	**Closed**

7 References

No	Reference	Document Title	Issue/Date
1	UAV-OAT DRAFT SPECS	EUROCONTROL Specifications for the Use of Military Unmanned Aerial Vehicles as Operational Air Traffic Outside Segregated Airspace	Version 0.5 2 December 2004
2	SAF.ET1.ST03.1000-MAN-01	Air Navigation System Safety Assessment Methodology	Edition 2.0 30 April 2004
3	P05005.10.3	UAV Functional Hazard Assessment/Preliminary System Safety Assessment Workshop: Minutes	Issue v1.0 28 June 2005
4	ESARR4	Risk Assessment and Mitigation in ATM	Edition 1.0 05-04-2001
5	JAA JAR25-1309	Classification of Airborne Equipment Failures	-
6	No reference	Draft EUROCONTROL Region Rules for OAT	Edition: 0.5 Date: 19 May 2005
7	AN-Conf/11-WP/4	Appendix A to ATM Operational Concept Document	September 2003
8	SRC POL DOC 2	SRC Policy Document 2: Use of Safety Nets in Risk Assessment & Mitigation in ATM	Edition: 1.0 Date: 28 April 2003
9	AMS.ET1.ST03.4000-TPIAS-01-02	Transition Plan for the Implementation of the EUROCONTROL Airspace Strategy for the ECAC States, Volume 2 Annexes	Edition 1.0, Date 19/04/02
10	ESARR 3	ESARR 3: Use of Safety Management Systems by ATM Service Providers	Edition: 1.0 17 July 2000
11	SAF.ET1.ST01.1000-POL-01-00	EATMP Safety Policy	Edition: 1.1 25 August 1999

Table 12 – Table of References

Appendix A UAV FHA/PSSA Workshop Agenda & Participants

A.1 UAV FHA/PSSA Workshop Agenda

Location: Crowne Plaza Brussels Airport, Brussels

Time: 0900 Wednesday 1st June to 1630 Thursday 2nd June

1. Introductions
    a. Ebeni Team;
    b. UAV FHA Workshop Participants.
2. Overview of the UAV FHA Workshop
    a. Objectives;
    b. Scope;
    c. Technical Approach Summary.
3. Review of UAV Functional and Logical Architecture Models
4. Identification of UAV Hazards
5. Consequence Analysis (ETA)
6. Causal Analysis (FTA)
7. Safety Requirements Implementation Issues
8. Discussion
9. Questions/AOB

A.2 List of FHA/PSSA Workshop Participants

Name	Company	Expertise	Contact Details	Other Info
Maj Michael Alder	Chief Pilot Swiss Ranger	UAV Pilot	michael.alder@vtg.admin.ch	-
Maj Todd Arvidson	NATO E-3 AWACS Navigator	Mil Navigator	todd.arvidson@ramstein.af.mil	-
Lt Col Trond Bakken	EUROCONTROL	Fighter Controller	trond.bakken@eurocontrol.int	TF Chairman
Ian Davies	LM Stasys Limited	ATM	ian.davies@stasys.co.uk	-
Lt Col Oliver Eckstein	German MOD	Mil Navigator	oliver.eckstein@bmvg.bund400.de	TF Member
Derek Fowler	EUROCONTROL	Safety	derek.fowler@eurocontrol.int	-
Capt Volker Göerldt	Bundeswehr GAF	Mil Pilot	volkergoerldt@bundeswehr.org	Day 1 Only
Dave Hilton	Thales/UAVS Association	Industry	dave.hilton@uk.thalesgroup.com	-
Maj Michael Jung	Bundeswehr GAF	Mil/Civil ATCO	michael.jung@bundeswehr.org	Day 2 Only
Lt Col Dave Long	US Army	Airspace coordinator	dave.long@hq.hqusareur.army.mil	Late addition
Benoit Reynders	Verhaert	Industry	benoit.reynders@verhaert.com	-
Michiel Selier	NLR	Dutch OUTCAST Project	selier@nlr.nl	-
Alan Simpson	Ebeni Limted	Safety	alan.simpson@ebeni.biz	FHA Facilitator
Antonio Soares	Maastricht UAC	Civil ATCO	antonio.soares@eurocontrol.int	-
Lt Col Michael Steinfurth	EUROCONTROL	Mil Pilot	michael.steinfurth@eurocontrol.int	-
Joanne Stoker	Ebeni Limted	Safety	jo.stoker@ebeni.biz	FHA Facilitator / Recorder

Wg Cdr Mike Strong	EUROCONTROL	Mil ATCO/ Airspace Policy	michael.strong@eurocontrol.int	FHA Chariman
Alec Trevett	LM Stasys Limited	Air Operations and Safety	alec.trevett@stasys.co.uk	-
Maj Marco Zeemeijer	RNLAF	Mil ATCO	mep.zeemeijer2@mindef.nl	TF Member

Table 13 - UAV FHA/PSSA Workshop Participants

Appendix B UAV-OAT Operational Models

B.1 Scenario Model

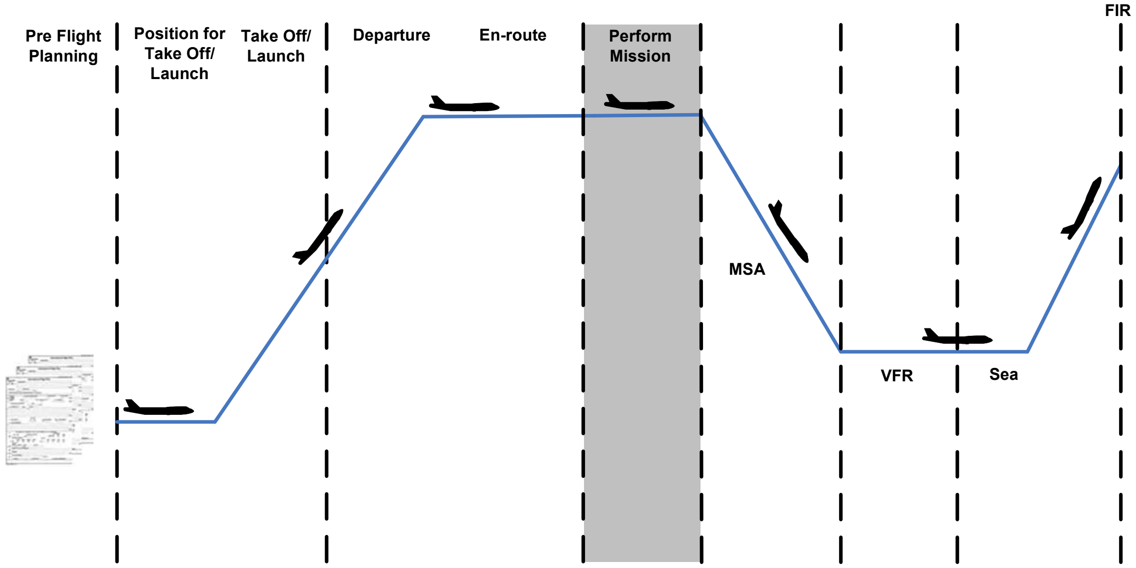


Figure 6 – Scenario Model (1)

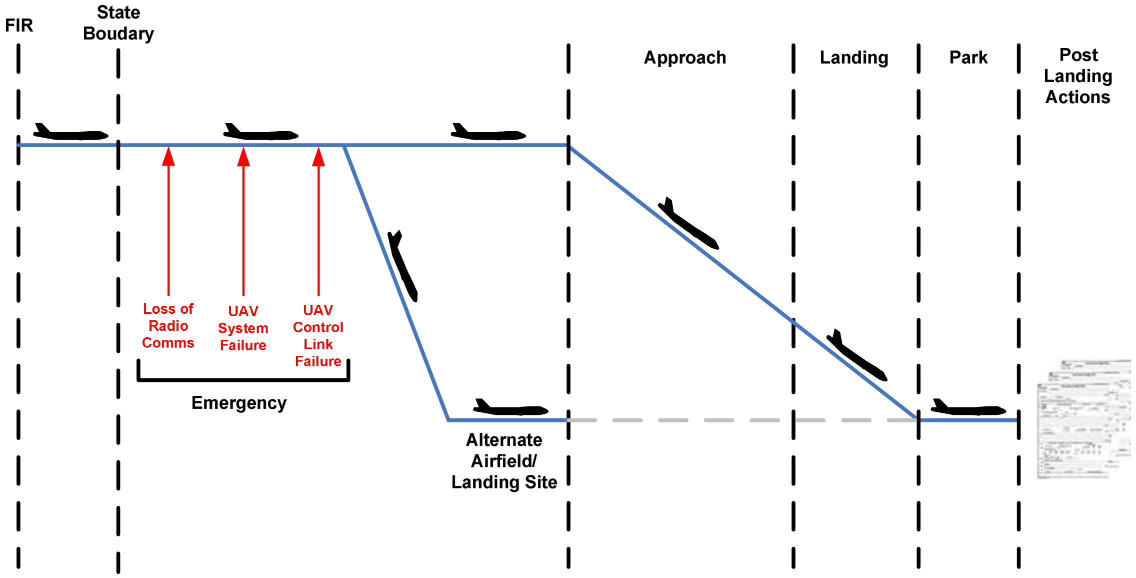


Figure 7 – Scenario Model (2)

B.2 Functional Model – ATC Responsible for Separation

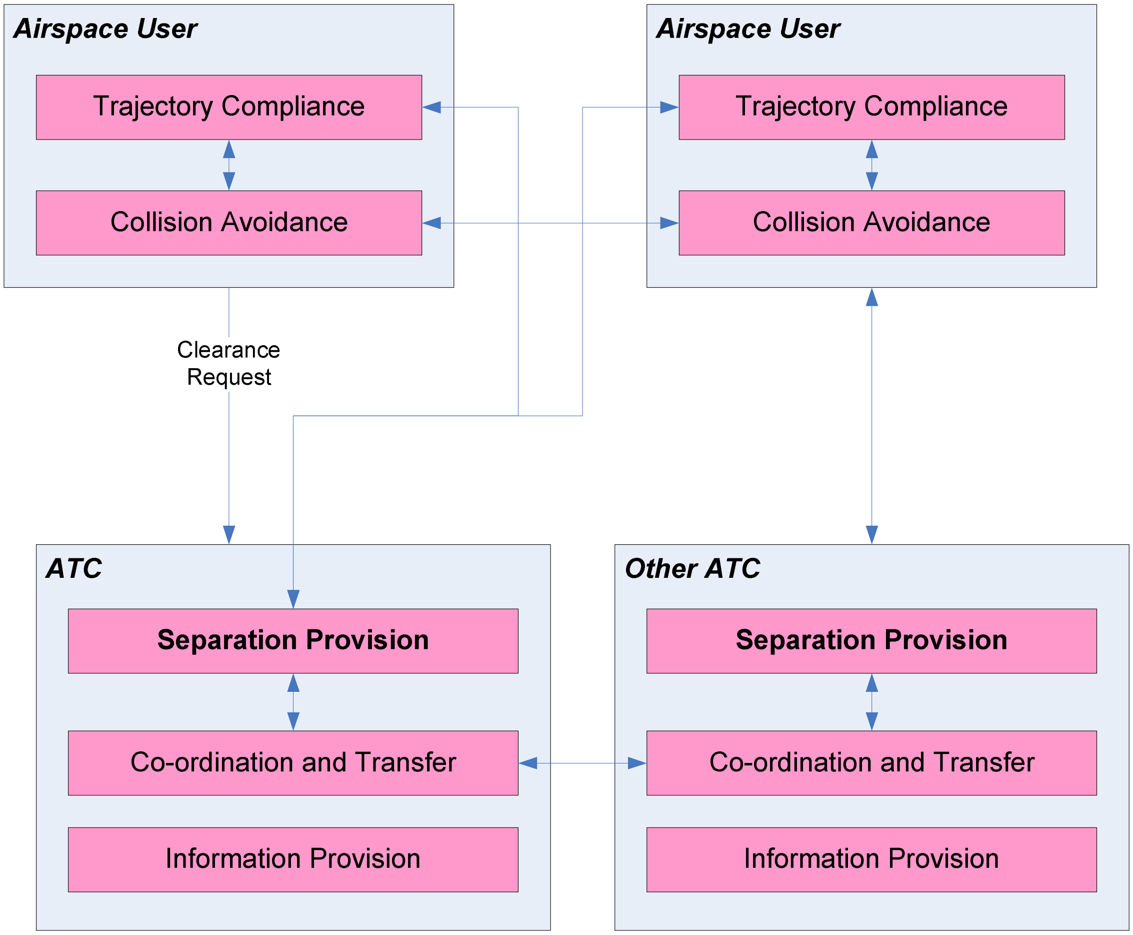


Figure 8 – Functional Model, ATC responsible for Separation

B.3 Functional Model – Pilot in Command Responsible for Separation

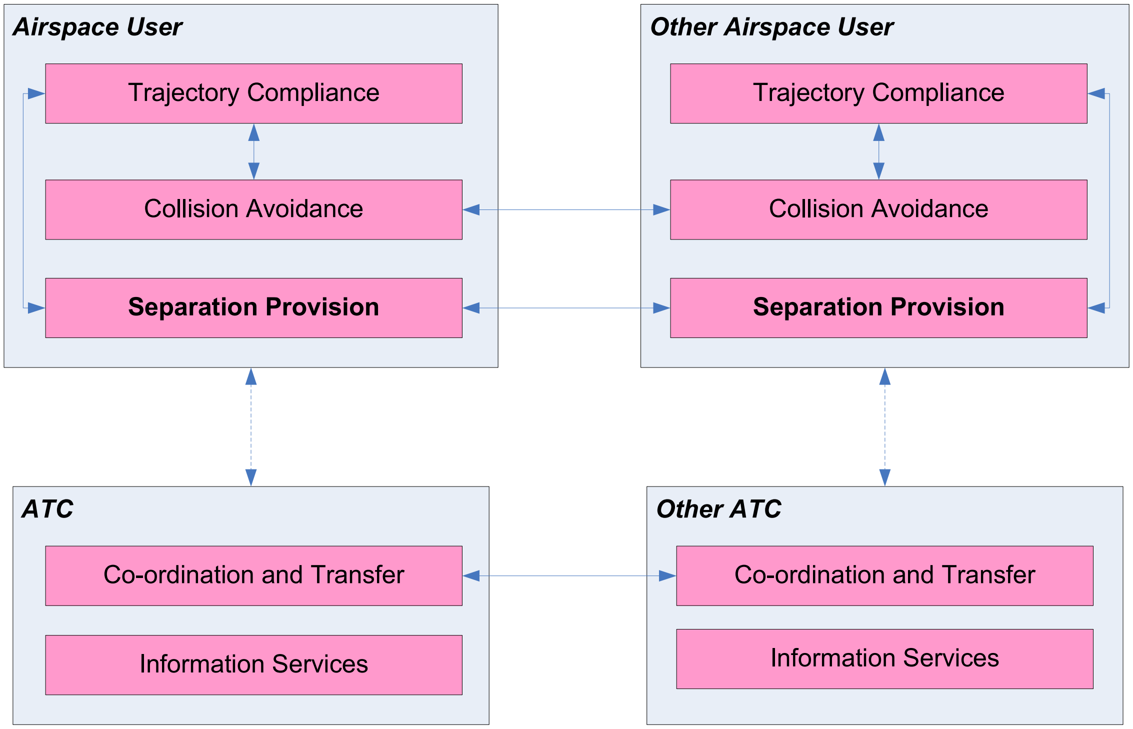


Figure 9 – Functional Model, Pilot in Command responsible for Separation

B.4 Logical Architecture Model – MIL Manned OAT Operations

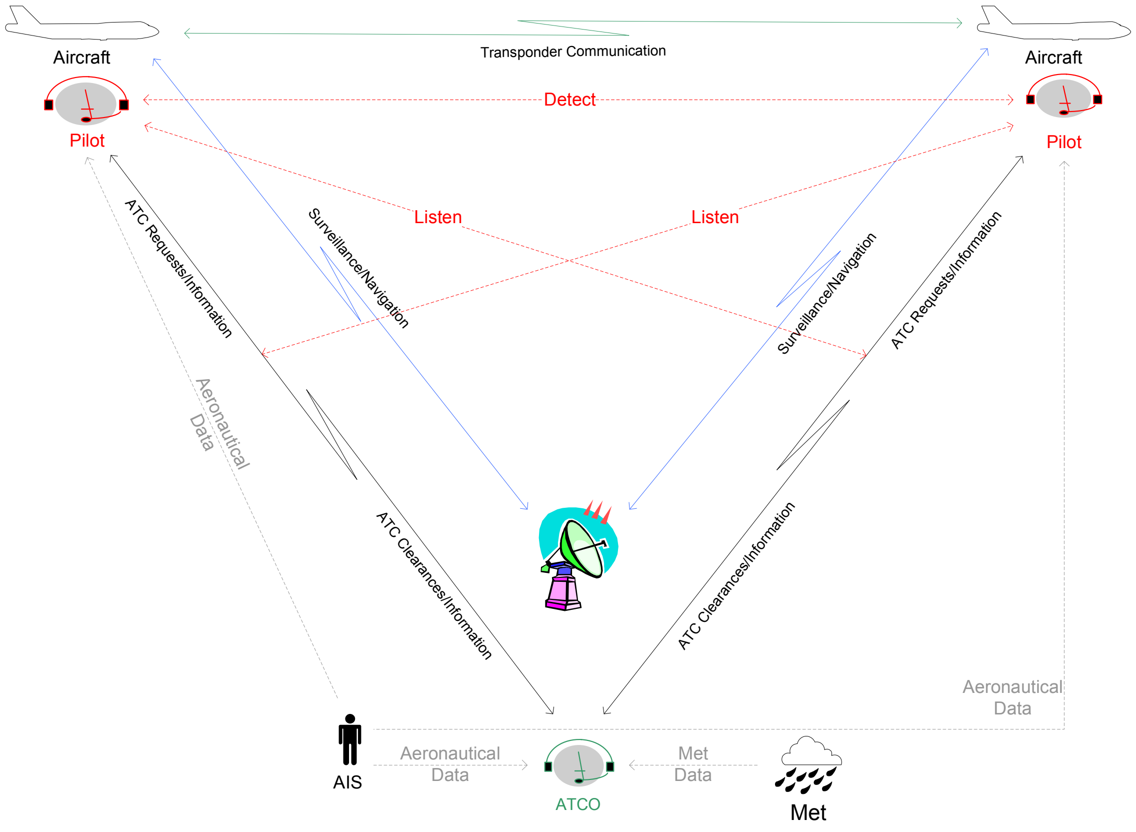


Figure 10 – Logical Architecture Model, Military Manned OAT Operations

B.5 Logical Architecture Model – MIL UAV-OAT Operations

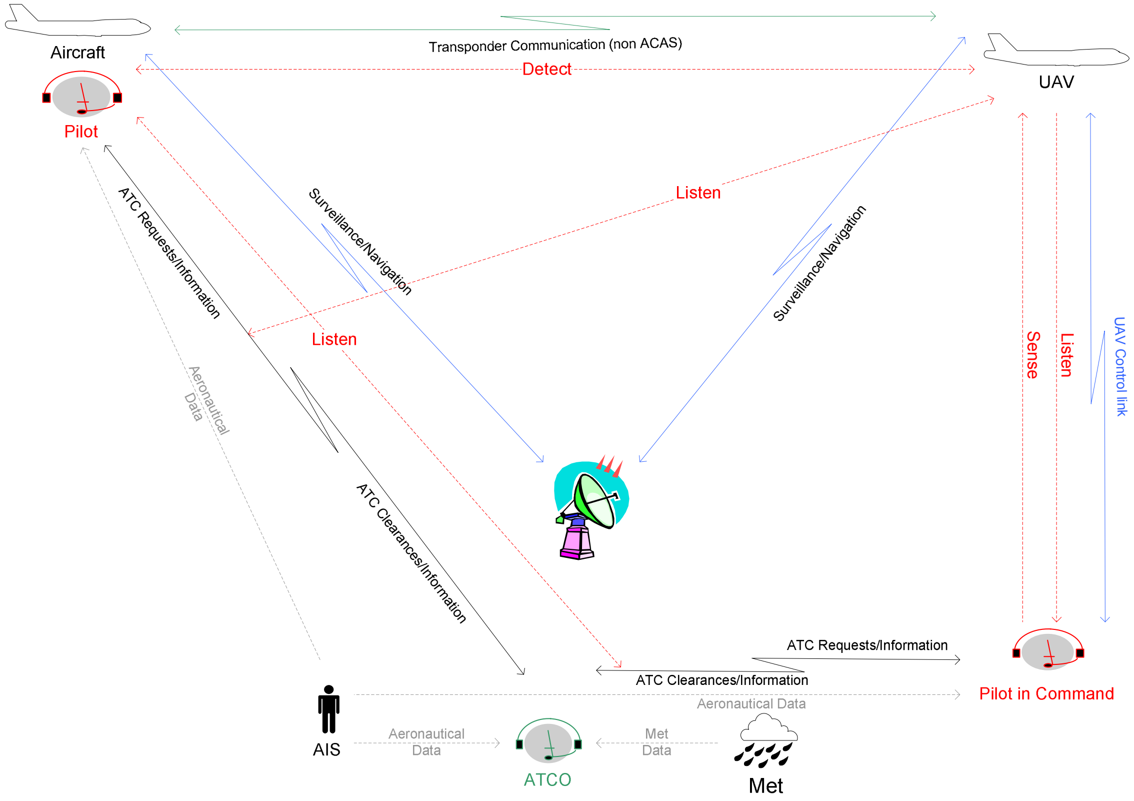


Figure 11 – Logical Architecture Model, Military UAV OAT Operations

B.6 Next Level Logical Model – Pilot in Command

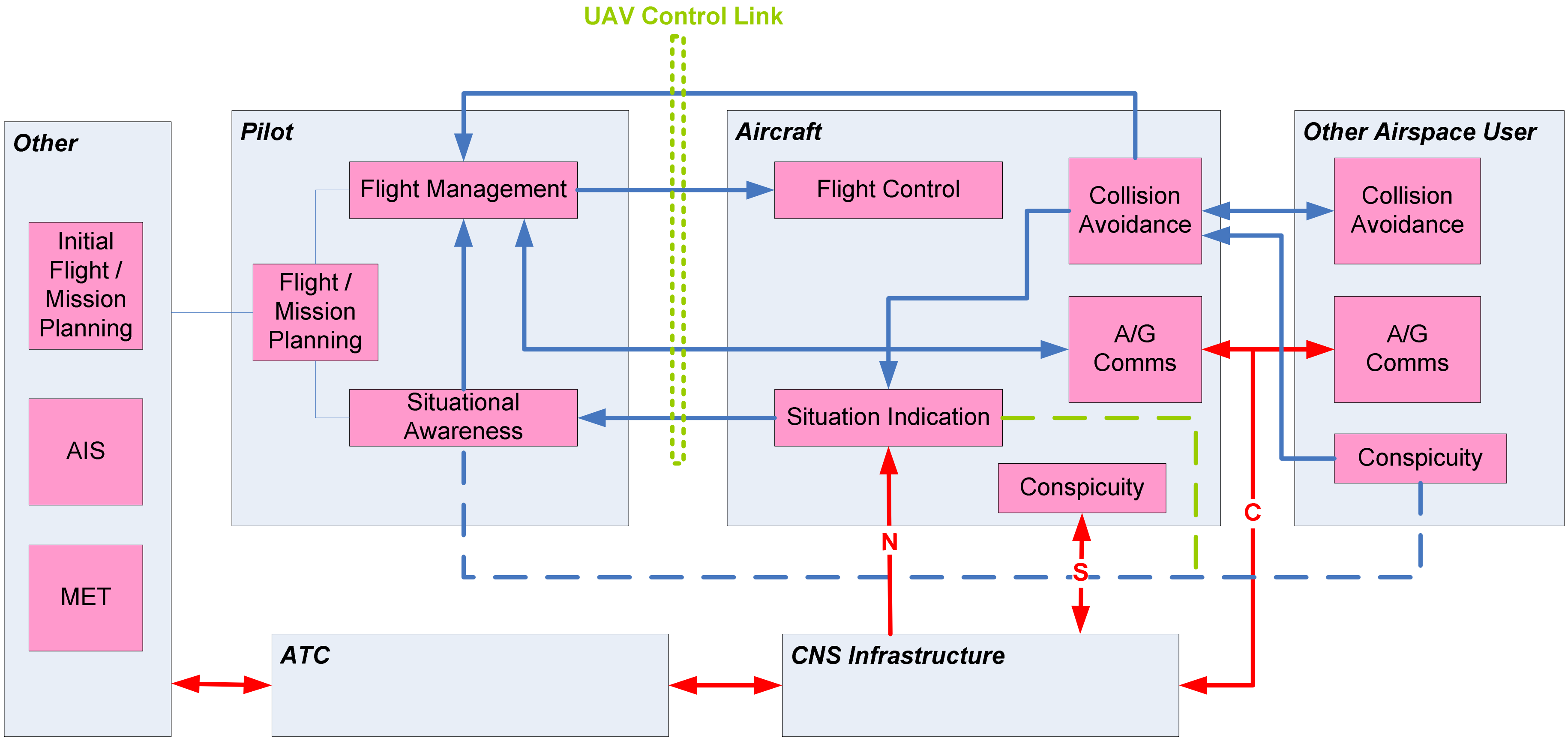


Figure 12 – Next Level Logical Model, Pilot in Command

B.7 Next Level Logical Model – Autonomous UAV

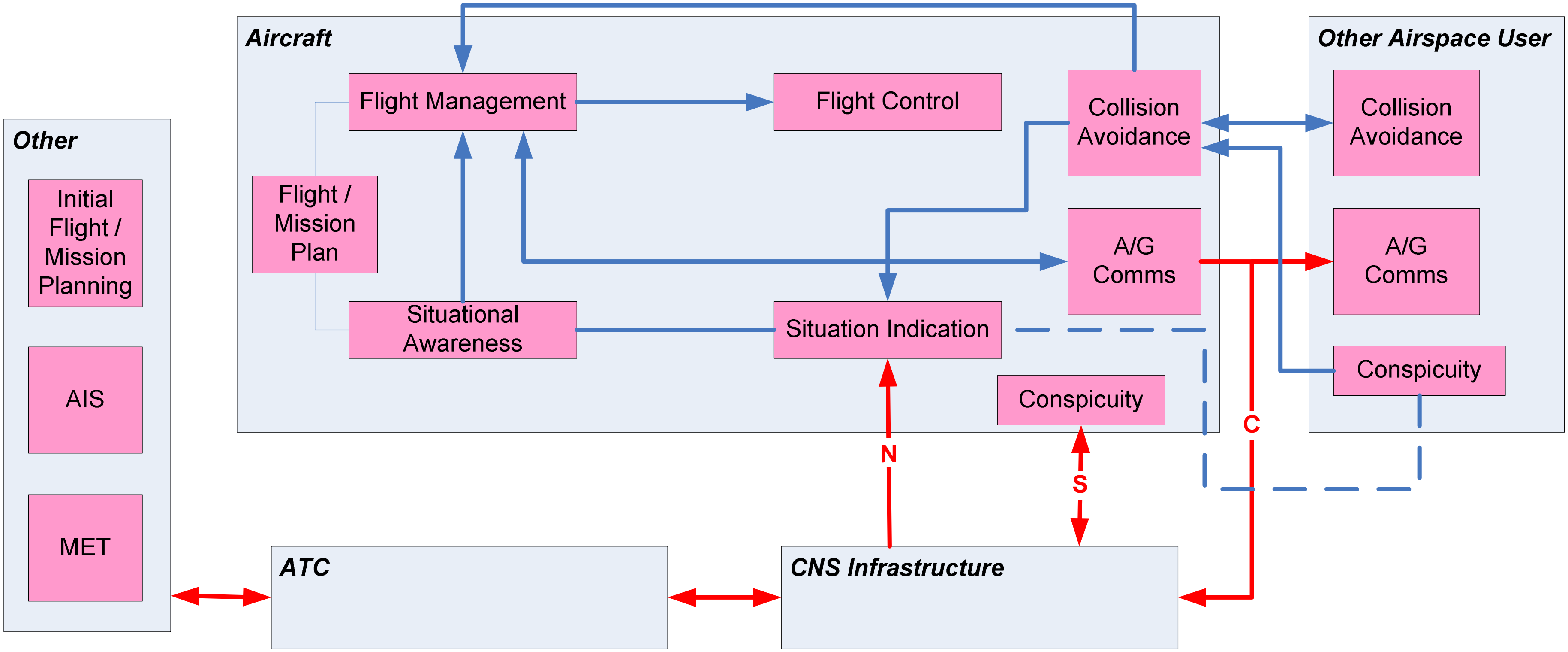


Figure 13 – Next Level Logical Model, Autonomous UAV

Appendix C Hazard and Risk Assessment Concepts and Terminology

Hazard to Accident modelling provides a mechanism for capturing the relationship between lower level events such as system failures, data error, etc. and higher level consequences.

The model first requires a clear definition of the system to be analysed. A system is a defined set of integrated elements (e.g. people, procedures, equipment) necessary to perform one or more functions. Most commonly in hazard analysis, the system under consideration is part of a larger system or interacts with other systems. In order to scope the boundary of the analysis it is necessary to define the boundary of the system. This boundary determines the relevance of accident and hazard sequences to the system under consideration

An **accident** is an unintended event that results in death or serious injury. Accidents occur in the real world. A **hazard** is a system state that can lead to an accident, and should be described at the boundary of the system, as indicated in Figure 14.

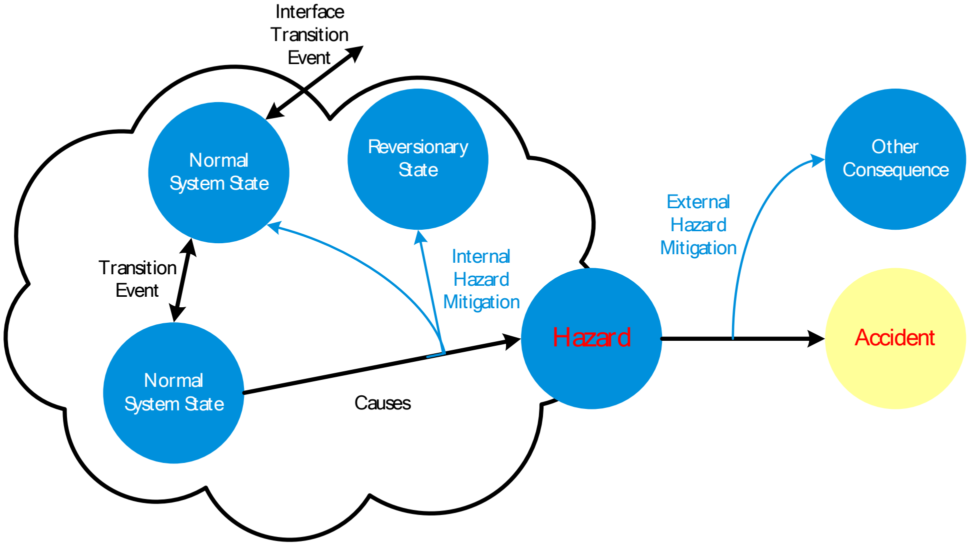


Figure 14 – Generic Hazard Model

When a system hazard has occurred, the system has no control over the consequences – i.e. it has in itself no means of stopping an accident occurring, although external mitigations (including pure chance) may reduce the likelihood of an accident[9]. Failures within a system that may cause hazards are called **causes** and it is important to distinguish them from hazards. Causes are properties of the design of the system and they determine the likelihood of occurrence of a hazard, but not its consequences. The chain of events from root cause through the accident is called a hazard chain.

Where the system is made up of a number of subsystems, the model can be modified as shown in Figure 15 with hazards defined at the boundary of each subsystem.

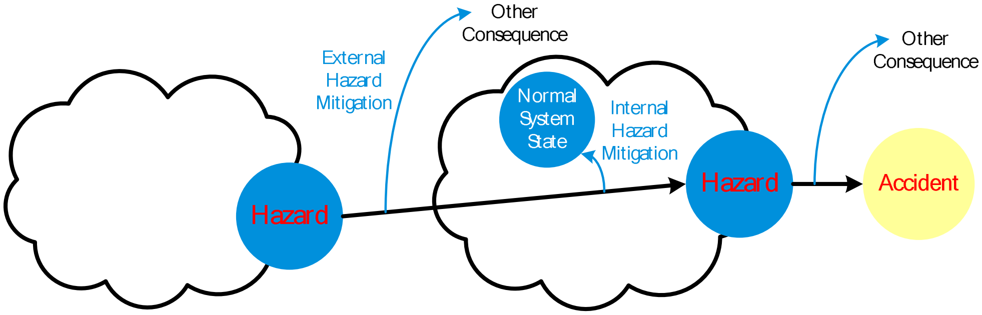


Figure 15 – Subsystem Interactions

The initial task of the Functional Hazard Assessment (FHA) is to develop the functional model from which the hazard analysis can be performed.

Hazard and Risk Analysis is carried out primarily by use of a “Bow-Tie” model, as illustrated in Figure 16, in which all the causes captured in a Fault Tree are linked directly to the possible outcomes (i.e. consequences) captured in an Event Tree.

The Event Tree is used to model all the credible outcomes of a hazard taking account of the mitigations that could break an accident sequence in the event that the hazard occurs. Working from left to right, each

[9] Note that the intended system function may be to detect and mitigate hazards of other systems. In this case, the system may not generate hazards in itself but is nonetheless safety-related.

branch of the Event Tree represents a mitigation to which probabilities can be applied, normally in order to express the relative likelihood of success (S) or failure (F) of the mitigation[10].

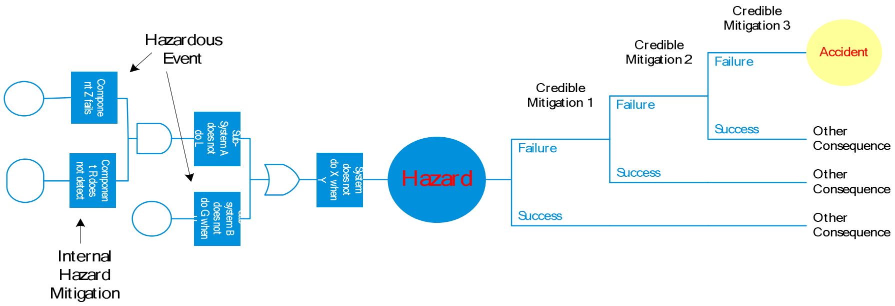


Figure 16 – “Bow-Tie” Model

In summary, given all the causes, consequences and credible mitigations of a hazard, the combination of Event Tree Analysis and Fault Tree Analysis in the “Bow-Tie” model provides a model that can be used in the FHA/PSSA activity to subsequently derive safety objectives and safety requirements

[10] Some mitigations in an event tree can be complex probability sets, for example where the system’s mode of operation is relevant to the outcome of the hazard chain.

Appendix D Severity Classification Scheme

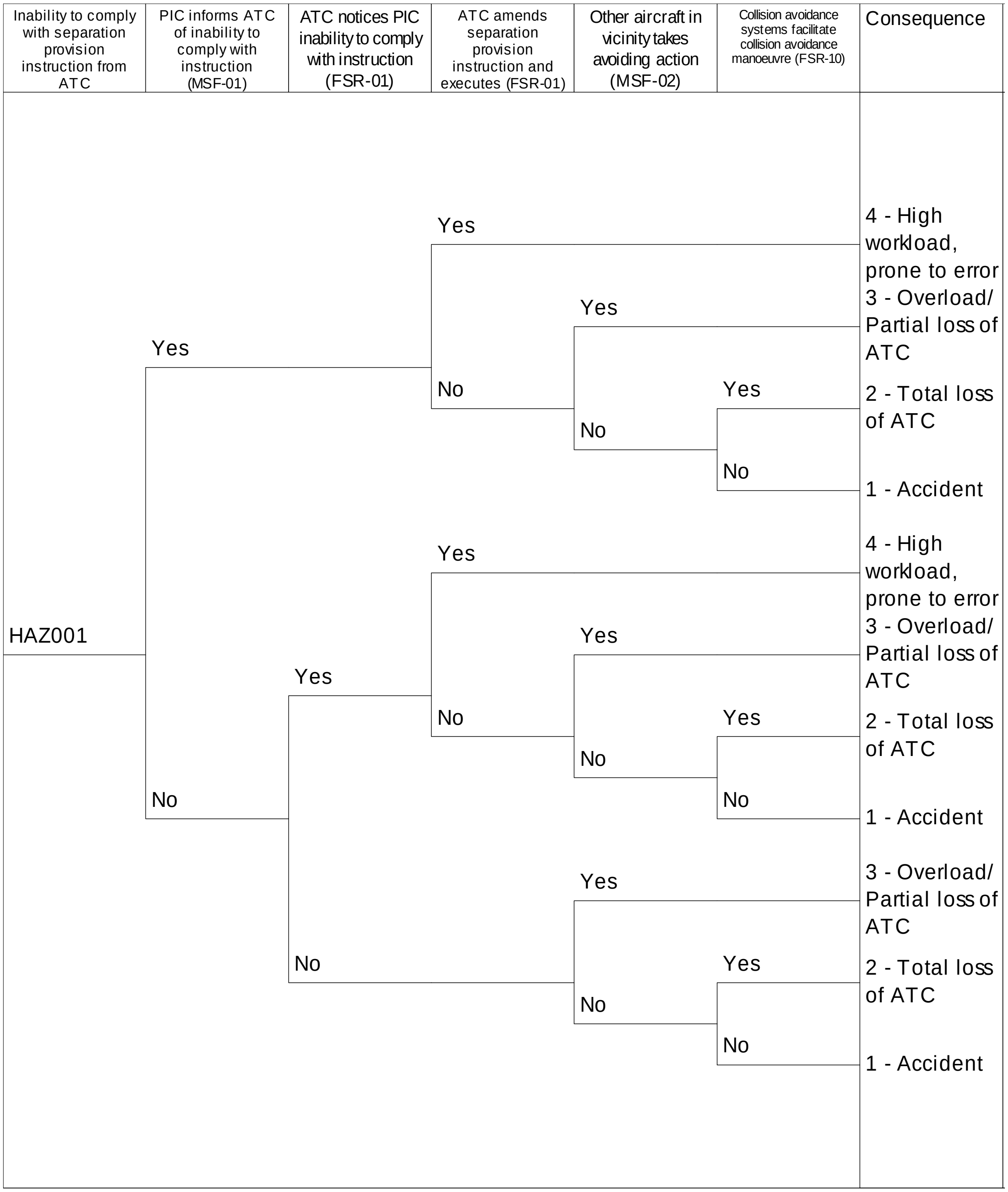
Effect	1. Complete loss of safety margins	2. Large reduction in safety margins	3. Major reduction in safety margins	4. Slight reduction in safety margins	5. No effect on safety
Examples of effects include	Accidents, including:- • one or more catastrophic accidents, • one or more mid-air collisions, • Total loss of flight control. No independent source of recovery mechanism, such as surveillance or ATC and/or flight crew procedures can reasonably be expected to prevent the accident(s).	Serious incidents, including: • large reduction in separation (e.g., more than half the separation minima), without crew or ATC fully controlling the situation or able to recover from the situation, or • abrupt collision or terrain avoidance manoeuvres are required to avoid an accident (or when an avoidance action would be	Major incidents, including: • large reduction in separation (e.g., more than half the separation minima) with crew or ATC fully controlling the situation and able to recover from the situation, • major reduction in separation (e.g., less than half the separation minima) without crew or ATC fully controlling the situation, hence	Significant incidents, including: • no direct impact on safety but indirect impact by increasing the workload of the ATCO or aircraft flight crew, or slightly degrading the functional capability of the enabling CNS system, • major reduction in separation (e.g., less than half the separation minima) with crew or ATC	No hazardous condition i.e. no direct or indirect impact to the operations.

		appropriate), or • a probability of structural damage (or serious injury) to crew or passengers.	jeopardising the ability to recover from the situation (without the use of collision avoidance manoeuvres).	controlling the situation and fully able to recover from the situation.	
Alternative definitions	Collision	Total loss of ability to maintain separation.	Ability to maintain separations is severely compromised.	Ability to maintain separations is impaired.	As above.

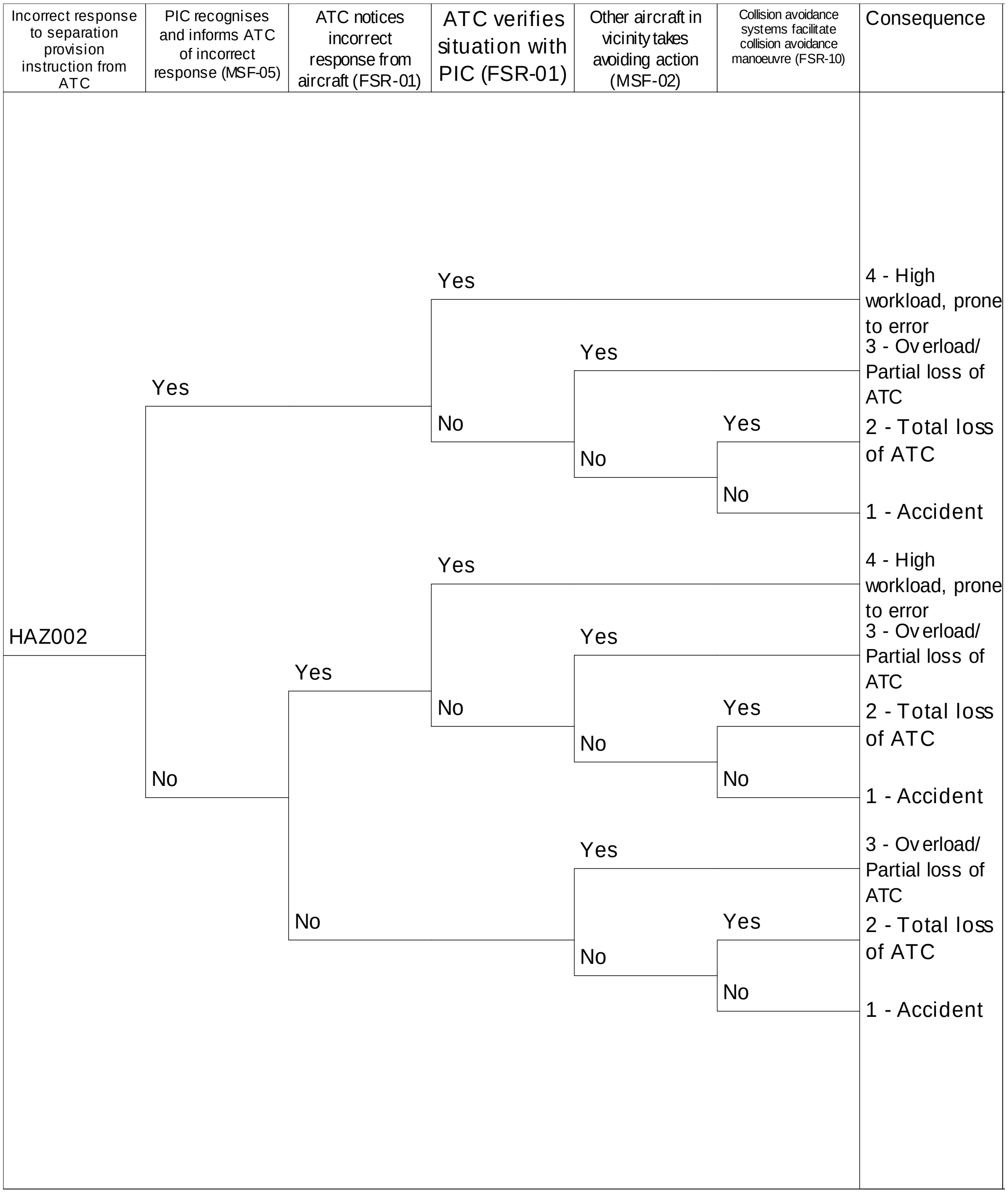
Table 14 – Severity Classification Scheme

Appendix E Event Trees

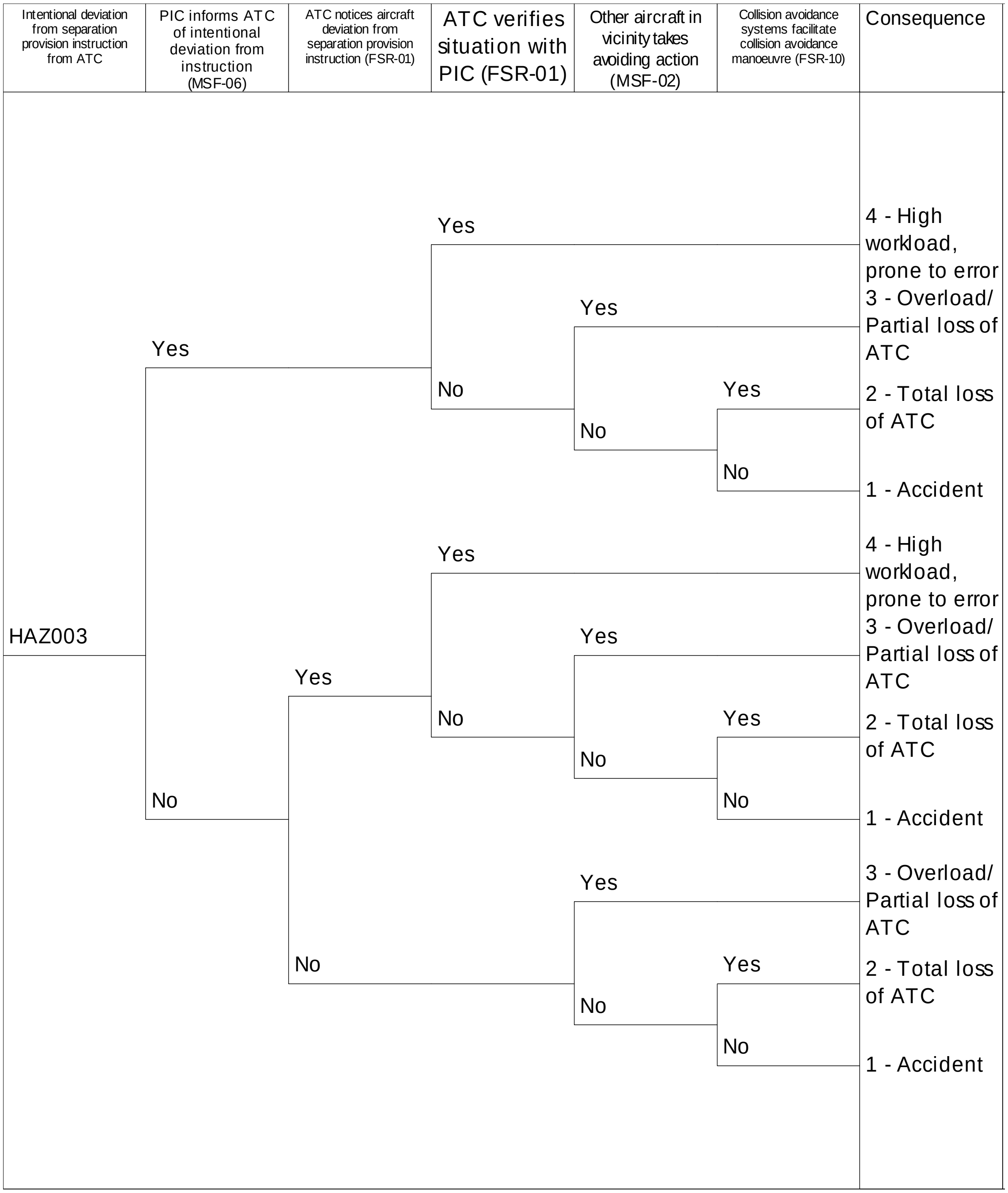
E.1 HAZ001 – Without and With UAVs


Inability to comply with separation provision instruction from ATC
PIC informs ATC of inability to comply with instruction (MSF-01)
ATC notices PIC inability to comply with instruction (FSR-01)
ATC amends separation provision instruction and executes (FSR-01)
Other aircraft in vicinity takes avoiding action (MSF-02)
Collision avoidance systems facilitate collision avoidance manoeuvre (FSR-10)
Consequence
HAZ001
Yes
No
Yes
No
Yes
No
Yes
No
Yes
No
Yes
No
Yes
No
Yes
No
Yes
No
Yes
No
4 - High workload, prone to error
3 - Overload/ Partial loss of ATC
2 - Total loss of ATC
1 - Accident
4 - High workload, prone to error
3 - Overload/ Partial loss of ATC
2 - Total loss of ATC
1 - Accident
3 - Overload/ Partial loss of ATC
2 - Total loss of ATC
1 - Accident

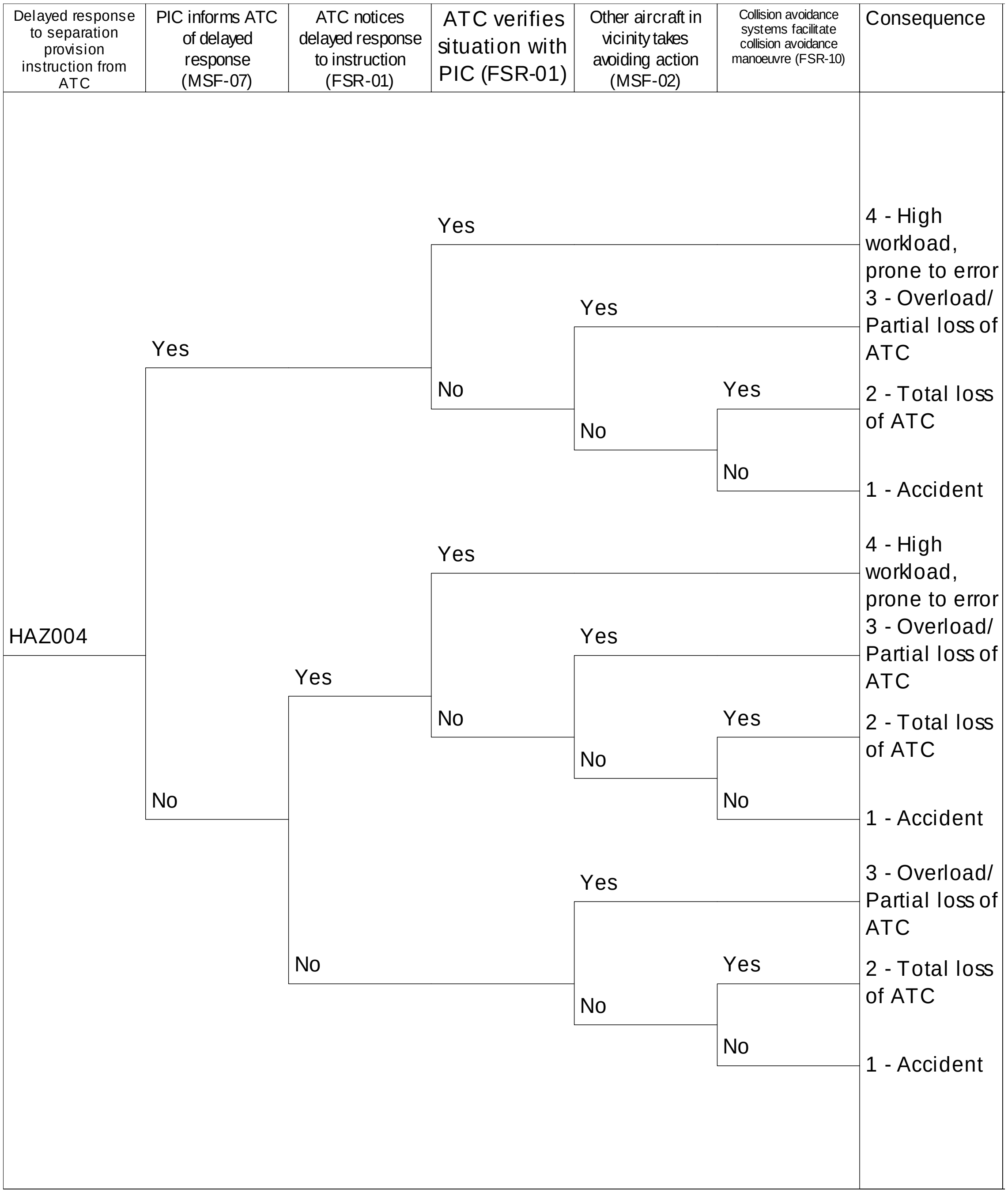
E.2 HAZ002 – Without and With UAVs


Incorrect response to separation provision instruction from ATC
PIC recognises and informs ATC of incorrect response (MSF-05)
ATC notices incorrect response from aircraft (FSR-01)
ATC verifies situation with PIC (FSR-01)
Other aircraft in vicinity takes avoiding action (MSF-02)
Collision avoidance systems facilitate collision avoidance manoeuvre (FSR-10)
Consequence
HAZ002
Yes
No
Yes
No
Yes
No
Yes
No
Yes
No
4 - High workload, prone to error
3 - Overload/ Partial loss of ATC
2 - Total loss of ATC
1 - Accident
4 - High workload, prone to error
3 - Overload/ Partial loss of ATC
2 - Total loss of ATC
1 - Accident
3 - Overload/ Partial loss of ATC
2 - Total loss of ATC
1 - Accident

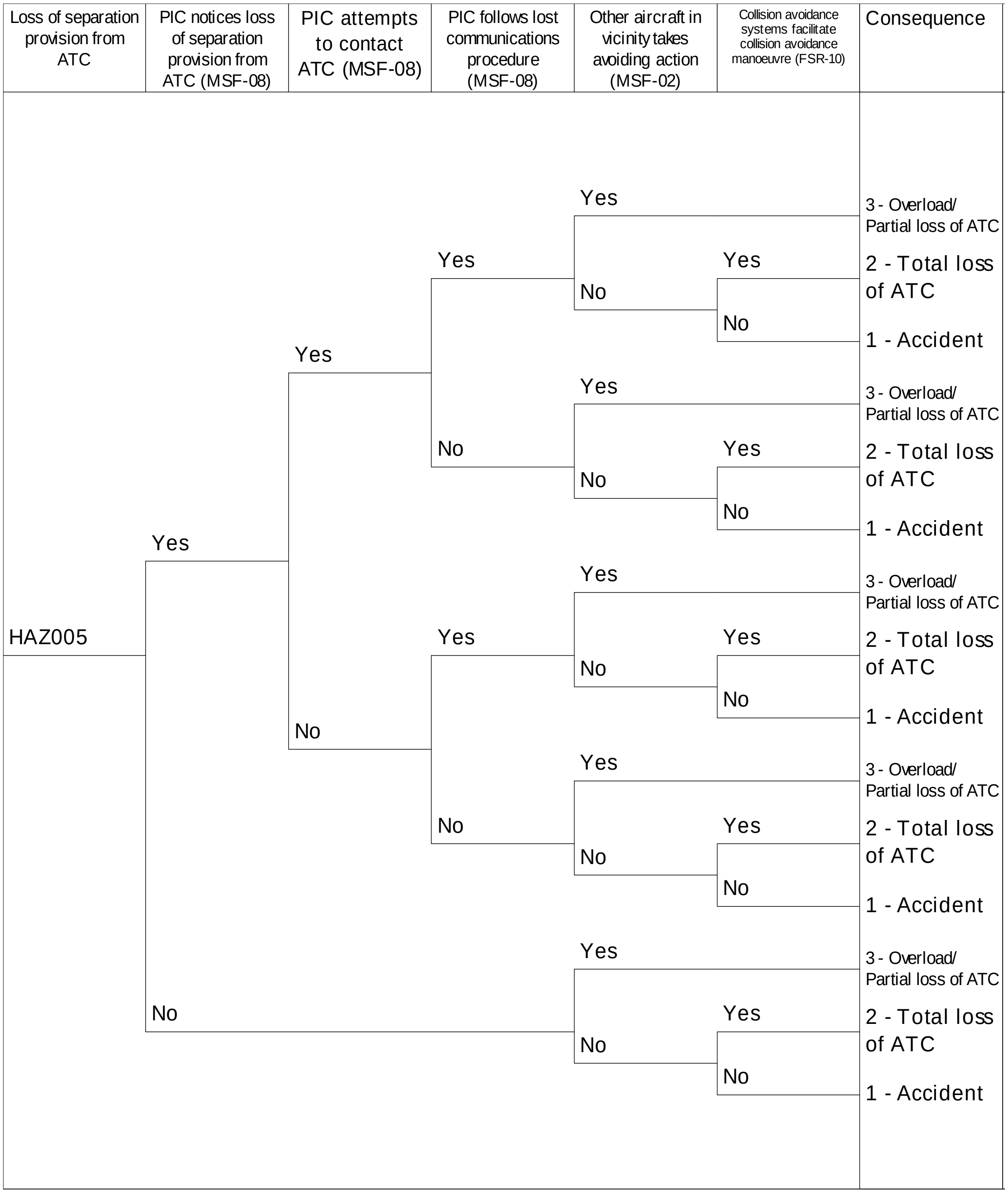
E.3 HAZ003 – Without and With UAVs


Intentional deviation from separation provision instruction from ATC
PIC informs ATC of intentional deviation from instruction (MSF-06)
ATC notices aircraft deviation from separation provision instruction (FSR-01)
ATC verifies situation with PIC (FSR-01)
Other aircraft in vicinity takes avoiding action (MSF-02)
Collision avoidance systems facilitate collision avoidance manoeuvre (FSR-10)
Consequence
HAZ003
Yes
No
Yes
No
Yes
No
Yes
No
Yes
No
Yes
No
Yes
No
Yes
No
Yes
No
Yes
No
4 - High workload, prone to error
3 - Overload/ Partial loss of ATC
2 - Total loss of ATC
1 - Accident
4 - High workload, prone to error
3 - Overload/ Partial loss of ATC
2 - Total loss of ATC
1 - Accident
3 - Overload/ Partial loss of ATC
2 - Total loss of ATC
1 - Accident

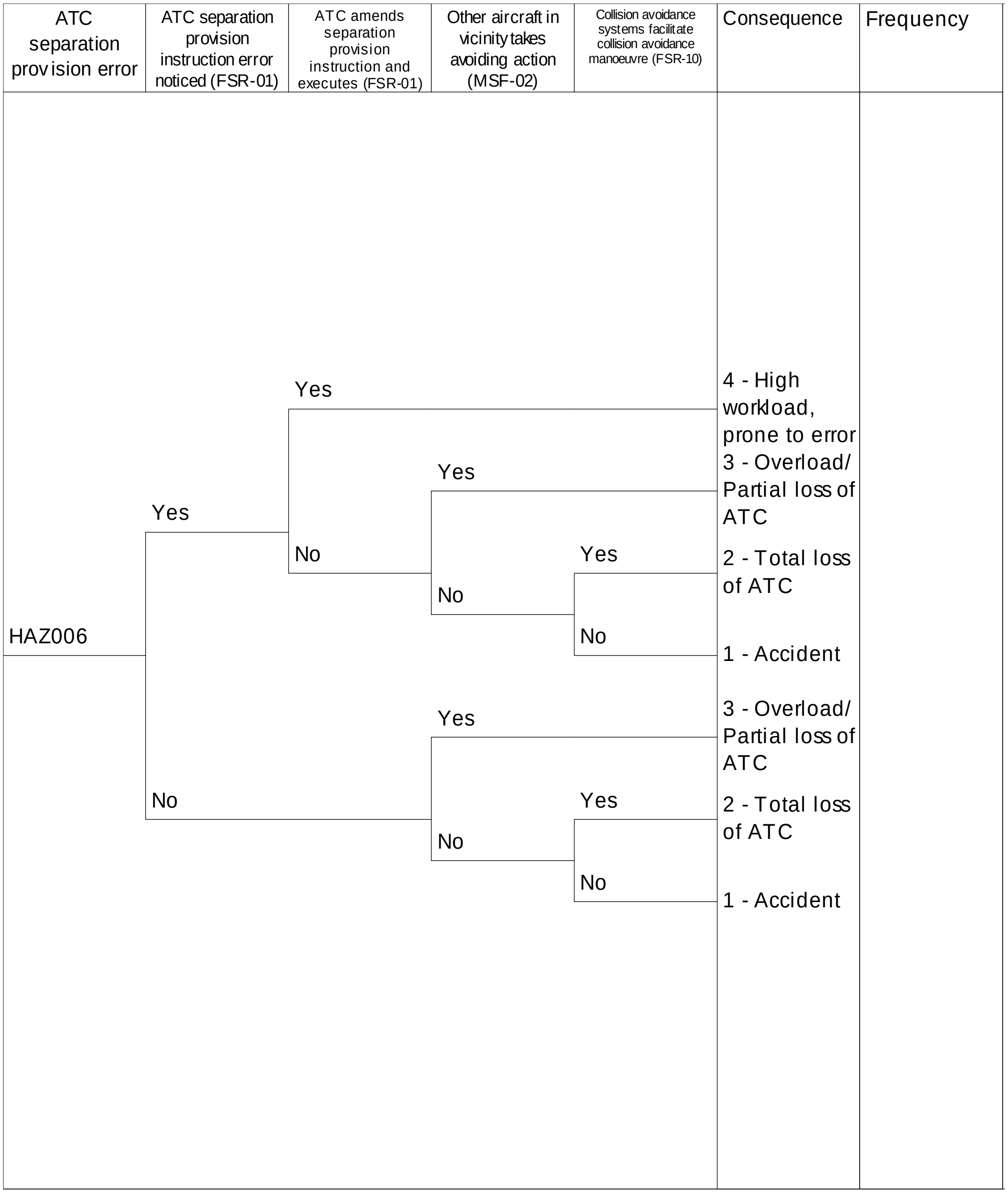
E.4 HAZ004 – Without and With UAVs


Delayed response to separation provision instruction from ATC
PIC informs ATC of delayed response (MSF-07)
ATC notices delayed response to instruction (FSR-01)
ATC verifies situation with PIC (FSR-01)
Other aircraft in vicinity takes avoiding action (MSF-02)
Collision avoidance systems facilitate collision avoidance manoeuvre (FSR-10)
Consequence
HAZ004
Yes
Yes
No
Yes
No
Yes
No
4 - High workload, prone to error
3 - Overload/ Partial loss of ATC
2 - Total loss of ATC
1 - Accident
No
Yes
Yes
No
Yes
No
Yes
No
4 - High workload, prone to error
3 - Overload/ Partial loss of ATC
2 - Total loss of ATC
1 - Accident
No
Yes
No
Yes
No
3 - Overload/ Partial loss of ATC
2 - Total loss of ATC
1 - Accident

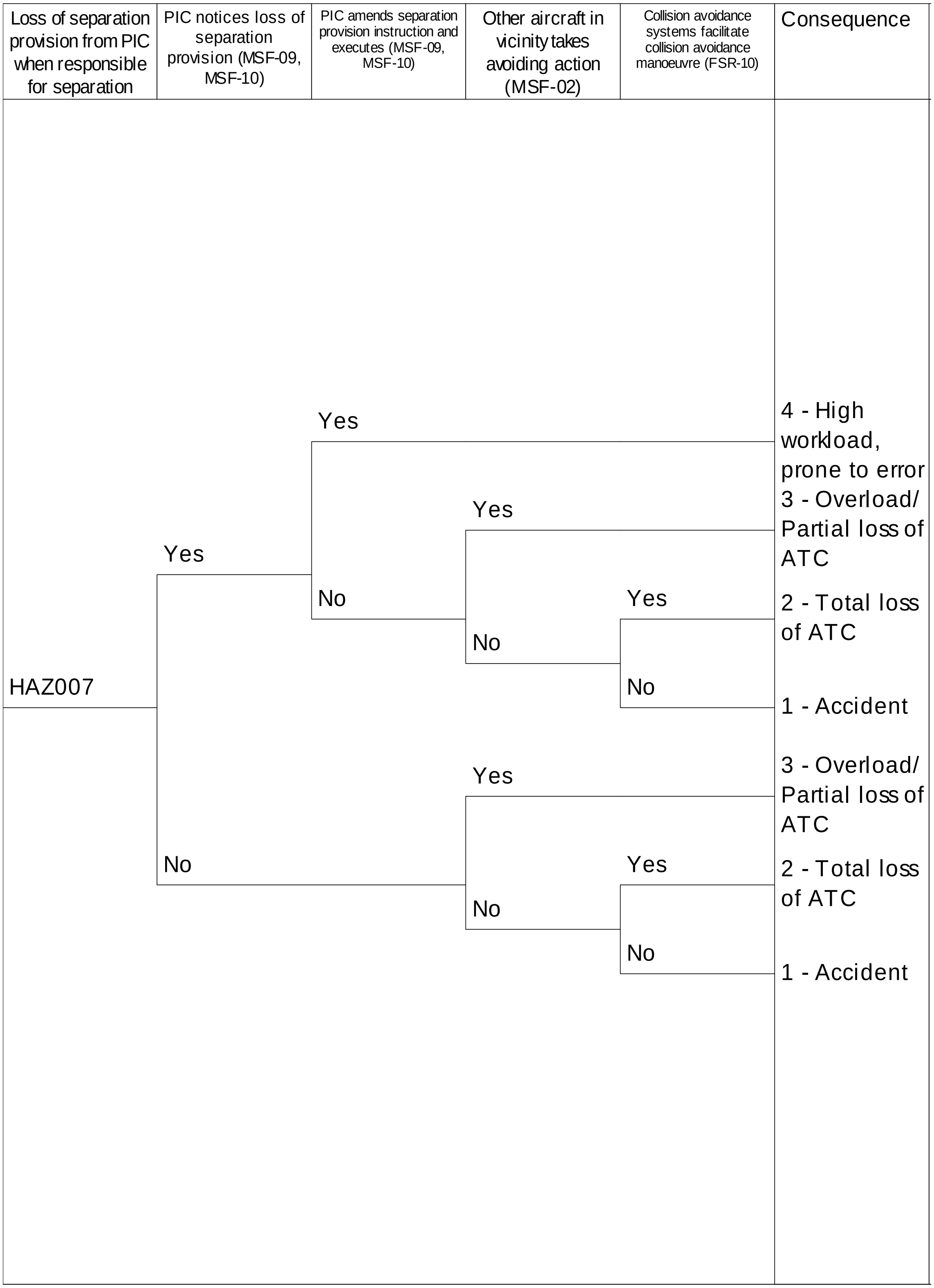
E.5 HAZ005 – Without and With UAVs


Loss of separation provision from ATC
PIC notices loss of separation provision from ATC (MSF-08)
PIC attempts to contact ATC (MSF-08)
PIC follows lost communications procedure (MSF-08)
Other aircraft in vicinity takes avoiding action (MSF-02)
Collision avoidance systems facilitate collision avoidance manoeuvre (FSR-10)
Consequence
HAZ005
Yes
No
Yes
No
Yes
No
Yes
No
Yes
No
Yes
No
Yes
No
Yes
No
Yes
No
Yes
No
Yes
No
Yes
No
Yes
No
Yes
No
Yes
No
Yes
No
Yes
No
Yes
No
3 - Overload/ Partial loss of ATC
2 - Total loss of ATC
1 - Accident
3 - Overload/ Partial loss of ATC
2 - Total loss of ATC
1 - Accident
3 - Overload/ Partial loss of ATC
2 - Total loss of ATC
1 - Accident
3 - Overload/ Partial loss of ATC
2 - Total loss of ATC
1 - Accident
3 - Overload/ Partial loss of ATC
2 - Total loss of ATC
1 - Accident

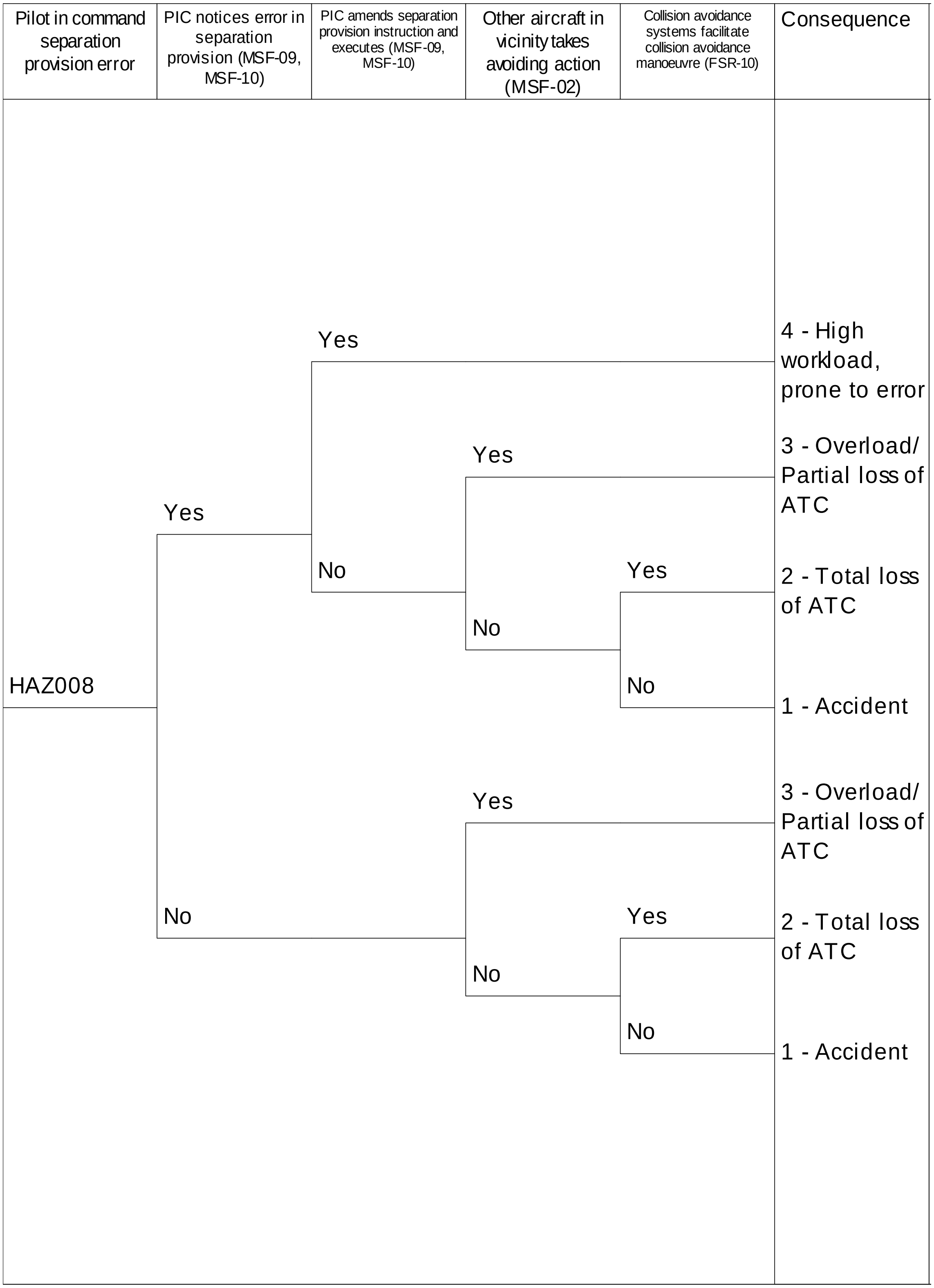
E.6 HAZ006 – Without and With UAVs


ATC separation provision error
ATC separation provision instruction error noticed (FSR-01)
ATC amends separation provision instruction and executes (FSR-01)
Other aircraft in vicinity takes avoiding action (MSF-02)
Collision avoidance systems facilitate collision avoidance manoeuvre (FSR-10)
Consequence
Frequency
HAZ006
Yes
No
Yes
No
Yes
No
Yes
No
Yes
No
Yes
No
4 - High workload, prone to error
3 - Overload/ Partial loss of ATC
2 - Total loss of ATC
1 - Accident
3 - Overload/ Partial loss of ATC
2 - Total loss of ATC
1 - Accident

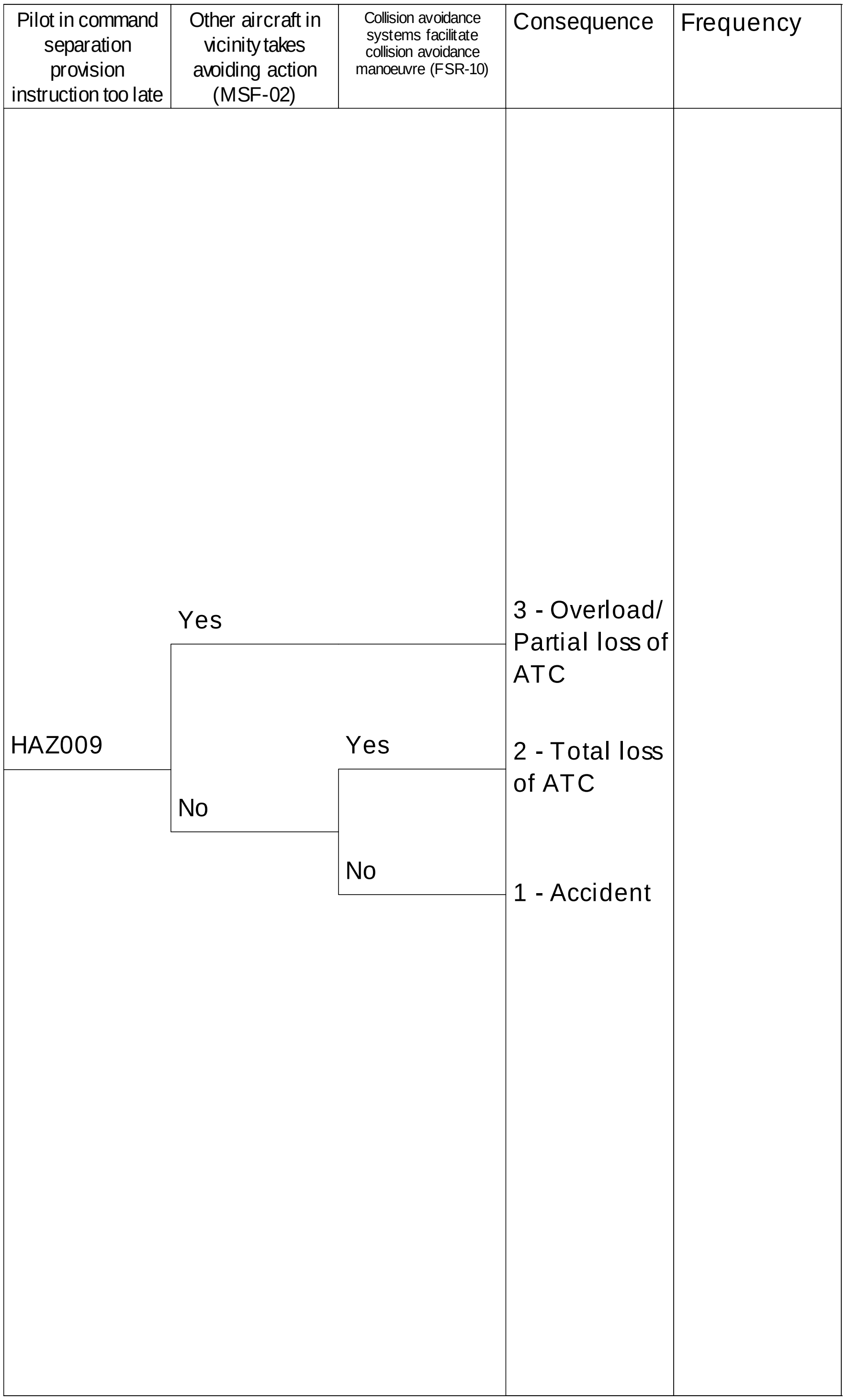
E.7 HAZ007 – Without and With UAVs


Loss of separation provision from PIC when responsible for separation
PIC notices loss of separation provision (MSF-09, MSF-10)
PIC amends separation provision instruction and executes (MSF-09, MSF-10)
Other aircraft in vicinity takes avoiding action (MSF-02)
Collision avoidance systems facilitate collision avoidance manoeuvre (FSR-10)
Consequence
HAZ007
Yes
Yes
No
Yes
No
Yes
No
No
Yes
Yes
No
No
4 - High workload, prone to error
3 - Overload/ Partial loss of ATC
2 - Total loss of ATC
1 - Accident
3 - Overload/ Partial loss of ATC
2 - Total loss of ATC
1 - Accident

E.8 HAZ008 – Without and With UAVs


Pilot in command separation provision error
PIC notices error in separation provision (MSF-09, MSF-10)
PIC amends separation provision instruction and executes (MSF-09, MSF-10)
Other aircraft in vicinity takes avoiding action (MSF-02)
Collision avoidance systems facilitate collision avoidance manoeuvre (FSR-10)
Consequence
HAZ008
Yes
No
Yes
No
Yes
No
Yes
No
Yes
No
Yes
No
4 - High workload, prone to error
3 - Overload/ Partial loss of ATC
2 - Total loss of ATC
1 - Accident
3 - Overload/ Partial loss of ATC
2 - Total loss of ATC
1 - Accident

E.9 HAZ009 – Without and With UAVs


Pilot in command separation provision instruction too late
Other aircraft in vicinity takes avoiding action (MSF-02)
Collision avoidance systems facilitate collision avoidance manoeuvre (FSR-10)
Consequence
Frequency
Yes
3 - Overload/ Partial loss of ATC
HAZ009
Yes
2 - Total loss of ATC
No
No
1 - Accident

Appendix F Fault Trees

F.1 Loss of Separation Provision

F.1.1 HAZ001 – Inability to comply with separation provision instruction from ATC (Situation 1: Manned Air Vehicle)

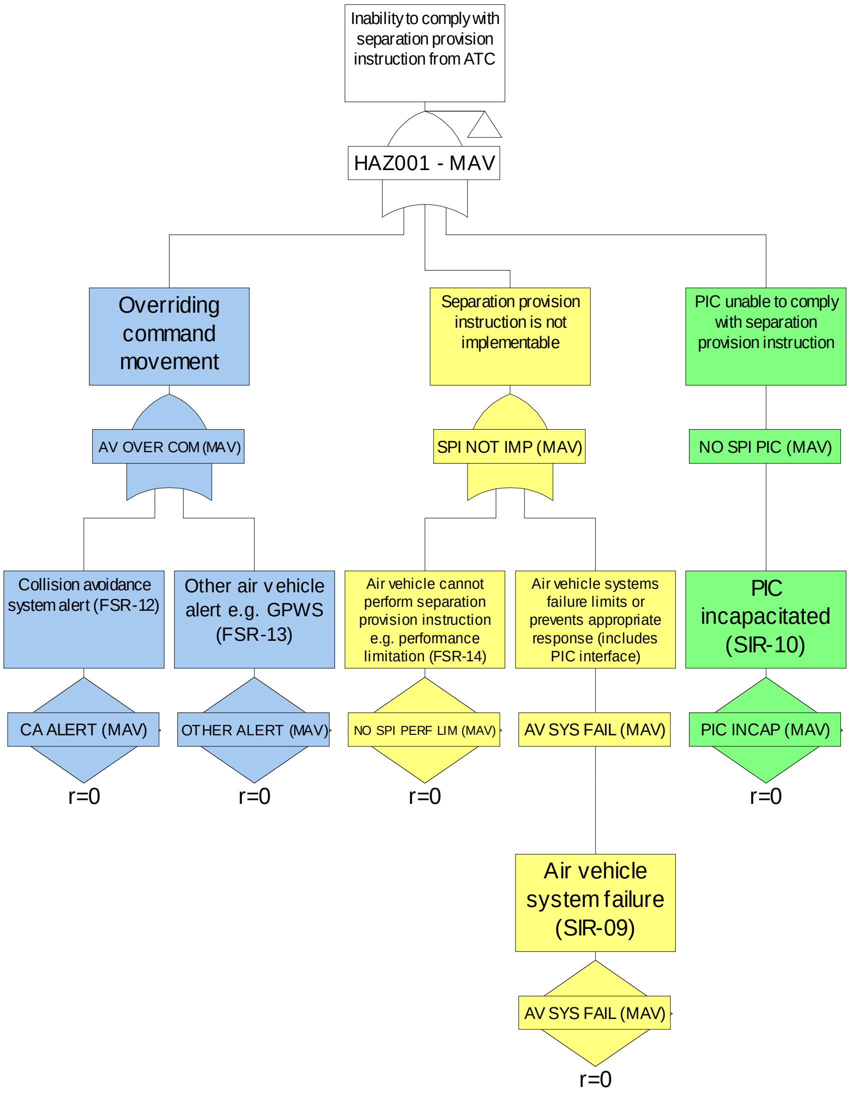

Inability to comply with separation provision instruction from ATC
HAZ001 - MAV
Overriding command movement
AV OVER COM (MAV)
Separation provision instruction is not implementable
SPI NOT IMP (MAV)
PIC unable to comply with separation provision instruction
NO SPI PIC (MAV)
Collision avoidance system alert (FSR-12)
CA ALERT (MAV)
r=0
Other air vehicle alert e.g. GPWS (FSR-13)
OTHER ALERT (MAV)
r=0
Air vehicle cannot perform separation provision instruction e.g. performance limitation (FSR-14)
NO SPI PERF LIM (MAV)
r=0
Air vehicle systems failure limits or prevents appropriate response (includes PIC interface)
AV SYS FAIL (MAV)
PIC incapacitated (SIR-10)
PIC INCAP (MAV)
r=0
Air vehicle system failure (SIR-09)
AV SYS FAIL (MAV)
r=0

Figure 17 – HAZ001 Situation 1: Manned Air Vehicle

F.1.2 HAZ001 – Inability to comply with separation provision instruction from ATC (Situation 2: UAV with PIC)

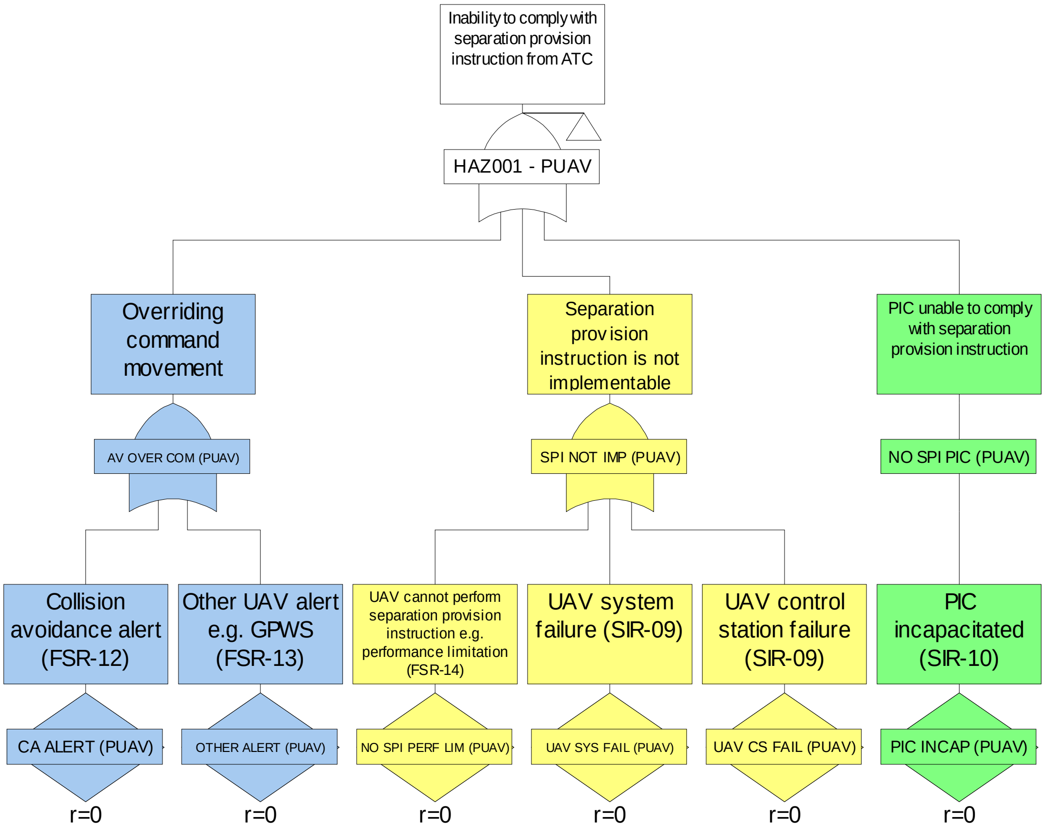

Inability to comply with separation provision instruction from ATC
HAZ001 - PUAV
Overriding command movement
AV OVER COM (PUAV)
Separation provision instruction is not implementable
SPI NOT IMP (PUAV)
PIC unable to comply with separation provision instruction
NO SPI PIC (PUAV)
Collision avoidance alert (FSR-12)
CA ALERT (PUAV)
r=0
Other UAV alert e.g. GPWS (FSR-13)
OTHER ALERT (PUAV)
r=0
UAV cannot perform separation provision instruction e.g. performance limitation (FSR-14)
NO SPI PERF LIM (PUAV)
r=0
UAV system failure (SIR-09)
UAV SYS FAIL (PUAV)
r=0
UAV control station failure (SIR-09)
UAV CS FAIL (PUAV)
r=0
PIC incapacitated (SIR-10)
PIC INCAP (PUAV)
r=0

Figure 18 – HAZ001 Situation 2: UAV with PIC

F.1.3 HAZ001 – Inability to comply with separation provision instruction from ATC (Situation 3: Autonomous UAV)

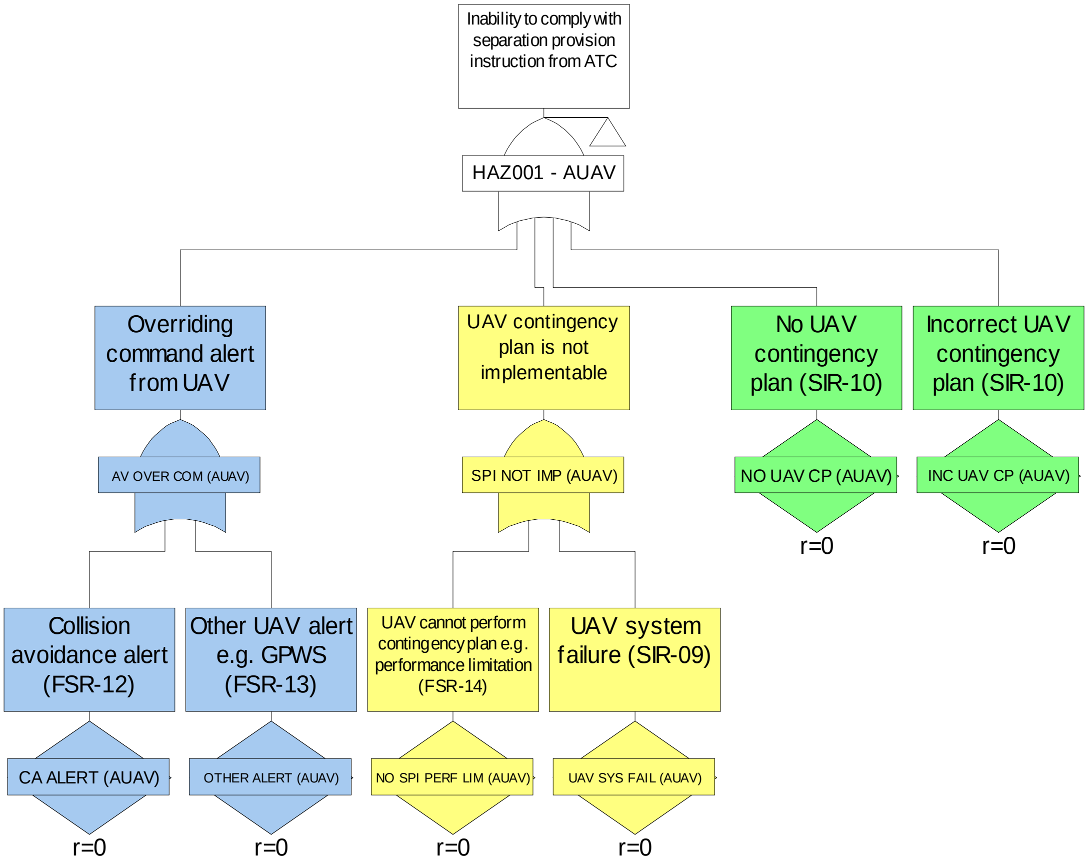

Inability to comply with separation provision instruction from ATC
HAZ001 - AUAV
Overriding command alert from UAV
UAV contingency plan is not implementable
No UAV contingency plan (SIR-10)
Incorrect UAV contingency plan (SIR-10)
AV OVER COM (AUAV)
SPI NOT IMP (AUAV)
NO UAV CP (AUAV)
INC UAV CP (AUAV)
r=0
r=0
Collision avoidance alert (FSR-12)
Other UAV alert e.g. GPWS (FSR-13)
UAV cannot perform contingency plan e.g. performance limitation (FSR-14)
UAV system failure (SIR-09)
CA ALERT (AUAV)
OTHER ALERT (AUAV)
NO SPI PERF LIM (AUAV)
UAV SYS FAIL (AUAV)
r=0
r=0
r=0
r=0

Figure 19 – HAZ001 Situation 3: Autonomous UAV

F.1.4 HAZ005 – Loss of separation provision from ATC (Situation 1: Manned Air Vehicle)

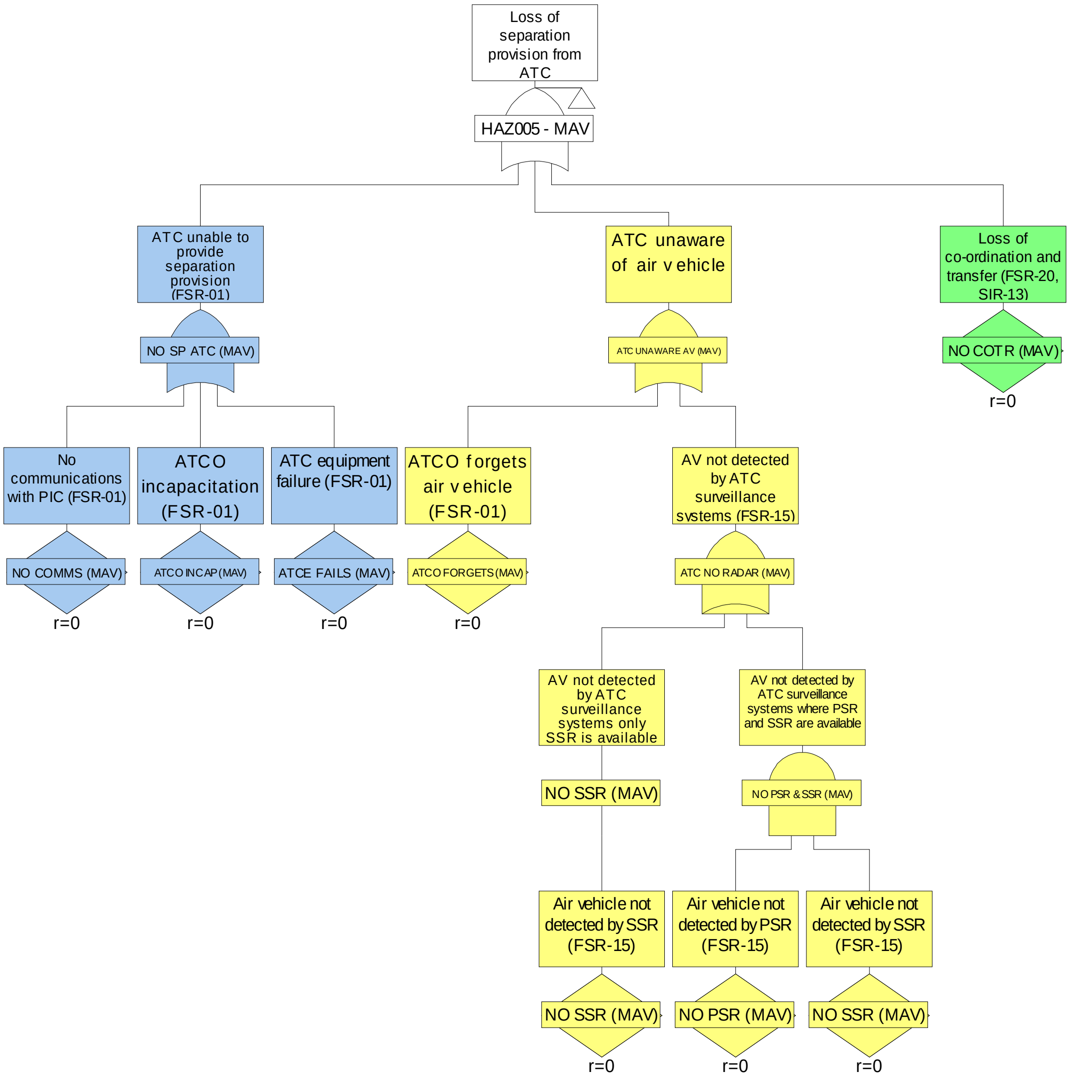

Loss of separation provision from ATC
HAZ005 - MAV
ATC unable to provide separation provision (FSR-01)
NO SP ATC (MAV)
ATC unaware of air vehicle
ATC UNAWARE AV (MAV)
Loss of co-ordination and transfer (FSR-20, SIR-13)
NO COTR (MAV)
r=0
No communications with PIC (FSR-01)
NO COMMS (MAV)
r=0
ATCO incapacitation (FSR-01)
ATCO INCAP (MAV)
r=0
ATC equipment failure (FSR-01)
ATCE FAILS (MAV)
r=0
ATCO forgets air vehicle (FSR-01)
ATCO FORGETS (MAV)
r=0
AV not detected by ATC surveillance systems (FSR-15)
ATC NO RADAR (MAV)
AV not detected by ATC surveillance systems only SSR is available
NO SSR (MAV)
AV not detected by ATC surveillance systems where PSR and SSR are available
NO PSR & SSR (MAV)
Air vehicle not detected by SSR (FSR-15)
NO SSR (MAV)
r=0
Air vehicle not detected by PSR (FSR-15)
NO PSR (MAV)
r=0
Air vehicle not detected by SSR (FSR-15)
NO SSR (MAV)
r=0

Figure 20 – HAZ005 Situation 1: Manned Air Vehicle

F.1.5 HAZ005 – Loss of separation provision from ATC (Situation 2: UAV with PIC)

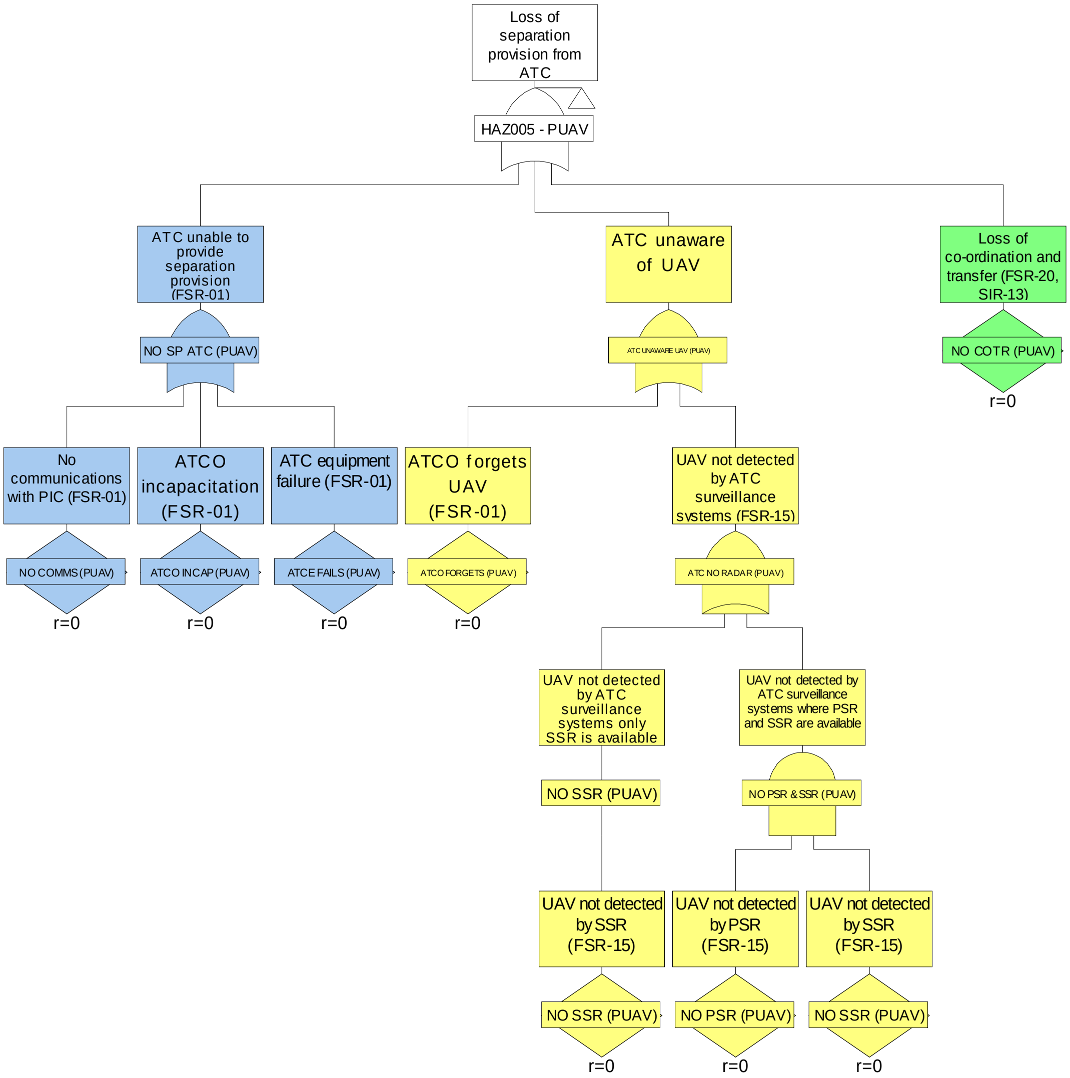

Loss of separation provision from ATC
HAZ005 - PUAV
ATC unable to provide separation provision (FSR-01)
NO SP ATC (PUAV)
ATC unaware of UAV
ATC UNAWARE UAV (PUAV)
Loss of co-ordination and transfer (FSR-20, SIR-13)
NO COTR (PUAV)
r=0
No communications with PIC (FSR-01)
ATCO incapacitation (FSR-01)
ATC equipment failure (FSR-01)
ATCO forgets UAV (FSR-01)
UAV not detected by ATC surveillance systems (FSR-15)
NO COMMS (PUAV)
ATCO INCAP (PUAV)
ATCE FAILS (PUAV)
ATCO FORGETS (PUAV)
ATC NO RADAR (PUAV)
r=0
r=0
r=0
r=0
UAV not detected by ATC surveillance systems only SSR is available
UAV not detected by ATC surveillance systems where PSR and SSR are available
NO SSR (PUAV)
NO PSR & SSR (PUAV)
UAV not detected by SSR (FSR-15)
UAV not detected by PSR (FSR-15)
UAV not detected by SSR (FSR-15)
NO SSR (PUAV)
NO PSR (PUAV)
NO SSR (PUAV)
r=0
r=0
r=0

Figure 21 – HAZ005 Situation 2: UAV with PIC

F.1.6 HAZ005 – Loss of separation provision from ATC (Situation 3: Autonomous UAV)

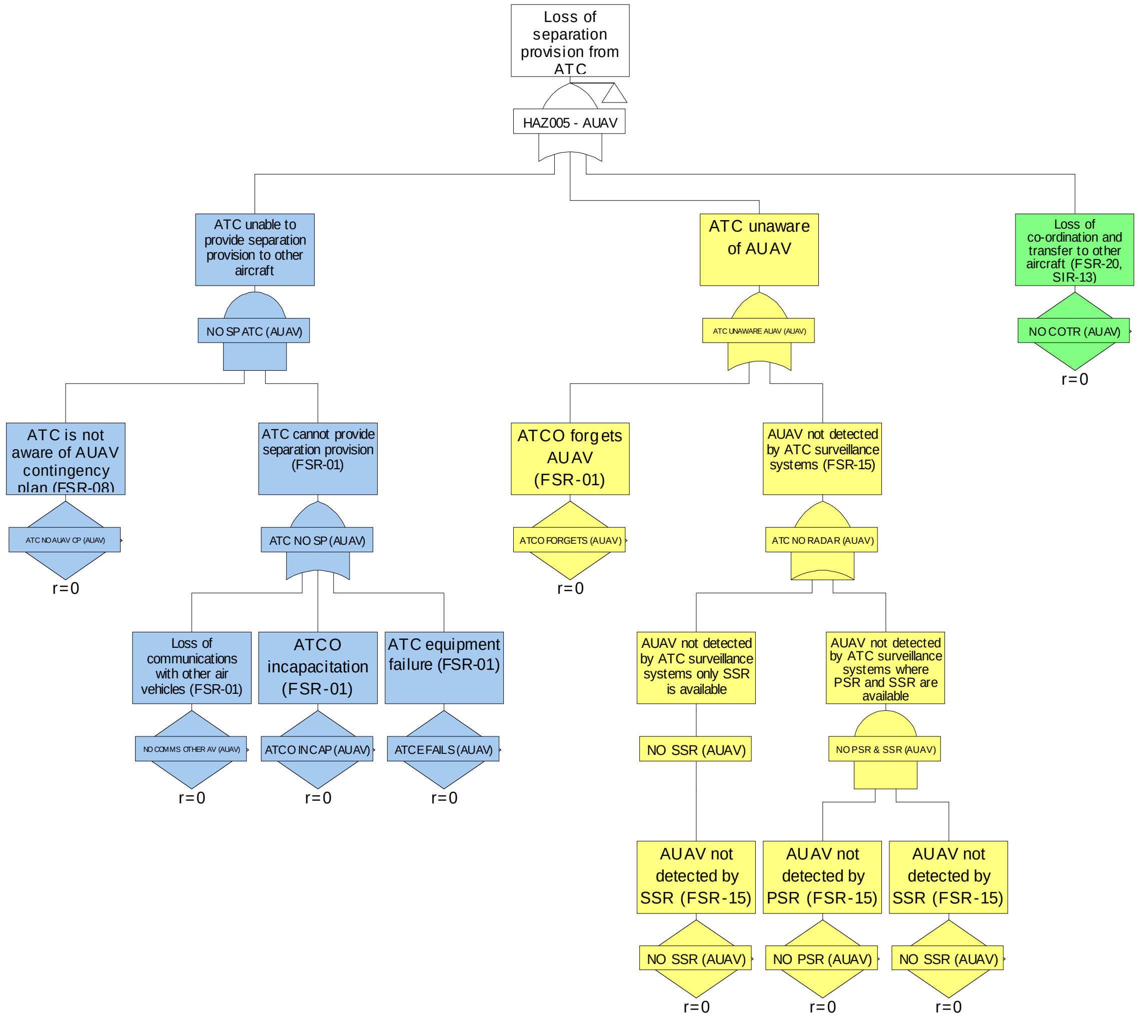

Loss of separation provision from ATC
HAZ005 - AUAV
ATC unable to provide separation provision to other aircraft
NO SP ATC (AUAV)
ATC unaware of AUAV
ATC UNAWARE AUAV (AUAV)
Loss of co-ordination and transfer to other aircraft (FSR-20, SIR-13)
NO COTR (AUAV)
r=0
ATC is not aware of AUAV contingency plan (FSR-08)
ATC NO AUAV CP (AUAV)
r=0
ATC cannot provide separation provision (FSR-01)
ATC NO SP (AUAV)
ATCO forgets AUAV (FSR-01)
ATCO FORGETS (AUAV)
r=0
AUAV not detected by ATC surveillance systems (FSR-15)
ATC NO RADAR (AUAV)
Loss of communications with other air vehicles (FSR-01)
NO COMMS OTHER AV (AUAV)
r=0
ATCO incapacitation (FSR-01)
ATCO INCAP (AUAV)
r=0
ATC equipment failure (FSR-01)
ATCE FAILS (AUAV)
r=0
AUAV not detected by ATC surveillance systems only SSR is available
NO SSR (AUAV)
AUAV not detected by ATC surveillance systems where PSR and SSR are available
NO PSR & SSR (AUAV)
AUAV not detected by SSR (FSR-15)
NO SSR (AUAV)
r=0
AUAV not detected by PSR (FSR-15)
NO PSR (AUAV)
r=0
AUAV not detected by SSR (FSR-15)
NO SSR (AUAV)
r=0

Figure 22 – HAZ005 Situation 3: Autonomous UAV

F.1.7 HAZ007 – Loss of separation provision from Pilot in Command when responsible for separation (Situation 1: Manned Air Vehicle)

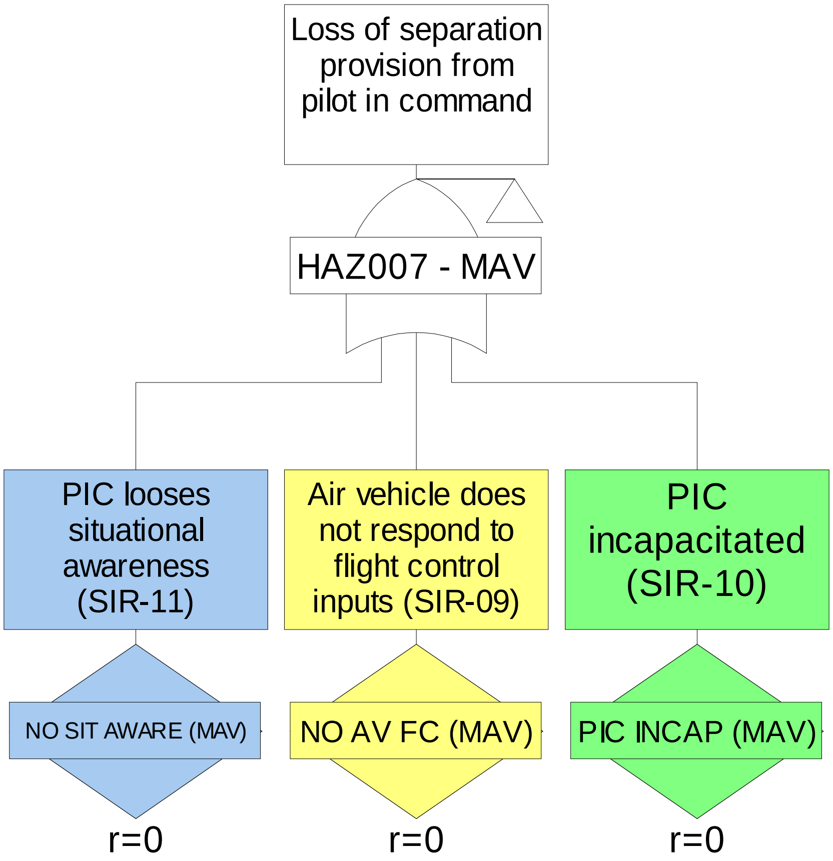

Loss of separation provision from pilot in command
HAZ007 - MAV
PIC looses situational awareness (SIR-11)
Air vehicle does not respond to flight control inputs (SIR-09)
PIC incapacitated (SIR-10)
NO SIT AWARE (MAV)
NO AV FC (MAV)
PIC INCAP (MAV)
r=0
r=0
r=0

Figure 23 – HAZ007 Situation 1: Manned Air Vehicle

F.1.8 HAZ007 – Loss of separation provision from Pilot in Command when responsible for separation (Situation 2: UAV with PIC)

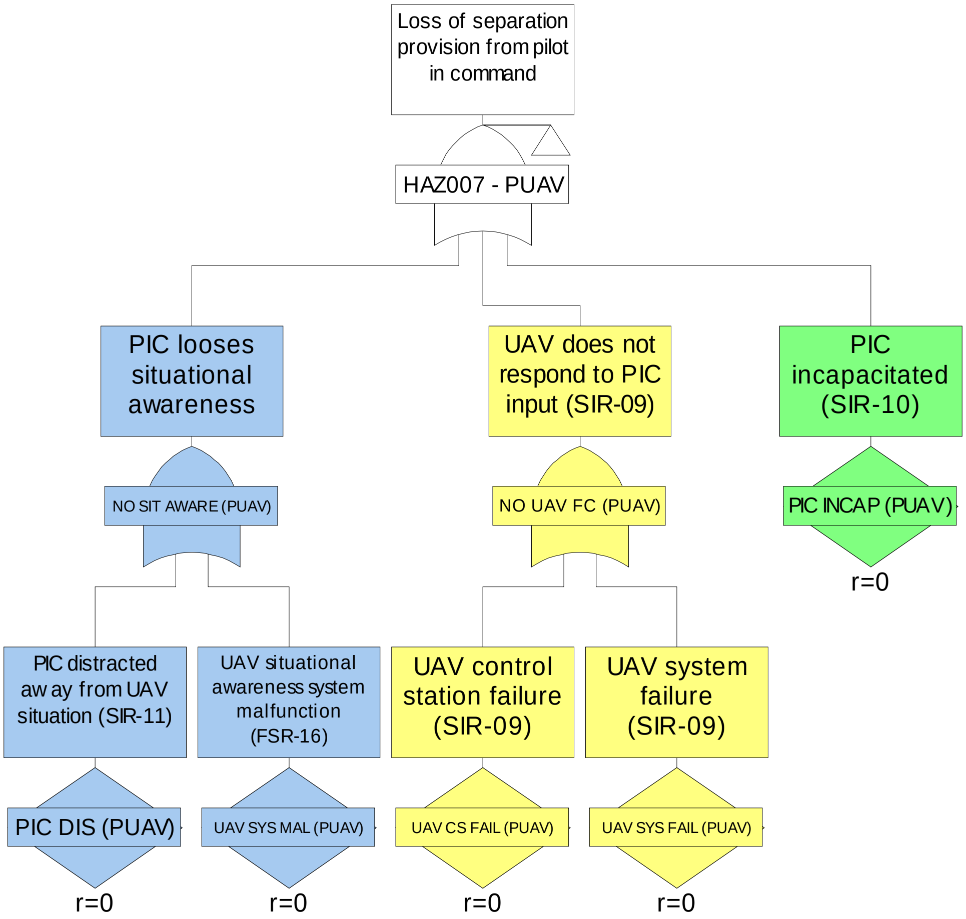

Loss of separation provision from pilot in command
HAZ007 - PUAV
PIC looses situational awareness
NO SIT AWARE (PUAV)
UAV does not respond to PIC input (SIR-09)
NO UAV FC (PUAV)
PIC incapacitated (SIR-10)
PIC INCAP (PUAV)
r=0
PIC distracted aw ay from UAV situation (SIR-11)
PIC DIS (PUAV)
r=0
UAV situational awareness system malfunction (FSR-16)
UAV SYS MAL (PUAV)
r=0
UAV control station failure (SIR-09)
UAV CS FAIL (PUAV)
r=0
UAV system failure (SIR-09)
UAV SYS FAIL (PUAV)
r=0

Figure 24 – HAZ007 Situation 2: UAV with PIC

F.1.9 HAZ007 – Loss of separation provision from Pilot in Command when responsible for separation (Situation 3: Autonomous UAV)

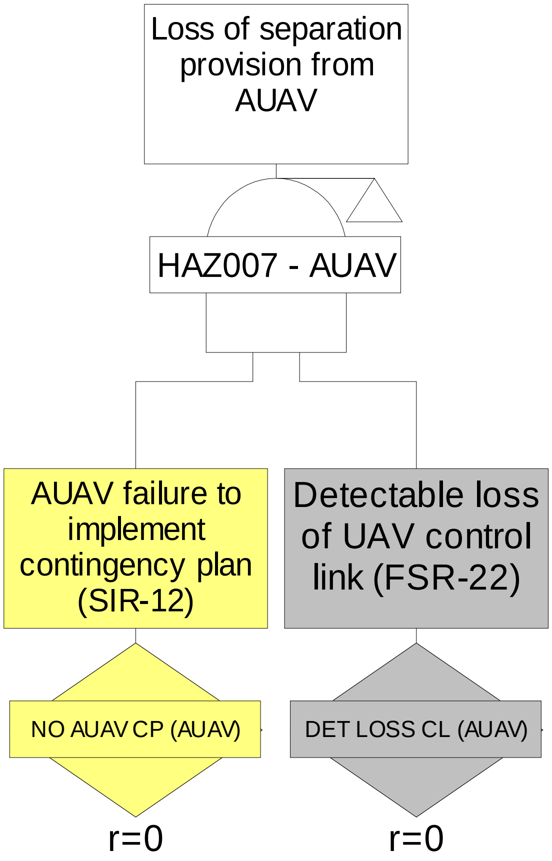

Loss of separation provision from AUAV
HAZ007 - AUAV
AUAV failure to implement contingency plan (SIR-12)
Detectable loss of UAV control link (FSR-22)
NO AUAV CP (AUAV)
DET LOSS CL (AUAV)
r=0
r=0

Figure 25 – HAZ007 Situation 3: Autonomous UAV

F.2 Separation Provision Error

F.2.1 HAZ002 – Incorrect Response to Separation Provision Instruction (Situation 1: Manned Aerial Vehicle)

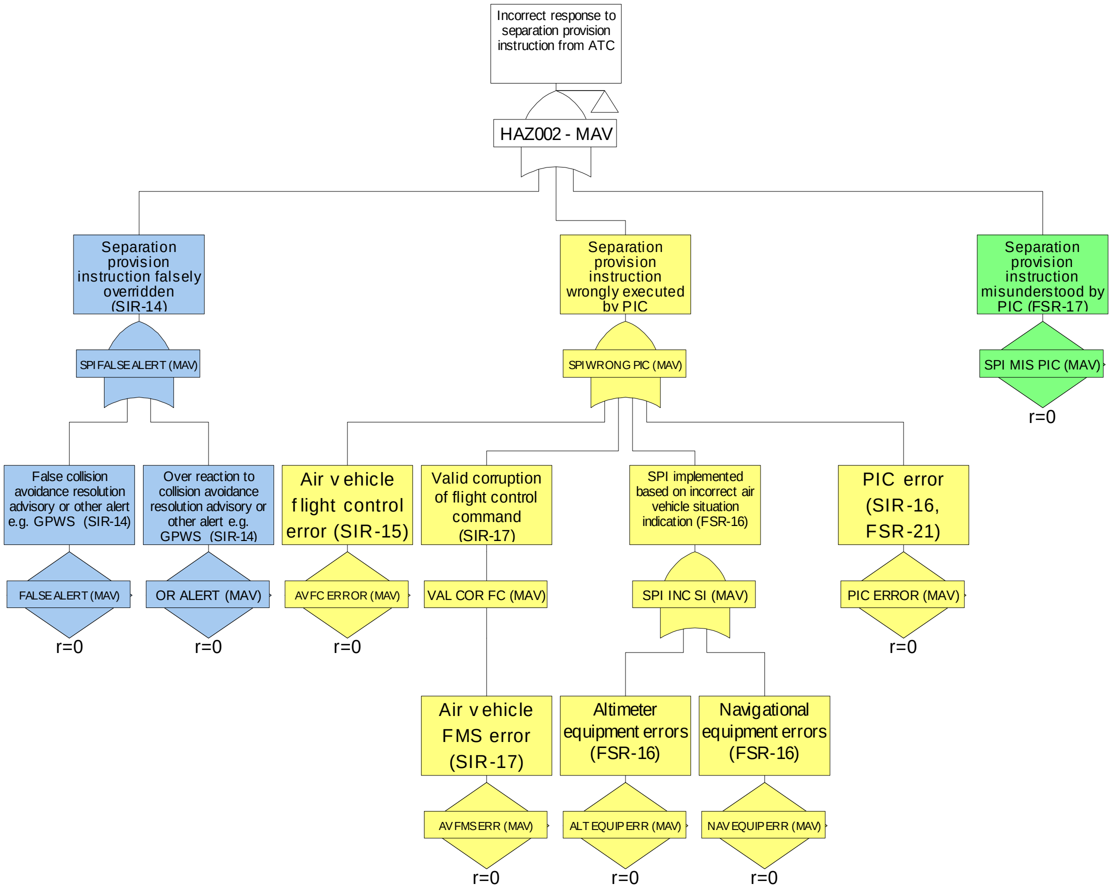

Incorrect response to separation provision instruction from ATC
HAZ002 - MAV
Separation provision instruction falsely overridden (SIR-14)
SPI FALSE ALERT (MAV)
Separation provision instruction wrongly executed by PIC
SPI WRONG PIC (MAV)
Separation provision instruction misunderstood by PIC (FSR-17)
SPI MIS PIC (MAV)
r=0
False collision avoidance resolution advisory or other alert e.g. GPWS (SIR-14)
FALSE ALERT (MAV)
r=0
Over reaction to collision avoidance resolution advisory or other alert e.g. GPWS (SIR-14)
OR ALERT (MAV)
r=0
Air vehicle flight control error (SIR-15)
AV FC ERROR (MAV)
r=0
Valid corruption of flight control command (SIR-17)
VAL COR FC (MAV)
SPI implemented based on incorrect air vehicle situation indication (FSR-16)
SPI INC SI (MAV)
PIC error (SIR-16, FSR-21)
PIC ERROR (MAV)
r=0
Air vehicle FMS error (SIR-17)
AV FMS ERR (MAV)
r=0
Altimeter equipment errors (FSR-16)
ALT EQUIP ERR (MAV)
r=0
Navigational equipment errors (FSR-16)
NAV EQUIP ERR (MAV)
r=0

Figure 26 – HAZ002 Situation 1: Manned Aerial Vehicle

F.2.2 HAZ002 – Incorrect Response to Separation Provision Instruction (Situation 2: UAV with PIC)

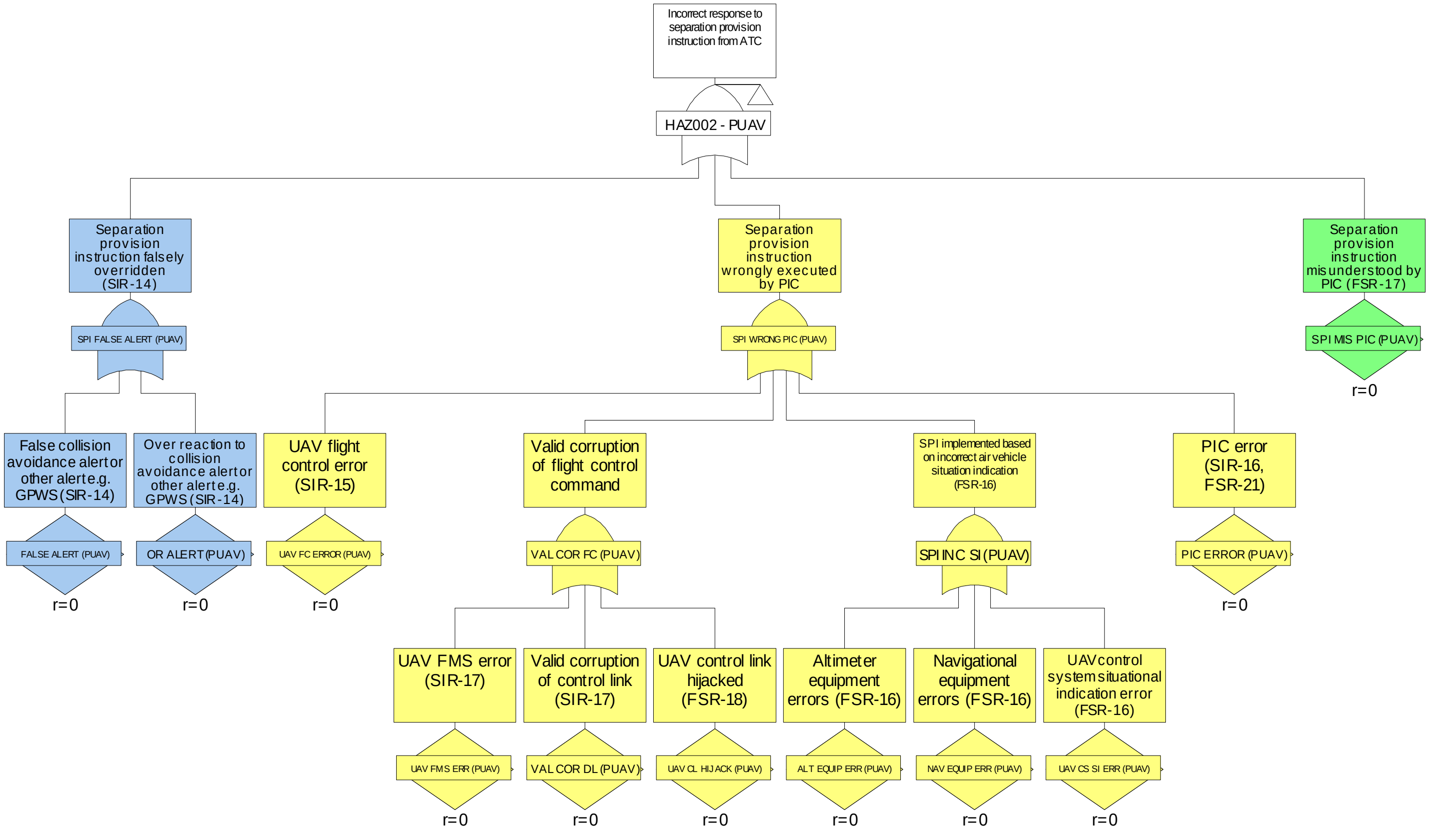

Incorrect response to separation provision instruction from ATC
HAZ002 - PUAV
Separation provision instruction falsely overridden (SIR-14)
SPI FALSE ALERT (PUAV)
Separation provision instruction wrongly executed by PIC
SPI WRONG PIC (PUAV)
Separation provision instruction misunderstood by PIC (FSR-17)
SPI MIS PIC (PUAV)
r=0
False collision avoidance alert or other alert e.g. GPWS (SIR-14)
FALSE ALERT (PUAV)
r=0
Over reaction to collision avoidance alert or other alert e.g. GPWS (SIR-14)
OR ALERT (PUAV)
r=0
UAV flight control error (SIR-15)
UAV FC ERROR (PUAV)
r=0
Valid corruption of flight control command
VAL COR FC (PUAV)
SPI implemented based on incorrect air vehicle situation indication (FSR-16)
SPI INC SI (PUAV)
PIC error (SIR-16, FSR-21)
PIC ERROR (PUAV)
r=0
UAV FMS error (SIR-17)
UAV FMS ERR (PUAV)
r=0
Valid corruption of control link (SIR-17)
VAL COR DL (PUAV)
r=0
UAV control link hijacked (FSR-18)
UAV CL HIJACK (PUAV)
r=0
Altimeter equipment errors (FSR-16)
ALT EQUIP ERR (PUAV)
r=0
Navigational equipment errors (FSR-16)
NAV EQUIP ERR (PUAV)
r=0
UAV control system situational indication error (FSR-16)
UAV CS SI ERR (PUAV)
r=0

Figure 27 – HAZ002 Situation 2: UAV with PIC

F.2.3 HAZ002 – Incorrect Response to Separation Provision Instruction (Situation 3: Autonomous UAV)

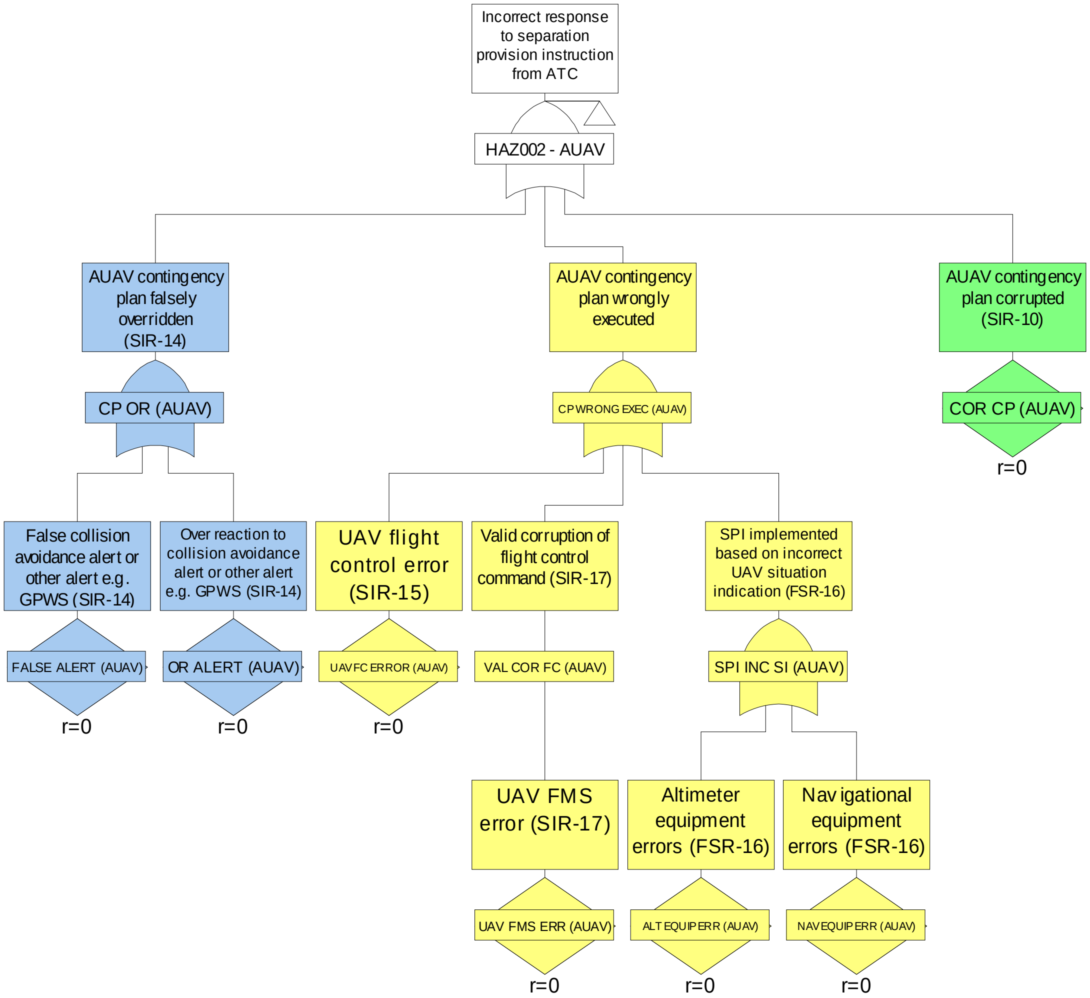

Incorrect response to separation provision instruction from ATC
HAZ002 - AUAV
AUAV contingency plan falsely overridden (SIR-14)
CP OR (AUAV)
AUAV contingency plan wrongly executed
CP WRONG EXEC (AUAV)
AUAV contingency plan corrupted (SIR-10)
COR CP (AUAV)
r=0
False collision avoidance alert or other alert e.g. GPWS (SIR-14)
FALSE ALERT (AUAV)
r=0
Over reaction to collision avoidance alert or other alert e.g. GPWS (SIR-14)
OR ALERT (AUAV)
r=0
UAV flight control error (SIR-15)
UAV FC ERROR (AUAV)
r=0
Valid corruption of flight control command (SIR-17)
VAL COR FC (AUAV)
SPI implemented based on incorrect UAV situation indication (FSR-16)
SPI INC SI (AUAV)
UAV FMS error (SIR-17)
UAV FMS ERR (AUAV)
r=0
Altimeter equipment errors (FSR-16)
ALT EQUIP ERR (AUAV)
r=0
Navigational equipment errors (FSR-16)
NAV EQUIP ERR (AUAV)
r=0

Figure 28 – HAZ002 Situation 3: Autonomous UAV

F.2.4 HAZ006 – ATC Separation Provision Error (Situation 1: Manned Aerial Vehicle)

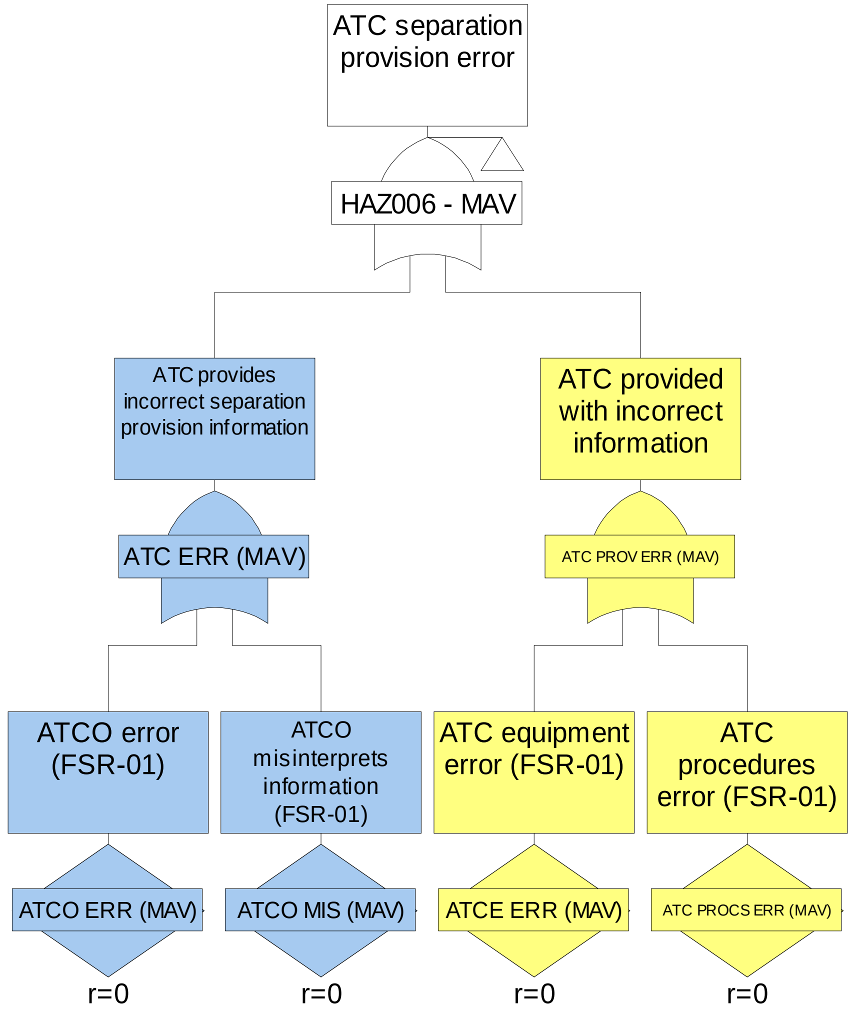

ATC separation provision error
HAZ006 - MAV
ATC provides incorrect separation provision information
ATC provided with incorrect information
ATC ERR (MAV)
ATC PROV ERR (MAV)
ATCO error (FSR-01)
ATCO misinterprets information (FSR-01)
ATC equipment error (FSR-01)
ATC procedures error (FSR-01)
ATCO ERR (MAV)
ATCO MIS (MAV)
ATCE ERR (MAV)
ATC PROCS ERR (MAV)
r=0
r=0
r=0
r=0

Figure 29 – HAZ006 Situation 1: Manned Aerial Vehicle

F.2.5 HAZ006 – ATC Separation Provision Error (Situation 2: UAV with PIC)

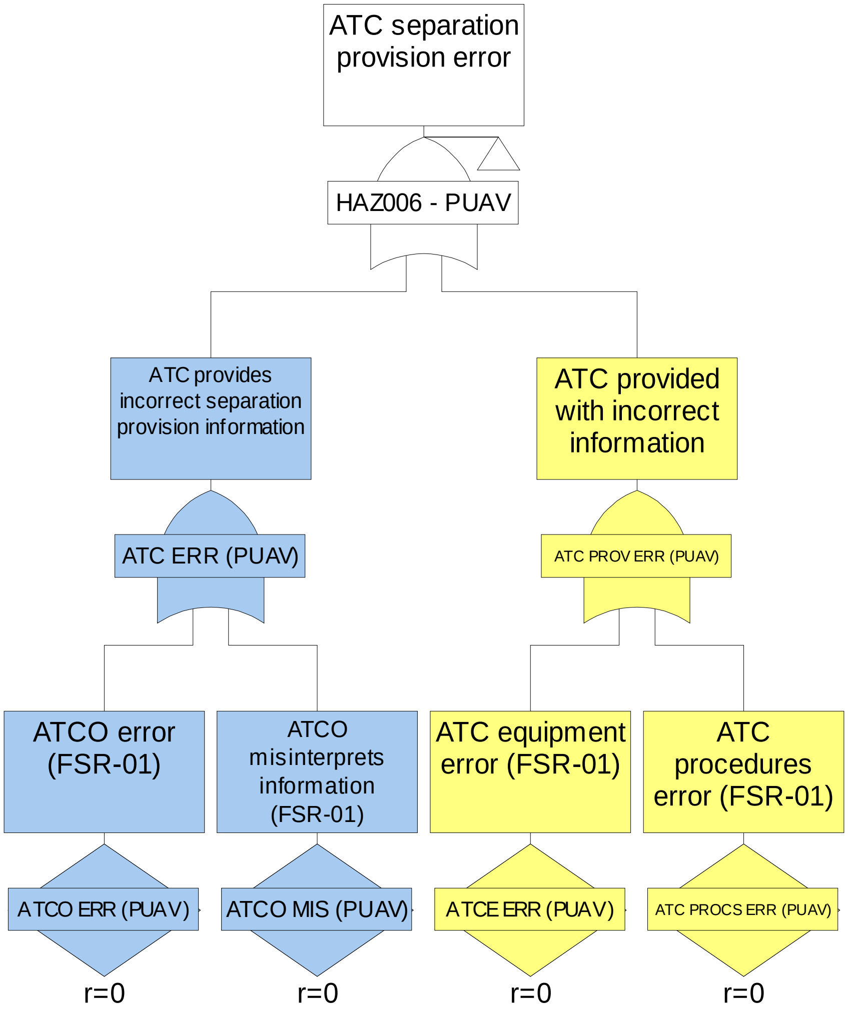

ATC separation provision error
HAZ006 - PUAV
ATC provides incorrect separation provision information
ATC provided with incorrect information
ATC ERR (PUAV)
ATC PROV ERR (PUAV)
ATCO error (FSR-01)
ATCO misinterprets information (FSR-01)
ATC equipment error (FSR-01)
ATC procedures error (FSR-01)
ATCO ERR (PUAV)
ATCO MIS (PUAV)
ATCE ERR (PUAV)
ATC PROCS ERR (PUAV)
r=0
r=0
r=0
r=0

Figure 30 – HAZ006 Situation 2: UAV with PIC

F.2.6 HAZ006 – ATC Separation Provision Error (Situation 3: Autonomous UAV)

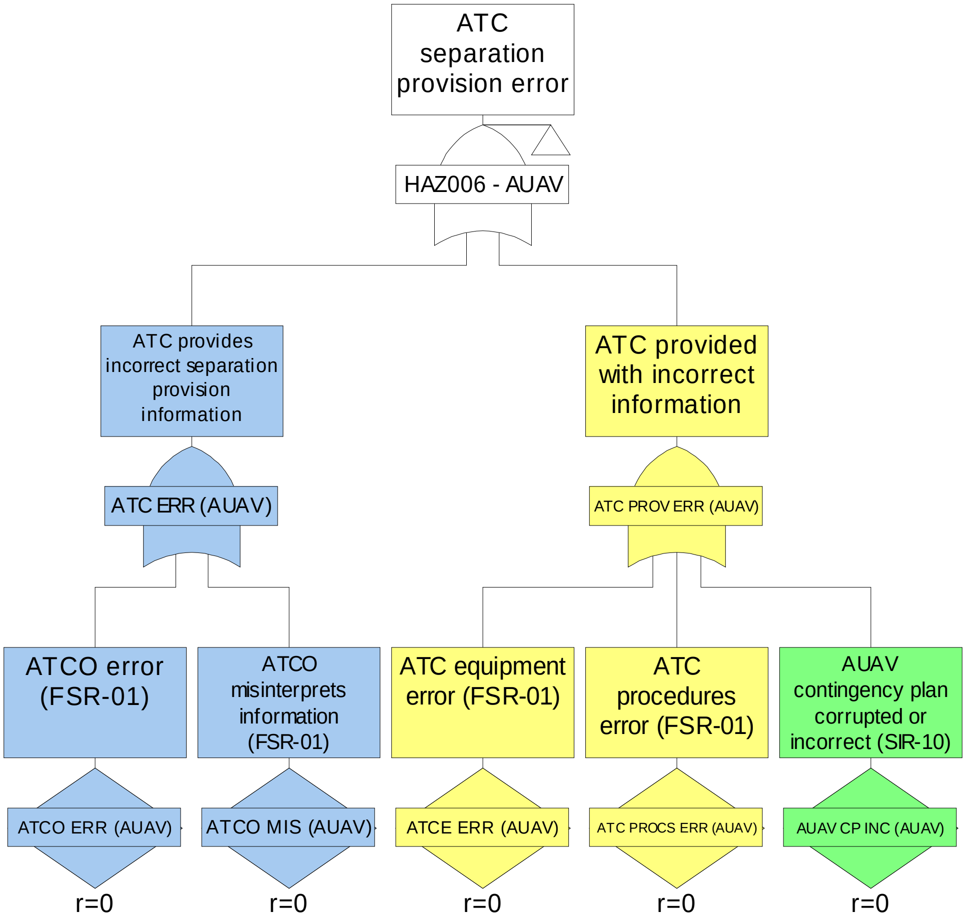

ATC separation provision error
HAZ006 - AUAV
ATC provides incorrect separation provision information
ATC provided with incorrect information
ATC ERR (AUAV)
ATC PROV ERR (AUAV)
ATCO error (FSR-01)
ATCO misinterprets information (FSR-01)
ATC equipment error (FSR-01)
ATC procedures error (FSR-01)
AUAV contingency plan corrupted or incorrect (SIR-10)
ATCO ERR (AUAV)
ATCO MIS (AUAV)
ATCE ERR (AUAV)
ATC PROCS ERR (AUAV)
AUAV CP INC (AUAV)
r=0
r=0
r=0
r=0
r=0

Figure 31 – HAZ006 Situation 3: Autonomous UAV

F.2.7 HAZ008 – Pilot in Command Separation Provision Error (Situation 1: Manned Aerial Vehicle)

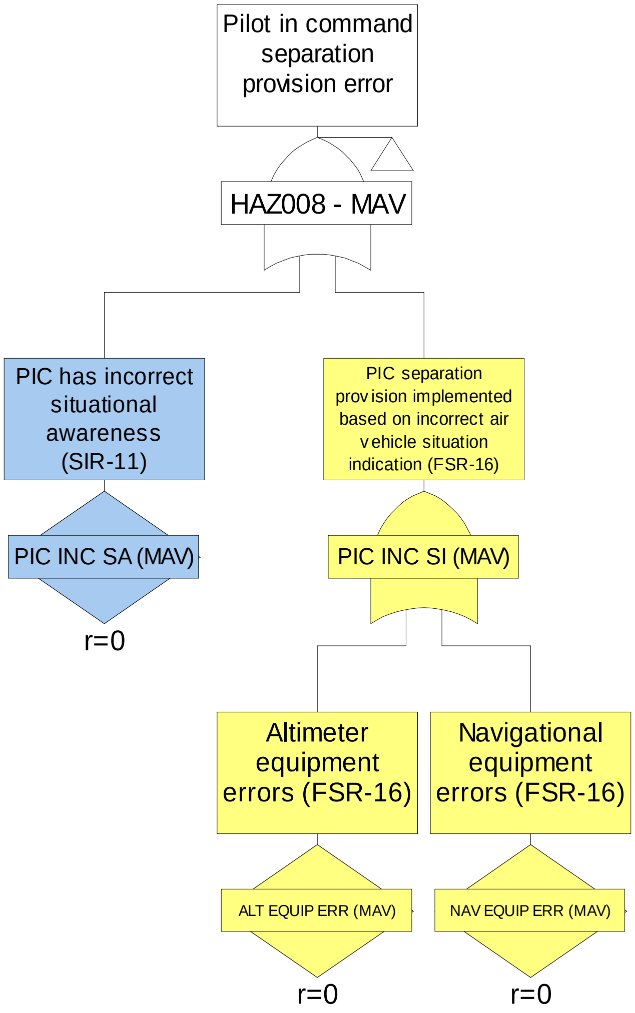

Pilot in command separation provision error
HAZ008 - MAV
PIC has incorrect situational awareness (SIR-11)
PIC separation provision implemented based on incorrect air vehicle situation indication (FSR-16)
PIC INC SA (MAV)
r=0
PIC INC SI (MAV)
Altimeter equipment errors (FSR-16)
Navigational equipment errors (FSR-16)
ALT EQUIP ERR (MAV)
NAV EQUIP ERR (MAV)
r=0
r=0

Figure 32 – HAZ008 Situation 1: Manned Aerial Vehicle

F.2.8 HAZ008 – Pilot in Command Separation Provision Error (Situation 2: UAV with PIC)

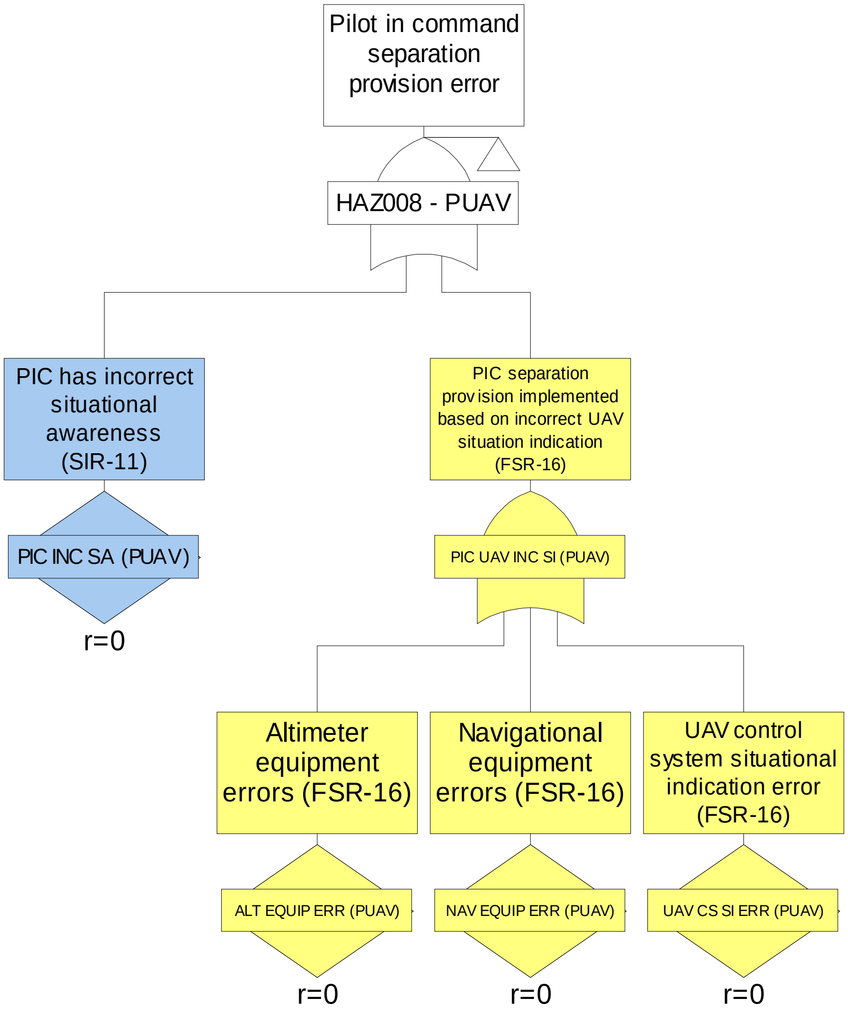

Pilot in command separation provision error
HAZ008 - PUAV
PIC has incorrect situational awareness (SIR-11)
PIC INC SA (PUAV)
r=0
PIC separation provision implemented based on incorrect UAV situation indication (FSR-16)
PIC UAV INC SI (PUAV)
Altimeter equipment errors (FSR-16)
ALT EQUIP ERR (PUAV)
r=0
Navigational equipment errors (FSR-16)
NAV EQUIP ERR (PUAV)
r=0
UAV control system situational indication error (FSR-16)
UAV CS SI ERR (PUAV)
r=0

Figure 33 – HAZ008 Situation 2: UAV with PIC

F.2.9 HAZ008 – Pilot in Command Separation Provision Error (Situation 3: Autonomous UAV)

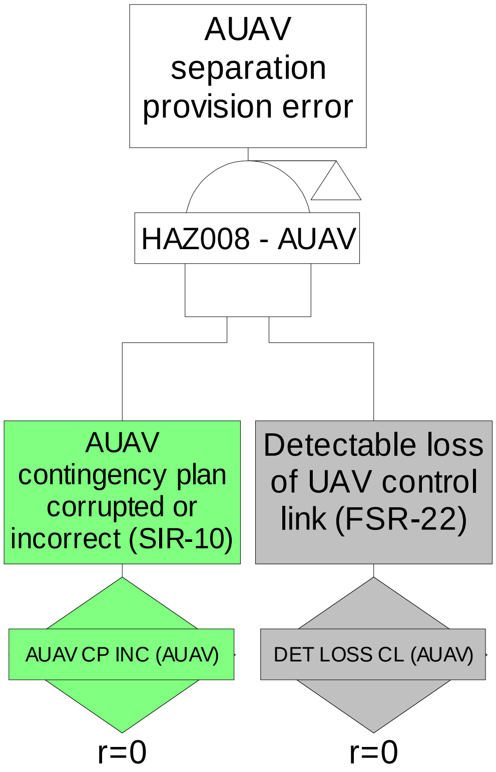

AUAV separation provision error
HAZ008 - AUAV
AUAV contingency plan corrupted or incorrect (SIR-10)
Detectable loss of UAV control link (FSR-22)
AUAV CP INC (AUAV)
DET LOSS CL (AUAV)
r=0
r=0

Figure 34 – HAZ008 Situation 3: Autonomous UAV

F.3 Delayed Separation Provision

F.3.1 HAZ004 – Delayed Response to Separation Provision Instruction from ATC (Situation 1: Manned Aerial Vehicle)

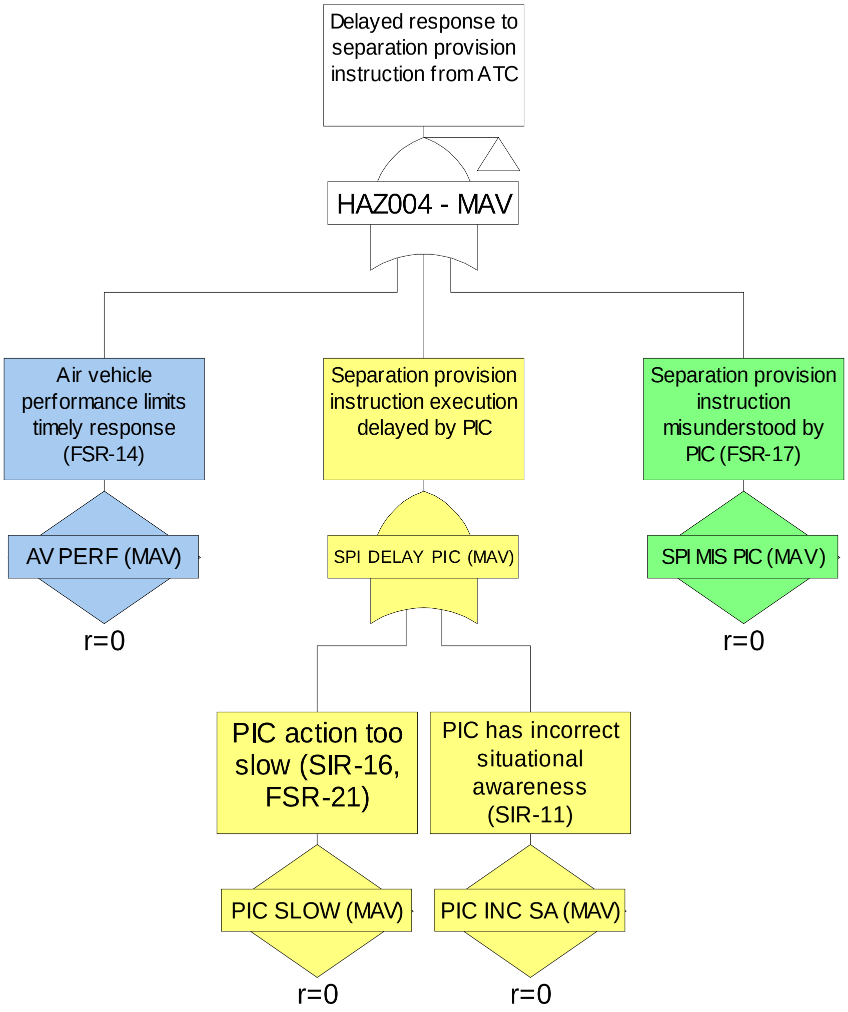

Delayed response to separation provision instruction from ATC
HAZ004 - MAV
Air vehicle performance limits timely response (FSR-14)
AV PERF (MAV)
r=0
Separation provision instruction execution delayed by PIC
SPI DELAY PIC (MAV)
Separation provision instruction misunderstood by PIC (FSR-17)
SPI MIS PIC (MAV)
r=0
PIC action too slow (SIR-16, FSR-21)
PIC SLOW (MAV)
r=0
PIC has incorrect situational awareness (SIR-11)
PIC INC SA (MAV)
r=0

Figure 35 – HAZ004 Situation 1: Manned Aerial Vehicle

F.3.2 HAZ004 – Delayed Response to Separation Provision Instruction from ATC (Situation 2: UAV with PIC)

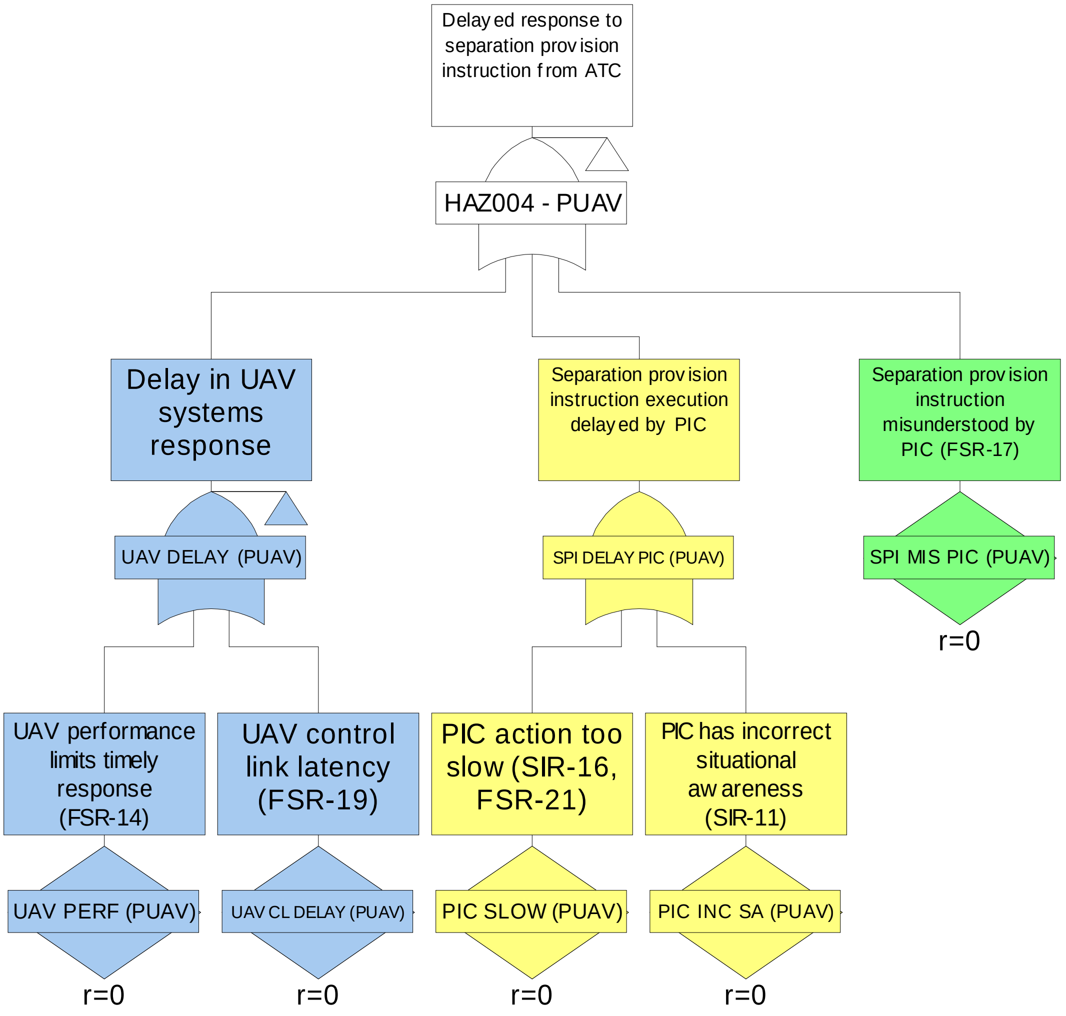

Delayed response to separation provision instruction from ATC
HAZ004 - PUAV
Delay in UAV systems response
Separation provision instruction execution delayed by PIC
Separation provision instruction misunderstood by PIC (FSR-17)
UAV DELAY (PUAV)
SPI DELAY PIC (PUAV)
SPI MIS PIC (PUAV)
r=0
UAV performance limits timely response (FSR-14)
UAV control link latency (FSR-19)
PIC action too slow (SIR-16, FSR-21)
PIC has incorrect situational awareness (SIR-11)
UAV PERF (PUAV)
UAV CL DELAY (PUAV)
PIC SLOW (PUAV)
PIC INC SA (PUAV)
r=0
r=0
r=0
r=0

Figure 36 – HAZ004 Situation 2: UAV with PIC

F.3.3 HAZ004 – Delayed Response to Separation Provision Instruction from ATC (Situation 3: Autonomous UAV)

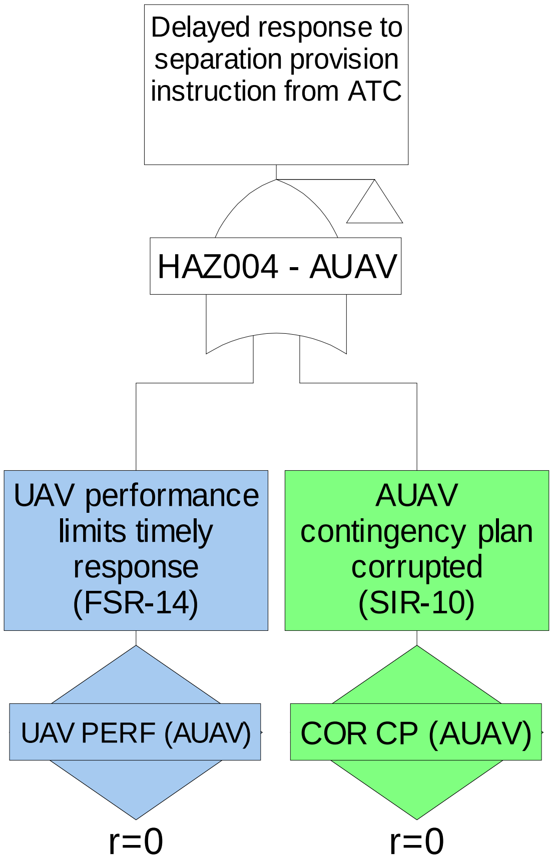

Delayed response to separation provision instruction from ATC
HAZ004 - AUAV
UAV performance limits timely response (FSR-14)
AUAV contingency plan corrupted (SIR-10)
UAV PERF (AUAV)
COR CP (AUAV)
r=0
r=0

Figure 37 – HAZ004 Situation 3: Autonomous UAV

F.3.4 HAZ009 – Pilot in Command Separation Provision Instruction too late (Situation 1: Manned Aerial Vehicle)

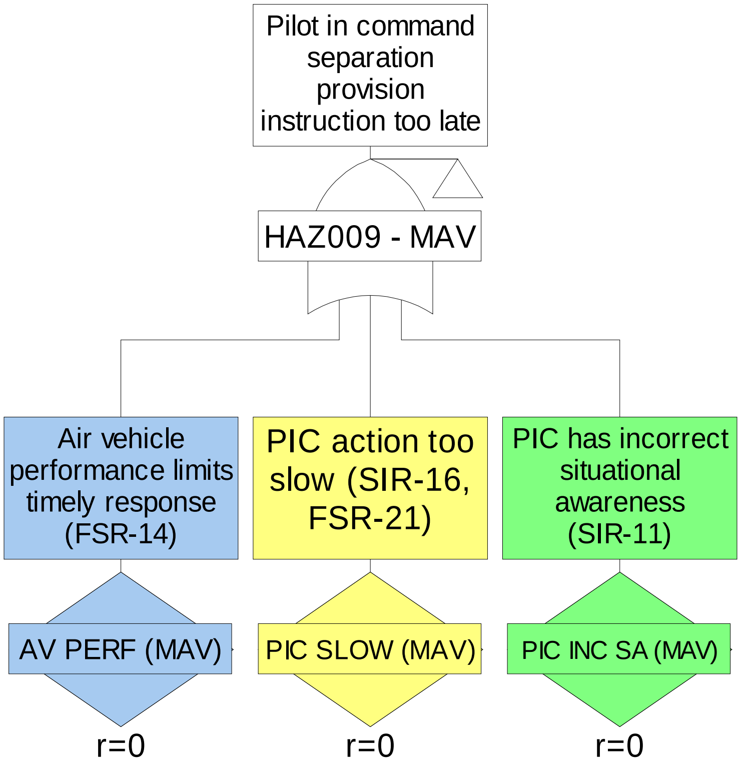

Pilot in command separation provision instruction too late
HAZ009 - MAV
Air vehicle performance limits timely response (FSR-14)
PIC action too slow (SIR-16, FSR-21)
PIC has incorrect situational awareness (SIR-11)
AV PERF (MAV)
PIC SLOW (MAV)
PIC INC SA (MAV)
r=0
r=0
r=0

Figure 38 – HAZ009 Situation 1: Manned Aerial Vehicle

F.3.5 HAZ009 – Pilot in Command Separation Provision Instruction too late (Situation 2: UAV with PIC)

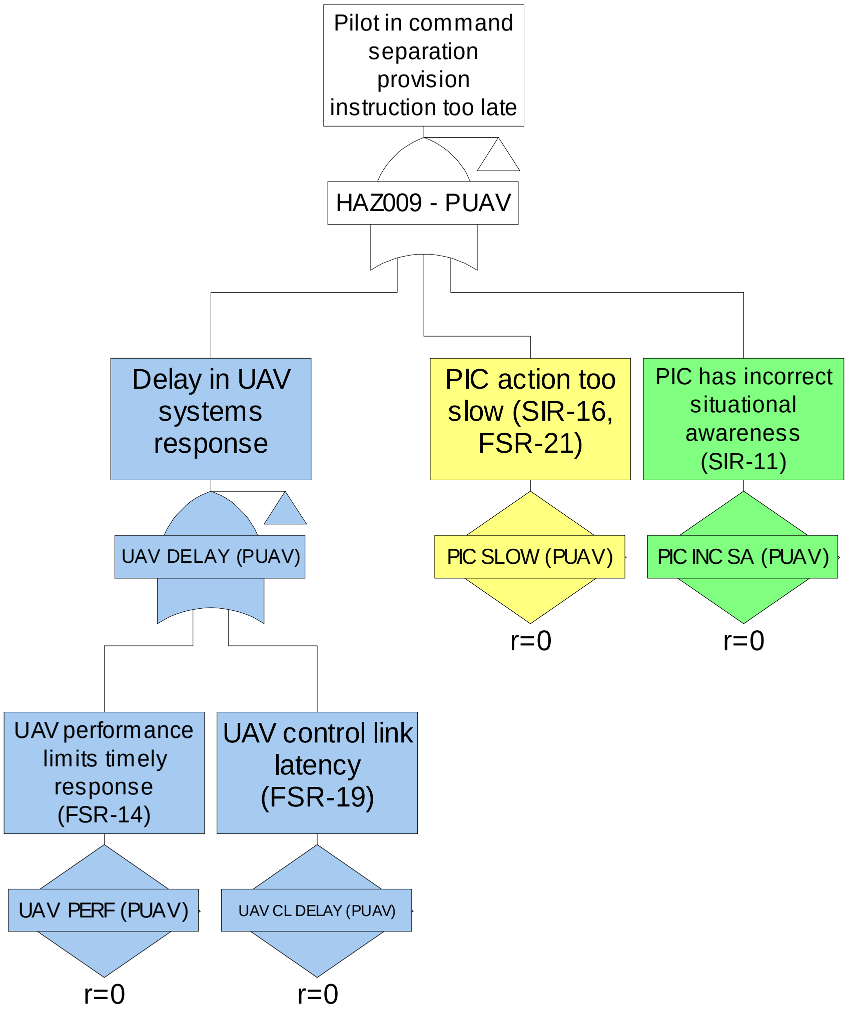

Pilot in command separation provision instruction too late
HAZ009 - PUAV
Delay in UAV systems response
PIC action too slow (SIR-16, FSR-21)
PIC has incorrect situational awareness (SIR-11)
UAV DELAY (PUAV)
PIC SLOW (PUAV)
PIC INC SA (PUAV)
r=0
r=0
UAV performance limits timely response (FSR-14)
UAV control link latency (FSR-19)
UAV PERF (PUAV)
UAV CL DELAY (PUAV)
r=0
r=0

Figure 39 – HAZ009 Situation 2: UAV with PIC

F.3.6 HAZ009 – Pilot in Command Separation Provision Instruction too late (Situation 3: Autonomous UAV)

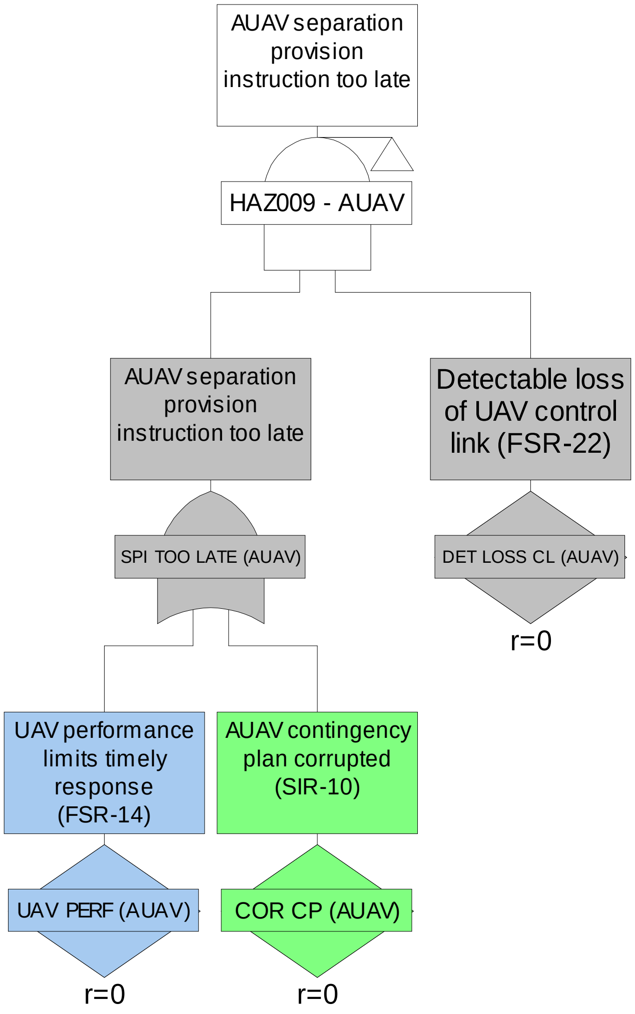

AUAV separation provision instruction too late
HAZ009 - AUAV
AUAV separation provision instruction too late
SPI TOO LATE (AUAV)
Detectable loss of UAV control link (FSR-22)
DET LOSS CL (AUAV)
r=0
UAV performance limits timely response (FSR-14)
UAV PERF (AUAV)
r=0
AUAV contingency plan corrupted (SIR-10)
COR CP (AUAV)
r=0

Figure 40 – HAZ009 Situation 3: Autonomous UAV

F.4 Intentional Deviation from Separation Provision Instruction

F.4.1 HAZ003 – Intentional Deviation from Separation Provision Instruction (Situation 1: Manned Aerial Vehicle)

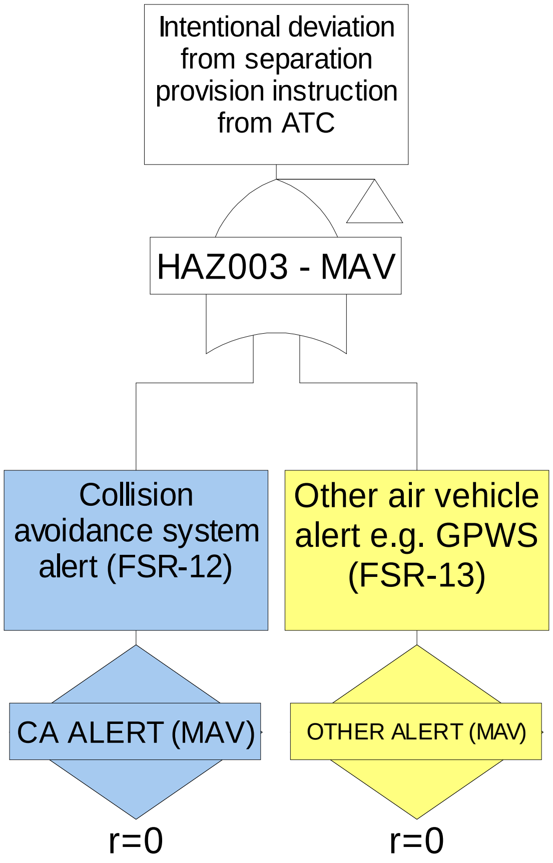

Intentional deviation from separation provision instruction from ATC
HAZ003 - MAV
Collision avoidance system alert (FSR-12)
Other air vehicle alert e.g. GPWS (FSR-13)
CA ALERT (MAV)
OTHER ALERT (MAV)
r=0
r=0

Figure 41 – HAZ003 Situation 1: Manned Aerial Vehicle

F.4.2 HAZ003 – Intentional Deviation from Separation Provision Instruction (Situation 2: UAV with PIC)

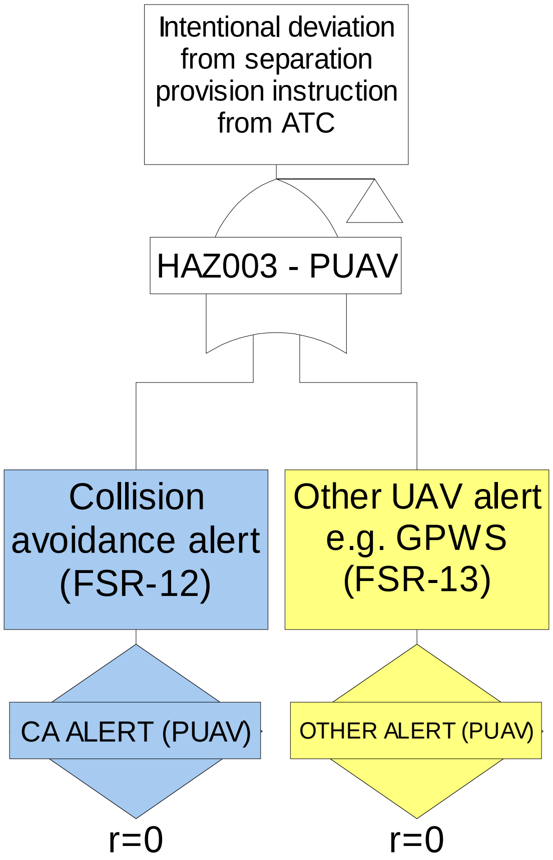

Intentional deviation from separation provision instruction from ATC
HAZ003 - PUAV
Collision avoidance alert (FSR-12)
Other UAV alert e.g. GPWS (FSR-13)
CA ALERT (PUAV)
OTHER ALERT (PUAV)
r=0
r=0

Figure 42 – HAZ003 Situation 2: UAV with PIC

F.4.3 HAZ003 – Intentional Deviation from Separation Provision Instruction (Situation 3: Autonomous UAV)

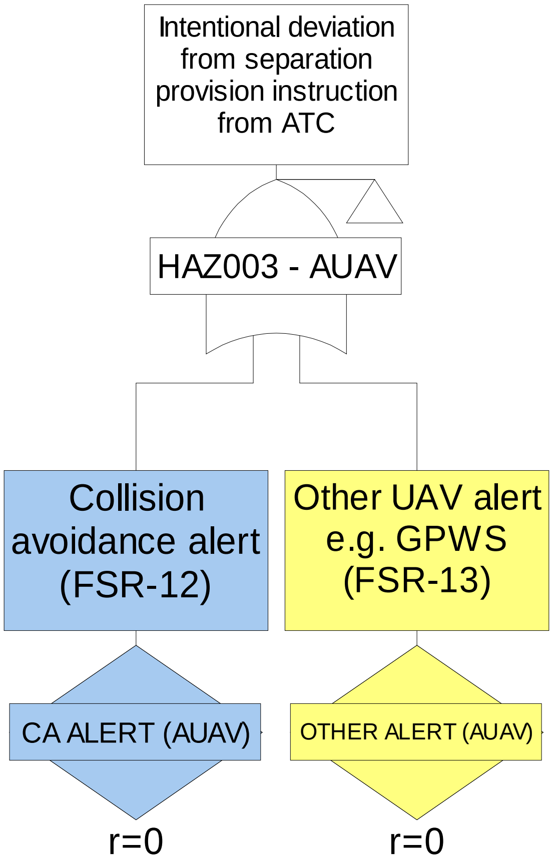

Intentional deviation from separation provision instruction from ATC
HAZ003 - AUAV
Collision avoidance alert (FSR-12)
Other UAV alert e.g. GPWS (FSR-13)
CA ALERT (AUAV)
OTHER ALERT (AUAV)
r=0
r=0

Figure 43 – HAZ003 Situation 3: Autonomous UAV

Appendix G Abbreviations and Acronyms

Acronym/ Abbreviation	Definition
ACAS	Airborne Collision Avoidance System
ACM	Airspace Control Means
AFARP	As Far As Reasonably Practicable
ATC	Air Traffic Control
ATM	Air Traffic Management
AUAV	Autonomous Unmanned Aerial Vehicle
CA	Collision Avoidance
EATMP	European Air Traffic Management Programme
ESARR	Eurocontrol Safety Regulatory Requirements
FHA	Functional Hazard Assessment
FIR	Flight Information Region
FSR	Functional Safety Requirements
GAT	General Air Traffic
GSN	Goal Structured Notation
HORGI	Harmonisation of OAT Rules and their GAT Interface
ICAO	International Convention
IFR	Instrument Flight Rules
MAV	Manned Aerial Vehicle
MILT	Military Team
MSF	Mitigating Safety Functions
OAT	Operational Air Traffic
PIC	Pilot In Command
PSSA	Preliminary System Safety Assessment
PUAV	Piloted Unmanned Aerial Vehicle
SIR	Safety Integrity Requirements
SP	Separation Provision
SRC	Safety Regulatory Commission
TCAS	Traffic Collision Avoidance System
TF	Task Force
UAV	Unmanned Aerial Vehicle

Acronym/ Abbreviation	Definition
UCL	UAV Control Link
UCS	UAV Control System
UIR	Upper Flight Information Region
VFR	Visual Flight Rules

Table 15 – Table of Abbreviations and Acronyms

Appendix H UAVs Safety Requirements and Traceability

Ref	Safety Requirement	Traceability to Annex E of the Draft Specifications
Functional Safety Requirements		
FSR-01	*The air traffic service provided to UAVs should accord with that provided to manned aircraft*	Paras 9.1, 11.1 and 12.2
FSR-02	The separation minima between UAVs and other traffic should be the same as for manned aircraft flying OAT in the same class of airspace	Paras 7.2 and 8.1
FSR-03	The Pilot in Command is responsible for ensuring that the UAV trajectory is compliant with any ATC clearance	Para 6.1
FSR-04	*While in receipt of an air traffic service, UAVs should be monitored continuously by the UAV Pilot in Command for adherence to the approved flight plan*	Paras 3.1 and 12.4
FSR-05	*The weather minima for UAV flight should be determined by the equipment and capabilities of each UAV System*	Para 13.1
FSR-06	UAVs shall be pre-programmed with appropriate contingency plan in the event that the Pilot in Command is no longer in control of the UAV	**Not covered within the Draft Specification [1]**
FSR-07	Following the above event in controlled airspace, UAVs should continue flight autonomously and in accordance with the pre-programmed contingency plan	Para 3.1
FSR-08	UAVs flying in controlled airspace shall notify ATC of contingency plans for emergency AUAV operations prior to operations	Para 12.3
FSR-09	*Where a UAV Pilot in Command has primary responsibility for separation provision, he should maintain a minimum distance of 500ft between his UAV and other airspace users, regardless of how the conflicting traffic was detected and irrespective of whether or not he was prompted by a collision avoidance system*	Para 8.2

Ref	Safety Requirement	Traceability to Annex E of the Draft Specifications
FSR-10	UAV collision avoidance systems should enable a UAV Pilot in Command to perform collision avoidance functions as least as well as, and preferably better, than a pilot in a manned aircraft	Paras 6.1, 6.2, 7.1, 9.2, 9.3 and 9.4
FSR-11	Autonomous UAV collision avoidance systems should have equivalent efficacy to a pilot performing threat detection and collision avoidance actions	Para 8.3
FSR-12	UAVs equipment carriage shall render it compatible with other mandated collision avoidance systems fitted to other aircraft	Para 8.3
FSR-13	UAVs should have limited alerting systems equivalent to those on a manned aircraft, to minimise the potential alerts that can disrupt separation provision	**Not covered within the Draft Specification [1]**
FSR-14	Pilots in Command of UAVs and ATC shall be familiar with individual UAV performance characteristics	**Not covered within the Draft Specification [1]**
FSR-15	*UAVs should carry similar equipment for flight, navigation and communication as required for manned aircraft, as mandated for the airspace in which the UAV is operating, with the exception of ACAS*	Para 15.1
FSR-16	UAVs should carry appropriate equipment to ensure UAV Pilots in Command are provided with an accurate situational indication equivalent to that provided to a pilot of a manned aircraft	Paras 6.2 and 9.3
FSR-17	*While in receipt of an air traffic service, the UAV Pilot in Command should maintain two-way communications with ATC, using standard phraseology when communicating via RTF. The word "unmanned" should be included on first contact with an ATC agency*	Paras 9.2 and 12.1

Ref	Safety Requirement	Traceability to Annex E of the Draft Specifications
FSR-18	*Where UAV emergency procedures necessarily differ from those for manned aircraft e.g. UAV control link hijacking, security breaches etc., they should be designed to ensure the safety of other airspace users and people on the ground, and they should be coordinated with ATC as appropriate*	Para 10.1
FSR-19	UAV Pilots in Command shall be able to respond to separation provision instructions and manoeuvre UAVs via a control link at least as quickly as a pilot can receive an instruction and manoeuvre a manned aircraft	**Not covered within the Draft Specification [1]**
FSR-20	*With regard to cross-border operations, state UAVs should be bound by the same international conventions as manned state aircraft. In addition, flights by state UAVs into the FIR/UIR of other states should be pre-notified to the relevant FIR/UIR authorities, normally by submission of a contingency plan. ATC transfers between adjacent states should accord with those for manned aircraft*	Para 14.1
FSR-21	UAVs Pilots in Command shall have equivalent piloting skills to pilots of conventional aircraft, enabling them to monitor, control and operate the air vehicle in a manner comparable to manned aircraft	Para 13.1
FSR-22	UAV Systems shall provide an indication to Pilots in Command when the UAV Control Link has been lost and the UAV is operating autonomously	**Not covered within the Draft Specification [1]**
FSR-23	Autonomous UAV separation provision systems should have equivalent efficacy to a pilot performing separation provision actions	Para 3.1, 6.2 and 9.4
FSR-24	Where a UAV is unable to continue to comply with any of the requirements for operations in non-segregated airspace then the UAV should be segregated from all other airspace users as soon as practicable	Para 9.5 and 11.1

Ref	Safety Requirement	Traceability to Annex E of the Draft Specifications
FSR-25	When the UAV Control Link has been lost Pilots in Command shall inform ATC as soon as possible	**Not covered within the Draft Specification [1]**
FSR-26	UAV Systems shall provide an indication to ATC when the UAV is operating autonomously	**Not covered within the Draft Specification [1]**
Mitigating Safety Requirements		
MSF-01	Pilot in Command must inform ATC when unable to comply with any ATC instruction	Paras 4.1 and 12.2
MSF-02	UAVs shall be fitted with suitable conspicuity devices to aid visual acquisition by other airspace users.	Para 6.2
MSF-03	Whilst for manned and unmanned operations the PIC is a common factor to both the Separation Provision and Collision Avoidance functions, to reduce the risk to AFARP then implementation of these functions should be as independent as far as is reasonably practicable	**Not covered within the Draft Specification [1]** **See Safety Issue 8**
MSF-04	Following failure of the UAV Collision Avoidance System, the UAV flight should be terminated as soon as safely practicable	Para 10.1
MSF-05	The PIC must inform ATC as soon as he becomes aware that the UAV is responding incorrectly to any ATC instruction	Paras 4.1 and 12.2
MSF-06	Pilot in Command must inform ATC of any intentional deviation from an ATC instruction	Paras 4.1 and 12.2
MSF-07	Pilot in Command must inform ATC of any delayed response to an ATC instruction	Paras 4.1 and 12.2
MSF-08	In the event of loss of Separation Provision from ATC the Pilot in Command shall attempt to contact ATC, if the attempt fails the Pilot in Command should follow lost communications procedures as per Manned operations	Paras 10.1 and 12.1
MSF-09	*UAVs should comply with VFR and IFR as they affect manned aircraft flying OAT*	Para 4.1
MSF-10	*UAVs should comply with the right-of-way rules as they apply to other airspace users*	Para 5.1

Table 16 – Traceability between FHA/PSSA Safety Requirements and Draft Specification

Appendix I Draft Specification Traceability Table

Para	Draft Specification	Traceability
1.1	For ATM purposes, where it becomes necessary to categorize UAV operations, this should be done on the basis of flight rules, namely IFR or VFR as applied to OAT	General requirement. See Functional Models Figure 1, Figure 8 and Figure 9
2.1	During UAV operations involving the use of a chase aircraft, the flight should be classified as a formation flight and should have the same right-of-way status as aircraft engaged in airborne refueling or towing	See Scoping Statement 4. UAVs operating with Chase Aircraft are considered outside the scope of the analysis
3.1	For ATM purposes, the primary mode of operation of a UAV should entail oversight by the pilot-in command. A back-up mode of operation should enable the UAV to revert to autonomous flight in the event of total loss of control data-link between the pilot-in-command and the UAV. This back-up mode of operation should ensure the safety of other airspace users	See FSR-04, FSR-07 and FSR-23
4.1	UAVs should comply with VFR and IFR as they affect manned aircraft flying OAT. For VFR flight, the UAV pilot-in-command should have the ability to assess in-flight meteorological conditions	MSF-01, MSF-05, MSF-06, MSF-07 and MSF-09
5.1	UAVs should comply with the right-of-way rules as they apply to other airspace users	MSF-10
6.1	For IFR OAT flight by UAVs in controlled airspace, the primary means of achieving separation from other airspace users should be by compliance with ATC instructions. However, additional provision should be made for collision avoidance against unknown aircraft	See FSR-03 and FSR-10
6.2	For VFR OAT flight by UAVs, the UAV pilot-in command should utilize available surveillance information to assist with collision avoidance. In addition, technical assistance should be available to the pilot-in-command to enable him to maintain VMC and to detect and avoid conflicting traffic. An automatic system should provide collision avoidance in the event of loss of control data-link	See FSR-10, FSR-16, FSR-23 and MSF-02

Para	Draft Specification	Traceability
7.1	A UAV S&A system should enable a UAV pilot-in-command to perform those collision avoidance functions normally provided by a pilot in a manned aircraft, and it should undertake similar collision avoidance functions automatically in the event of loss of control data-link. The S&A system should achieve an equivalent level of safety to an aircraft with a pilot onboard	See FSR-10
7.2	A UAV S&A system should notify the UAV pilot-in command when another aircraft in flight is projected to pass within a specified minimum distance. Moreover, it should do so in sufficient time for the UAV pilot-in command to manoeuvre the UAV to avoid the conflicting traffic by at least that distance or, exceptionally, for the onboard system to manoeuvre the UAV autonomously to miss the conflicting traffic	See FSR-02
8.1	Within controlled airspace where primary collision avoidance is provided by ATC, the separation minima between UAVs operating IFR and other IFR traffic should be at least the same as for manned aircraft flying OAT in the same class of airspace	See FSR-02
8.2	Where a UAV pilot-in-command has primary responsibility for collision avoidance, he should maintain a minimum distance of 500ft between his UAV and other airspace users, regardless of how the conflicting traffic was detected and irrespective of whether or not he was prompted by a S&A system	See FSR-09 and **Safety Issue 7**
8.3	Where a UAV system initiates collision avoidance autonomously, it should achieve miss distances similar to those designed into ACAS. The system should be compatible with ACAS	See FSR-11 and FSR-12
9.1	UAV operations at airfields should interface with ATC as near as possible in the same way as manned aircraft	See FSR-01
9.2	When taxiing, and in the absence of adequate technical assistance, a UAV should be accompanied by ground-based observers, who should be in communication with ATC and with the UAV pilot-in-command	See FSR-10 and FSR-17
9.3	For take-off and landing and flight in an airfield visual circuit when VFR apply, the UAV pilot-in-command should be able to view the runway and the airfield circuit to fulfill his responsibility for collision avoidance, and he should comply with ATC instructions	See FSR-10 and FSR-16
9.4	For take-off and landing at an airfield when IFR apply, the pilot-in-command should comply with ATC instructions but without any requirement to be able to view the runway and airfield circuit	See FSR-10 and FSR-23
9.5	Where safe integration is impracticable, consideration should be given to excluding other aircraft from the airspace in the immediate vicinity of an airfield during the launch and recovery of UAVs	See FSR-24

Para	Draft Specification	Traceability
10.1	Where UAV emergency procedures necessarily differ from those for manned aircraft, they should be designed to ensure the safety of other airspace users and people on the ground, and they should be coordinated with ATC as appropriate	See FSR-18, MSF-04 and MSF-08
11.1	Where a UAV system cannot meet the technical and/or functional requirements for operation as OAT, the sortie should be accommodated within temporary reserved airspace to provide segregation from other airspace users	See FSR-01 and FSR-24
12.1	While in receipt of an air traffic service, the UAV pilot-in command should maintain 2-way communications with ATC, using standard phraseology when communicating via RTF. The word ‘unmanned’ should be included on first contact with an ATC agency	See FSR-17 and MSF-08
12.2	The air traffic service provided to UAVs should accord with that provided to manned aircraft	See FSR-01, MSF-01, MSF-05, MSF-06 and MSF-07
12.3	Where flight by manned aircraft requires the submission of a flight plan to ATC, the same should apply to flight by UAVs. The UAV flight plan should indicate that it relates to an unmanned aircraft, and should include details of any requirement for en-route holding	See FSR-08
12.4	While in receipt of air traffic service, UAVs should be monitored continuously by the UAV pilot-in command for adherence to the approved flight plan	See FSR-04
13.1	The weather minima for UAV flight should be determined by the equipment and capabilities of each UAV system, the qualifications of the UAV pilot-in command and the class of airspace in which the flight is conducted	See FSR-05 and FSR-21
14.1	With regard to cross-border operations, state UAVs should be bound by the same international conventions as manned state aircraft. In addition, flights by state UAVs into the FIR/UIRs of other states should be pre-notified to the relevant FIR/UIR authorities, normally by submission of a flight plan. ATC transfers between adjacent states should accord with those for manned aircraft	See FSR-20
15.1	UAVs should carry similar equipment for flight, navigation and communication as required for manned aircraft when flying VFR and IFR, with the exception of ACAS. The exemption policy for manned state aircraft with regard to specific equipage requirements should also apply to state UAVs	See FSR-15

Table 17 – Traceability between Draft Specification and FHA/PSSA Safety Requirements

Appendix J FHA/PSSA Relationship Diagram

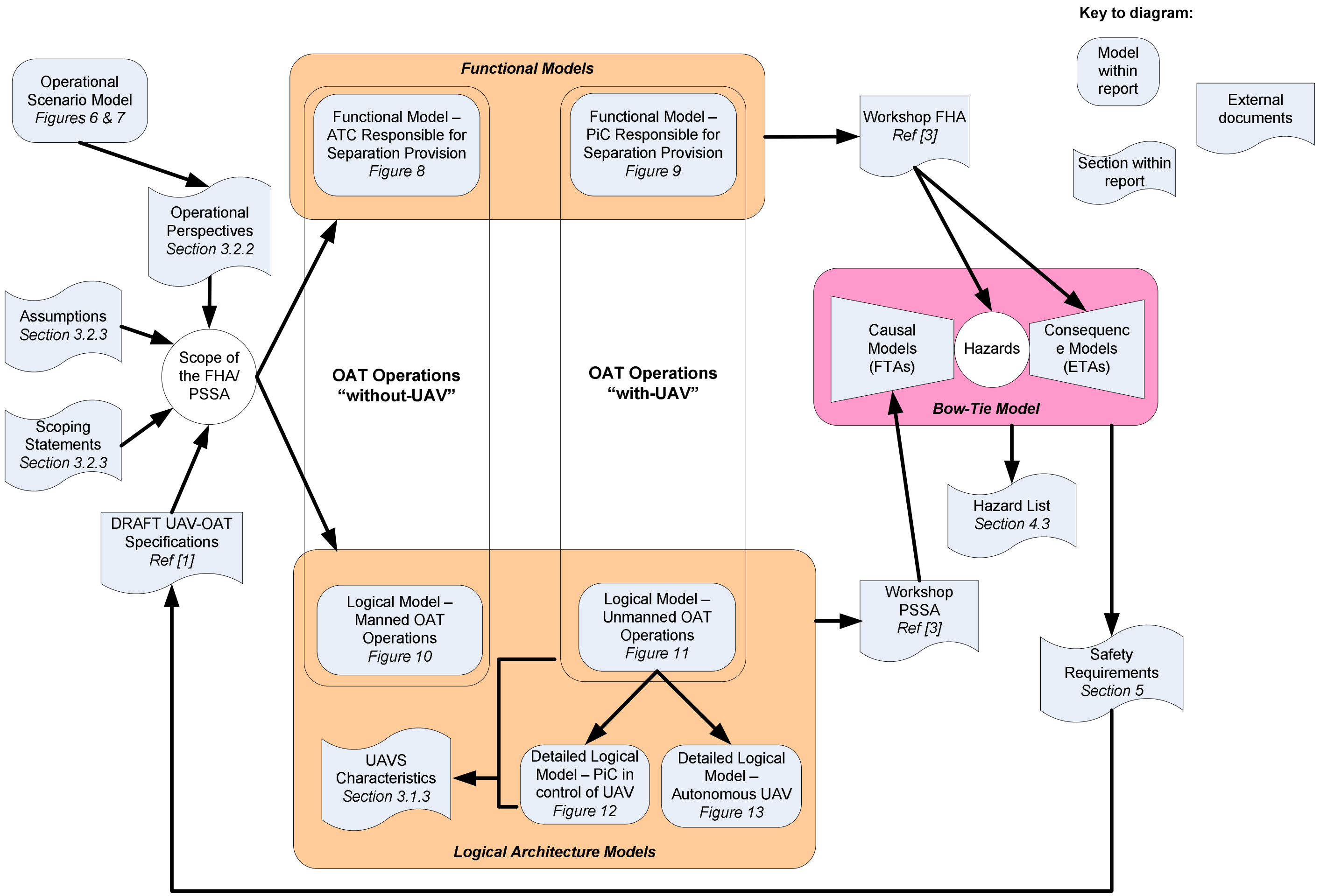

Key to diagram:
Model within report
External documents
Section within report
Operational Scenario Model Figures 6 & 7
Operational Perspectives Section 3.2.2
Assumptions Section 3.2.3
Scoping Statements Section 3.2.3
Scope of the FHA/ PSSA
DRAFT UAV-OAT Specifications Ref [1]
Functional Models
Functional Model – ATC Responsible for Separation Provision Figure 8
Functional Model – PiC Responsible for Separation Provision Figure 9
OAT Operations "without-UAV"
OAT Operations "with-UAV"
Logical Model – Manned OAT Operations Figure 10
Logical Model – Unmanned OAT Operations Figure 11
UAVS Characteristics Section 3.1.3
Detailed Logical Model – PiC in control of UAV Figure 12
Detailed Logical Model – Autonomous UAV Figure 13
Logical Architecture Models
Workshop FHA Ref [3]
Causal Models (FTAs)
Hazards
Consequence Models (ETAs)
Bow-Tie Model
Hazard List Section 4.3
Workshop PSSA Ref [3]
Safety Requirements Section 5

Figure 44 – FHA/PSSA Relationship Diagram