T4 Report - Simulation Campaign & Safety Case Assessment (D3)

MALE RPAS Accommodation Study

EDA CALL REFERENCE: 17.CPS.OP.017

Doc. Ref: SIRENS/20180906/T4/003

Issue 05 – 19th October 2018

Team SIRENS:

Thales UK

Manor Royal
Crawley
West Sussex, RH10 9HA
United Kingdom

Netherlands Aerospace Centre (NLR)

Anthony Fokkerweg 2
1059 CM Amsterdam
The Netherlands

This page is intentionally left blank

Table of Contents

List of References

1 EUROCONTROL ESARR 4 - Risk Assessment and Mitigation in ATM
2 EUROCONTROL SAM/SAME - Safety Assessment Methodology
3 EUROCONTROL Air Traffic Management Guidelines for GLOBAL HAWK in European airspace
4 EUROCONTROL RPAS ATM Concept of Operations (February 2017)
5 EUROCONTROL Roadmap for the integration of civil RPAS into the European Aviation System
6 EUROCONTROL European Operational Concept Validation Methodology - EOCVM
7 EUROCONTROL E-OCVM Version 3.0 - Volume II Annexes – Safety Case description; Master Plan RPAS Addendum
8 EASA Policy Statement: Airworthiness Certification of Unmanned Aircraft Systems (UAS) - E.Y01301 and EASA Rule Making Task.0230
9 EASA RMP-EPAS 2017-2021
10 EASA NPA 2017-05
11 JARUS Guidelines on Specific Operations Risk Assessment (SORA)
12 JARUS SORA tool (dated July 2017)
13 SESAR, European ATM Master Plan, Edition 2015
14 ICAO 9854 Global Air Traffic Management Operational Concept
15 ICAO 4444 Procedures for Air Navigation Services Air Traffic Management
16 ICAO 8173 Procedures for Air Navigation Services – Aircraft Operations
17 ICAO 9859 Safety Management Manual
18 ICAO RPAS Concept of Operations Edition 4 (March 2017)
19 ICAO 10019 Manual on RPAS
20 SESAR JU Project CLAIRE (RPAS.07) Demonstration Report, Edition 01.00.00, 30/11/2015
21 NATO Standardisation Agreement (STANAG) 4671
22 EDA Study on RPAS Detect And Avoid (15.CAT.OP.138)
23 EUROCONTROL Specifications for the use of Military RPAS as OAT
24 MALE RPAS Accommodation Study Technical Proposal – November 15 2017 (Team SIRENS)
25 SESAR Safety Reference Material (SRM) – 16.06.01/D27
26 ASTRAEA Entry Level Detect and Avoid Virtual Safety Assessment Report – P11003.10.6, 31 May 2013
27 SIRENS D1 - General Approach and Safety Assessment Method Definition – Issue 04 - 24th July 2018
28 SIRENS D2 – Simulation Readiness Report – Issue 5.0, August 2018

List of Figures

List of Tables

Document History

Issue	Date	Reason for change
Draft 01	6th August 2018	Initial framework for internal review
Draft 02	17th August 2018	Document update incorporating Safety Methodology inserts and text updates
Draft 03	29th August 2018	Update incorporating ATM detail and inserts from NLR on Simulation Campaign
Draft 04	30th August 2018	SIRENS Draft for internal review
Issue 01	26th September 2018	First Issue to EDA customer
Issue 02	3rd October 2018	Revised Issue following customer review and re-work
Issue 03	3rd October 2018	Restructuring to address EDA Stakeholder key concerns regarding linking aspects of the study and ease of readership
Issue 04	4th October 2018	Reconciliation with final comments spreadsheet and print-ready
Issue 05	19th October 2018	Updated to incorporate Stakeholder (EDA & EUROCONTROL) comments raised at D3 Workshop on 5th October 2018

Number of pages: 73

Executive Summary

Team SIRENS has developed an holistic Air Systems Safety Case assessment methodology by combining together the key elements of: Equipment Safety, Operational Organization Safety and Air Traffic Management Safety, based on systems already in place for an in-service Military-type, Tactical UAS and outputs from the SESAR ATM Safety Case assessment [Ref. 25]. This methodology was then used to assess the top-level **"Claim"** that it will be ***safe to fly a MALE-type RPAS in the two Implementation Scenarios*** previously derived in D2 [Ref. 28] by providing a number of ***"Arguments"*** and ***"Evidence"*** to support the claim (see below).

"Arguments" are provided in the form of high-level safety statements such as: *"All ATCO's will be Suitably Qualified Experienced Persons (SQEP)"* and *"The RPAS has the correct type-certification and has been properly maintained"* and are supported at a more detailed, lower level by the results of conducting a Hazard Analysis (using the methodology developed during this study). The hazard analysis is designed to identify things that would undermine or invalidate the **Claim**. Each hazard is characterised by one or more **"Top-Level Events"** (TLEs) the occurrence of which would potentially lead to a **"Consequence"** which is usually a **"Risk to life".** Each TLE is devolved into a series of ***"Threats"*** which could individually cause the TLE to occur and each threat is analysed in order to identify one or more "***Barriers***" that would eliminate or minimise the probability of occurrence of the threat resulting in the TLE. The consequence of a TLE resulting in a risk to or loss of life is analysed and mitigated by identifying further barriers that aim to reduce the impact of the TLE.

The outcome of this analysis results in the generation of ***"Evidence"*** to support the ***"Arguments"*** and to prove that the original ***"Claim"*** is justified.

Another key part of proving each ***"Argument"*** is to ensure that each of the identified ***"Threats"*** are real and that the ***"Barriers"*** are sufficient, either individually or collectively, to reduce the risk of the consequences occurring to ALARP[1]. This verification exercise was undertaken in a series of Real-Time Simulations conducted under the Simulation campaign (see Section 4).

The entire Air Systems Safety Case (ASSC) is too large to summarise in this study but the principles and methodology can be fully illustrated by taking a single 'thread' through the aforementioned Claim, Argument, Evidence, Simulation cycle. This document examines two such 'threads' comprising a 'generic' as well as a 'RPAS specific' worked example to highlight the approach advocated by team SIRENS.

Claim: ***It will be safe to fly a MALE-type RPAS from Rotterdam under Netherlands ATC over the North Sea towards the UK, crossing the border into UK airspace and handing over ATC responsibilities to UK ATCOs; for the MALE-type RPAS to then conduct a Military ISR Mission in UK airspace and when complete, returning back into Netherlands airspace under Netherlands ATC to return to its operating base in Rotterdam.*** (Please note that take-off and landing and ground operations are outside the scope of this study).

[1] As Low As Reasonably Practicable

Argument: Clearly this claim is multi-dimensional and covers many and varied aspects but there are a number of basic measures in place that apply to each scenario which help support the claim such as:

In terms of '**Equipment'** we argue that flying the two ***Implementation Scenarios*** (as described in D2 and Section 2 of this document) will be safe because the RPAS has type certification, it is maintained by SQEP under a strict set of institutionalised rules, procedures and supervision and that the correct flight permit has been granted by the relevant authorities. In essence, the Air system design is safe because:

- The Design organisation are appropriately trained, assessed & approved
- Air System – Type approval certificate/Flight permit/release to service (military)
- Equipment – Robust qualification/testing process
- Approved Maintenance provider – Licenced Engineers etc…
- Continued Airworthiness oversight is provided by the organisation

In terms of '**Operational Organisation'** we argue that flying the two ***Implementation Scenarios*** will be safe because the organisation is subject to a regulated Design Approvals process, that the team operate to strictly-controlled and regulated procedures and are all SQEP. In detail, the Operational Organisation is safe because:

- Operators & Maintainers are appropriately trained, assessed & approved.
- Terms Of Reference (TORs) are in place for all staff and the Staff are suitably Qualified & Experienced
- The organisation is compliant to appropriate Regulations
- Risk to Life (RtL) is understood and managed within the organisation
- Appropriate processes are in place to support the claim the Operational Organisation is safe.

In terms of '**Air Traffic Management'** we argue that flying either of the two ***Implementation Scenarios*** will be safe because the ATCOs are SQEP and they follow strictly enforced and supervised procedures. In detail, the Air traffic Management Organisation is safe because:

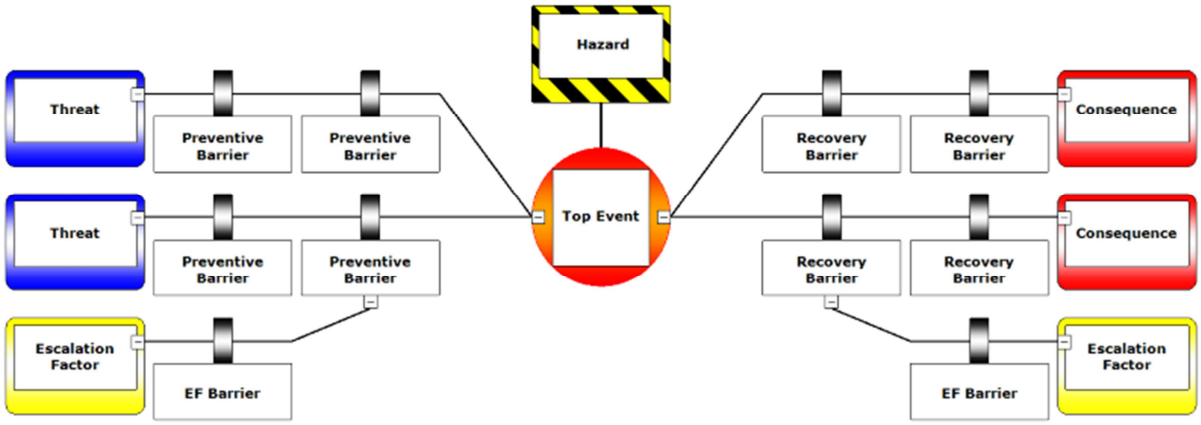
- Air traffic controllers are appropriately trained, assessed & approved.
- Standardised Air Traffic Management processes are used.
- The ATM organisation is compliant with appropriate regulations including any additional RPAS Accommodation procedures.

Our methodology is risk-based and concentrates on the identification and mitigation of ***Hazards*** before they become ***Consequences*** where the main consequences are risk to and ultimately loss of life. Essentially we have one 'Hazard' – ***It is dangerous to fly MALE-type RPAS alongside manned aviation*** and expert analysis / decomposition of this hazard has led to the identification of six Top Level Events (TLEs), any one of which could lead to an occurrence of the hazard. Each TLE is then broken-down into a number of ***Threats*** that could each lead to the realisation of a TLE. Threats have been determined using operational experience across all domains of the ASSC, prior art and intimate

knowledge of the problem space and for each threat, we propose one or more ***Barriers*** designed to prevent / reduce the probability of occurrence of the TLE leading to the hazard being realised.

On the ***"Consequences"*** side we also propose mitigation ***Barriers*** that aim to reduce the severity of the consequence once the hazard has occurred. For example, if the hazard is a fire and the ultimate consequence of the fire is loss of life or lives, the presence and availability of fire-fighting crew and equipment is a 'Barrier' to help prevent the ultimate extreme of the consequence – the fire will happen but no one will die because the fire brigade will put out the fire and effect a rescue beforehand, but some people may get burned and/or suffer smoke inhalation and their house will be damaged.

Our methodology captures and illustrates this risk analysis in the form of 'BowTie' diagrams which can be found in their entirety in Annex B. Below is a generic BowTie diagram illustrating the Hazard and a TLE (which could be one of many) that would lead to the Hazard occurring. The diagram shows the TLE with Threats on the left-hand side and Consequences on the right-hand side - each mitigate by introducing Preventative or Recovery Barriers (depending on whether the barrier is preventing a threat of recovering from a consequence).



If we consider the risk of Mid-Air Collision (MAC), one of the TLEs that could result in such an event, is 'Loss of Separation' which can be mitigated in several ways. For example, separation assurance services will be provided by the ATCOs 'as if' the MALE-type RPAS were manned aviation but it could also be mitigated by automatic sensing equipment to provide warnings and alerts to both the RPAS Pilots and ATCOs and, in extremis, by automatic flight procedures that take control to prevent airborne collisions . The risk analysis conducted highlighted potential loss of separation as a risk that could lead to loss of life in either the 1st, 2nd or 3rd party[2]. As this is a 'real' RPAS specific issue team SIRENS decided to verify the Threat and examine the barriers during the Simulation campaign by dedicating a simulation run to this threat.

[2] 1st party means flight crew or passengers on-board, 2nd party means other personal involved in operating the system or other airspace users and 3rd party means members of the general public

During the study and particularly during the Simulation campaign, the ATCOs interviewed agreed that 'Loss of Separation' is a key part of their day-to-day job and that maintaining the ability to ensure adequate separation will be a major concern to them as RPAS begin to be accommodated in the airspace alongside manned aviation. This was further vindication of our analysis and the selection of this issue to be simulated. On the other hand, in the actual simulation run we found that the ATCOs predicted the impending loss of separation a significant time before it would have occurred and took appropriate avoidance measures. When questioned they said it was "all part of their day-job", something they are trained to do and something routine they almost do automatically regardless of the presence of a pilot on the platform.

This led us to question whether the simulation run was sufficiently complex but the background (commercial) air traffic used had been recorded on a 'normal', busy day and so was clearly representative of current real world operations. We are left to conclude, that under current circumstances, the ATCOs are able to cope adequately with the threat of loss of separation between an RPAS and one intruding manned aircraft. Nonetheless, team SIRENS recognise that there are several unanswered questions such as:

- What happens as the level of background air traffic and airspace complexity increases?
    - At what point would 'normal' ATCOs start to miss spotting and dealing with potential conflicts?
    - Is there a point where the level of traffic is so high that the ATCOs could get overwhelmed and this Barrier begins to fail?
    - What then is the potential for the hazard to occur leading to consequential risk to life?
- What happens if there are more RPAS for the ATCOs to manage? At what point would the same set of issues outlined above start to occur?
- What happens if RPAS pilots begin to fly more than one Aircraft each? Does their ability to liaise with ATC diminish and at what point does this represent a failure of the Barrier leading to the occurrence of the TLE/Hazard?
- What happens in a contingency situation where an RPAS performance is compromised in some form? The Simulation Campaign covered datalink failure and degradation but did not cover issues such as reduced rate of climb or loss of manoeuvrability.
- What happens if all of these situations occur?

Evidence: Our ***"Argument"*** that the original claim is true ***– it IS safe to fly a MALE-type RPAS in either scenario 1 or 2*** – is backed-up by the ASSC as described in the Bowties presented in Annex B and a number of key elements (threats and barriers) that have been verified via Simulation. Notwithstanding this, the treatment is not complete, not all threats and barriers have been fully verified but we believe that the methodology is sound and, if applied completely and comprehensively, would provide sufficient ***"Evidence"*** to support the **"Claim"** fully.

Our recommendation is that additional of Simulation runs be conducted to complete the verification exercise and to explore the additional levels of complexity described above (the set of outstanding questions) individually and in combination in order to understand ATCO limits so that the skies can be kept safe while increasing air traffic densities and accommodating MALE-type RPAS. In addition,

other elements of the Safety Case not explored, such as take-off and landing, engine failure or the incremental addition of DAA equipment could also be examined.

Another recommendation is that the next steps in flying MALE-type RPAS alongside manned aviation keep the air traffic density levels at or below the ones simulated by this study until the aforementioned experiments have been conducted and the results analysed and incorporated.

The BowTies developed under this study can be found in Annex B and it is worth noting their providence. Six TLEs were identified using the analysis of a military-type UAS (in terms of Equipment and Operational Organization) and another six were identified in the SESAR ATM work covered in the SESAR Safety Reference Material [Ref. 25]. Team SIRENS was then able to successfully amalgamate these hazards into a composite set of six top-level BowTie diagrams with all of the ATM Hazards incorporated as Threats to already identified TLEs.

Finally, whilst it was the intention to conduct a quantitative analysis within the BowTies it was not possible to give an accurate quantitative analysis due to the generic nature of the study. No specific MALE RPAS was used and assumptions over Human factors issues were not able to be sensitised to the platform and operating areas.

In summary, we believe that the methodology developed is sound and can be used as a basis to develop a more comprehensive Safety Case Assessment in order to go fly MALE-type RPAS alongside manned aviation under certain circumstances. We also believe that the safety case is a solid beginning to the goal of integrating MALE-type RPAS alongside manned aviation

1 Introduction

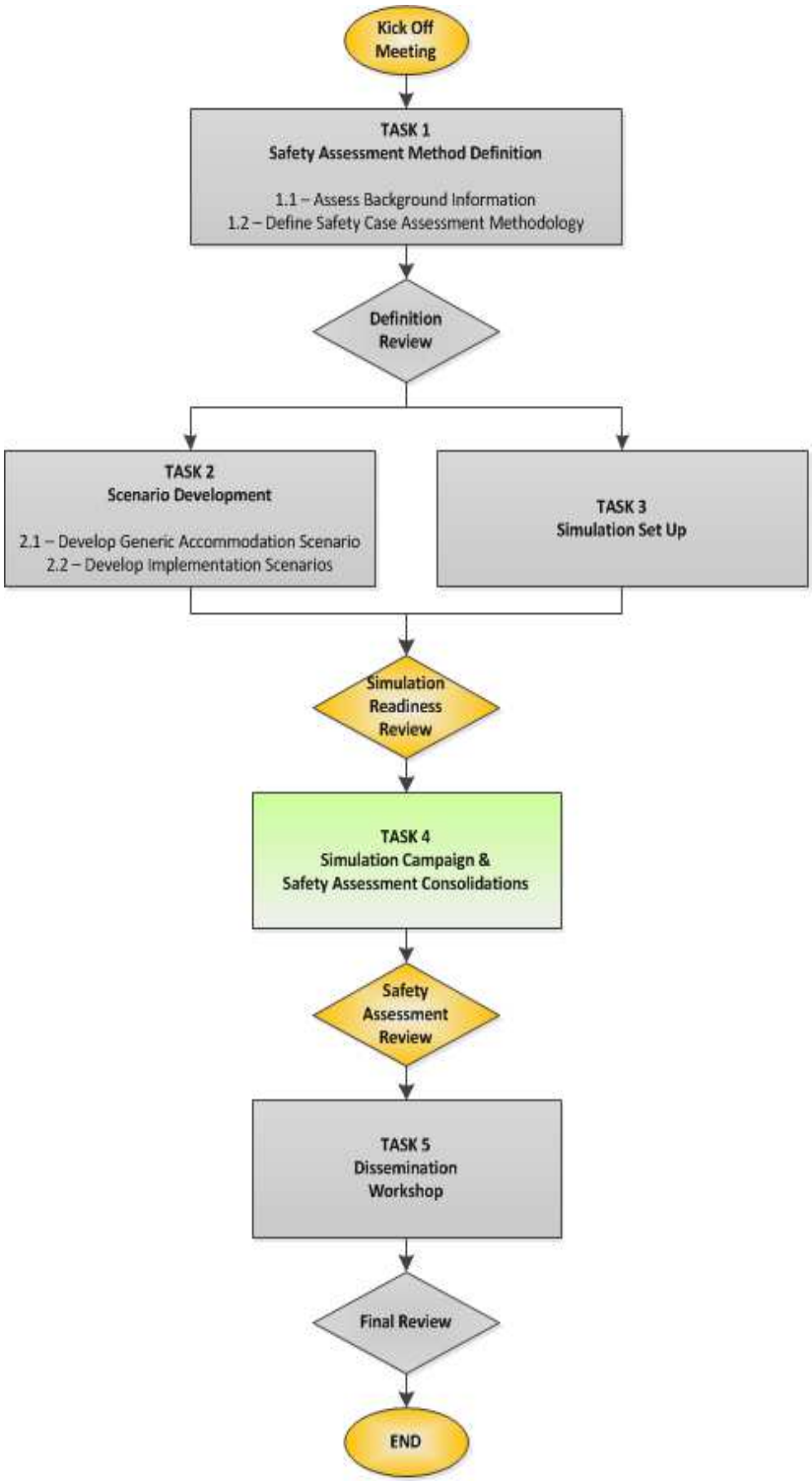


Figure 1 - Project Process Flow Illustrating Task 4

1.1 Document Purpose

This document is the Milestone deliverable (D3) report for Task 4 of the MALE RPAS Accommodation Study (Ref: 17.CPS.OP.017) let by the EDA to Team SIRENS at the Project Launch Workshop held at EDA HQ in Brussels on January 11th 2018.

This study set out to deliver an enhanced Aviation Safety Case Assessment Methodology for RPAS by assimilating and consolidating current best practice across both manned and unmanned aviation, testing this methodology through simulation and developing a consolidated version of the generic RPAS Accommodation scenario to allow all aspects of aviation hazard analysis to be exercised for MALE-type RPAS integration into European skies alongside manned aviation.

Figure 1 illustrates the planned flow of activities to be undertaken during this study programme and the position of Task 4 within that structure.

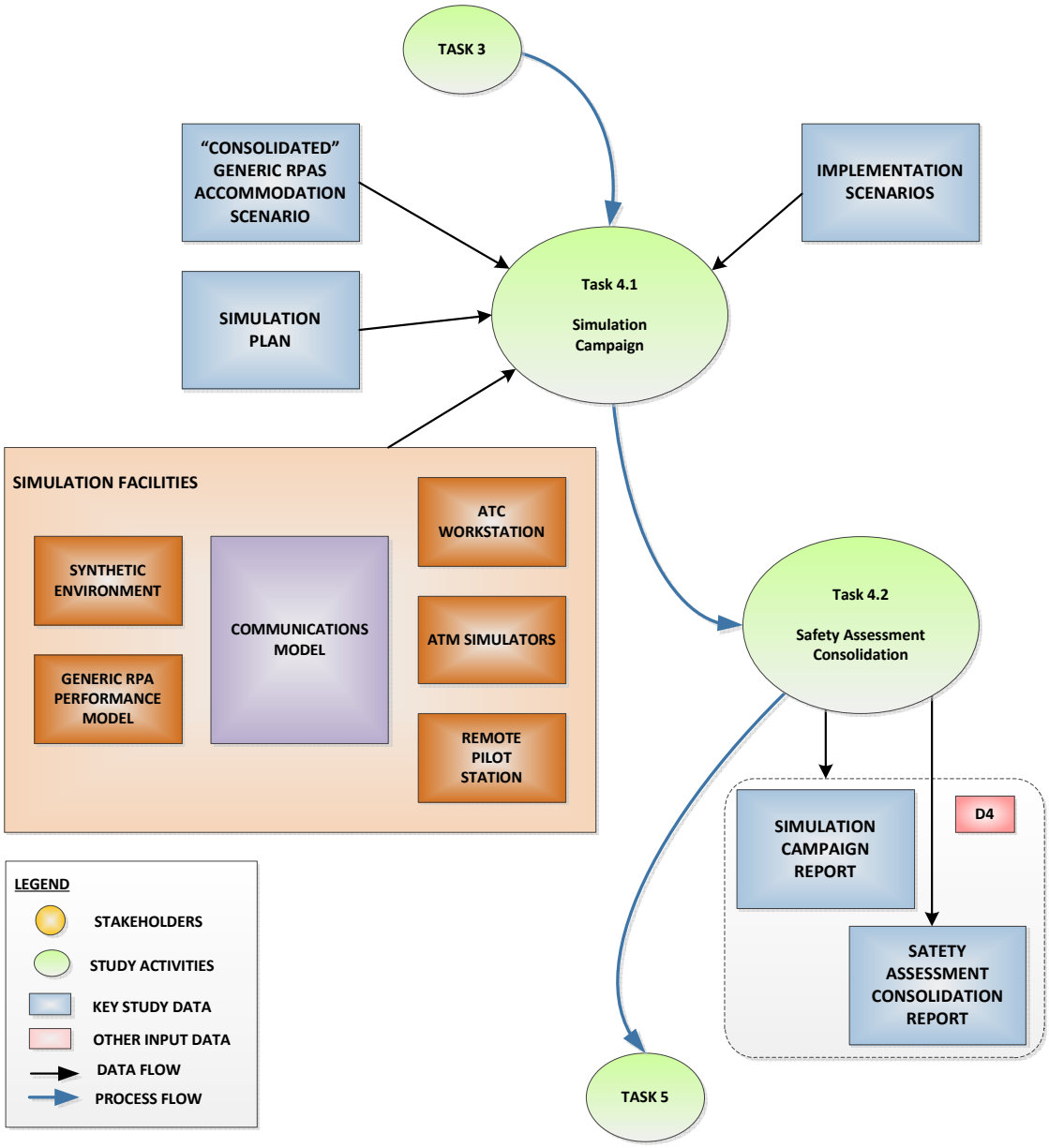


Figure 2 - Activity Flow & Task Decomposition

1.2 Task 4 – Conduct

Figure 2 illustrates the sequence of activities that have been undertaken to complete Task 4 in which Team SIRENS were able to validate aspects of the previously reported Safety Case Assessment Methodology based on the Simulation Campaign as reported in this document. The derived simulation scenarios (as defined in Task 3) were run in the NLR simulation facilities to trial the methodology against a set of agreed Implementation Scenarios (IS) as reported in Task 2. The results of the simulation exercises and safety assessment process will be presented to the EDA and other stakeholders for comment prior the forthcoming Safety Assessment Review Meeting in Brussels.

1.3 Longer-term Aims

The EDA have embarked on a longer-term strategy to enable the safe and routine integration of RPAS into European airspace alongside manned aviation and this study forms an important part of the initial work programme aimed at achieving that longer-term goal – more information may be found at:

https://www.eda.europa.eu/what-we-do/activities/activities-search/remotely-piloted-aircraft-systems---rpas/

Figure 3 illustrates the contribution made by this study in the overall drive towards the safe Integration of MALE-type RPAS alongside manned aviation in European skies. The activities will help define future requirement and outstanding challenges necessary to advance from accommodation to full integration of RPAS unlocking potential set operational, economic and environmental benefits for all member states. It is important to recognise how aspects of the safety assessment and validation methodology can be reused to undertake more enduring and higher fidelity studies in the future.

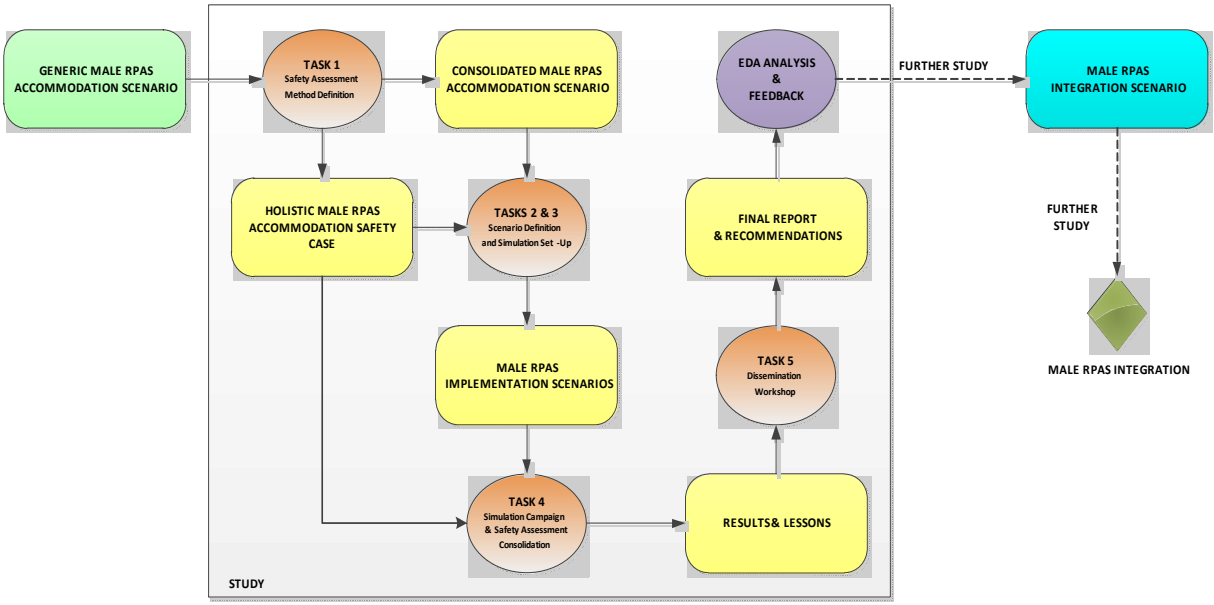


Figure 3 - Study Linkage Diagram

2 Implementation Scenarios

Two Implementation Scenarios were developed during Task 2 of this study and their derivation was described in D2 – Simulation Readiness Report [Ref.28]. Figure 4 below illustrates how the Implementation Scenarios were developed and used to support the simulation campaign within the context of the overall RPAS accommodation study.

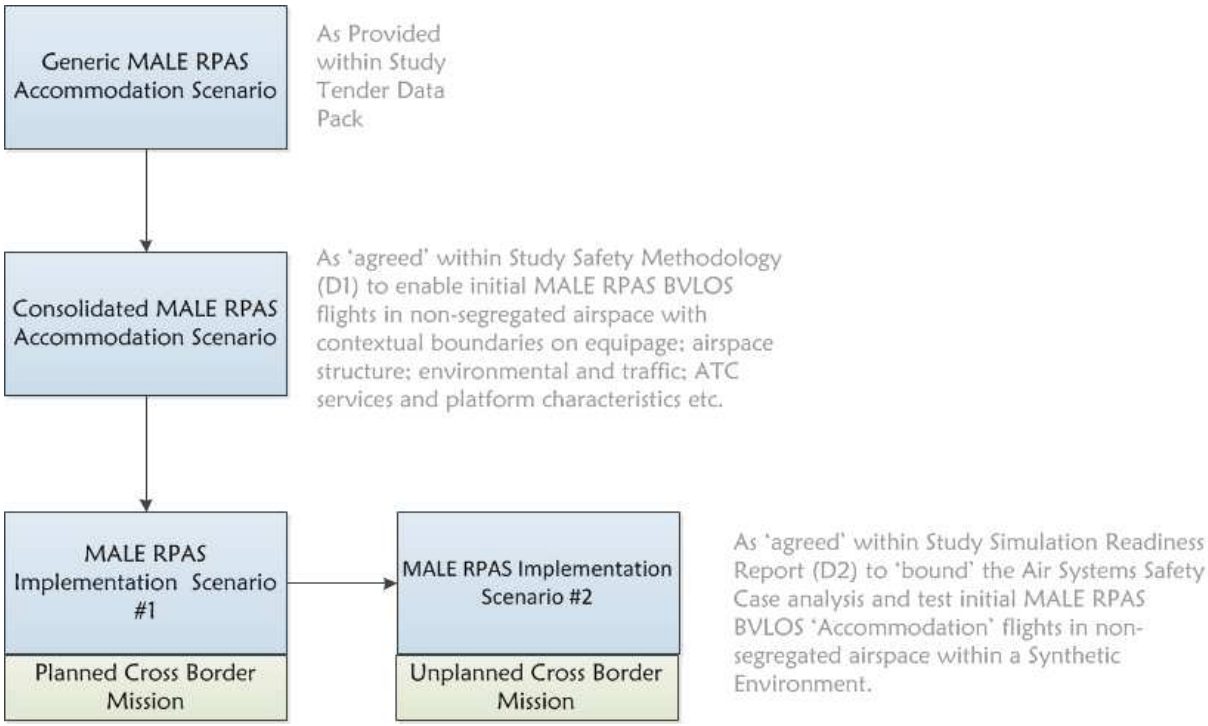


Figure 4 - Implementation Scenarios

Scenario 1 covers a pre-planned cross-border operation that begins in Rotterdam a single runway mid-sized airport, which for the purposes of this study was chosen as a representative RPAS operating base that may be able to support MALE type RPAS operations. The geographic location was deemed to be ideal because team SIRENS needed to be able to simulate cross-border operations between EU Member States (and so naturally chose The Netherlands and the UK). Furthermore, Rotterdam already existed in the NLR Simulation environment.

The MALE-type RPAS takes off from Rotterdam and flies a route over the North Sea towards the UK. Once the RPAS reaches the airspace border, it crosses-over into UK controlled airspace under jurisdiction of UK ATCOs. Air traffic control is therefore handed over between The Netherlands and UK controllers as agreed in the previously filed flight plan and in accordance with extant authorisations and protocols before the RPAS took off. Once in UK airspace the RPAS flies into the Mission operational area and conducts the military mission (in a pre-determined volume of segregated airspace). When the military mission is complete the RPAS transitions back across the border, control is handed back to Netherlands ATC and the RPAS returns to its base in Rotterdam. This particular scenario was chosen to examine the issues of hand-over between different national

ATC jurisdictions even when it had been pre-planned and agreed and to explore how the ATCOs and RPAS Pilots interacted.

Scenario 2 begins at Rotterdam airport but this time the RPAS Mission area is further north along the Dutch coast and the scenario implements an 'unplanned' cross-border operation due to an urgent operational mission necessity. The RPAS leaves Rotterdam FIR and flies north along the Dutch coast to the mission area. Once it has started the mission it is re-tasked to perform a different mission across the border in UK airspace (in a different area to that used in Scenario 1). Once complete the RPAS requests to return back across the border into Netherlands airspace and then flies back to base at Rotterdam. This scenario was chosen to examine the issues emerging when the border crossing (and re-crossing) was not pre-planned and pre-agreed.

Each of these scenarios was used as the baseline for the Simulation runs. Simple runs were performed with no emergencies (occurrence of 'Threat') to provide a baseline understanding of 'normal' workload for all participants. Other simulation runs were then used to explore ATCO and RPAS Pilot behaviors in response to threat events that could lead to hazards and consequences in order to verify the Safety Case Assessment and analysis conducted thus far.

Figure 5 below illustrates how the two Implementation Scenarios were implemented, tested and verified in the Simulation campaign via separate simulation runs:

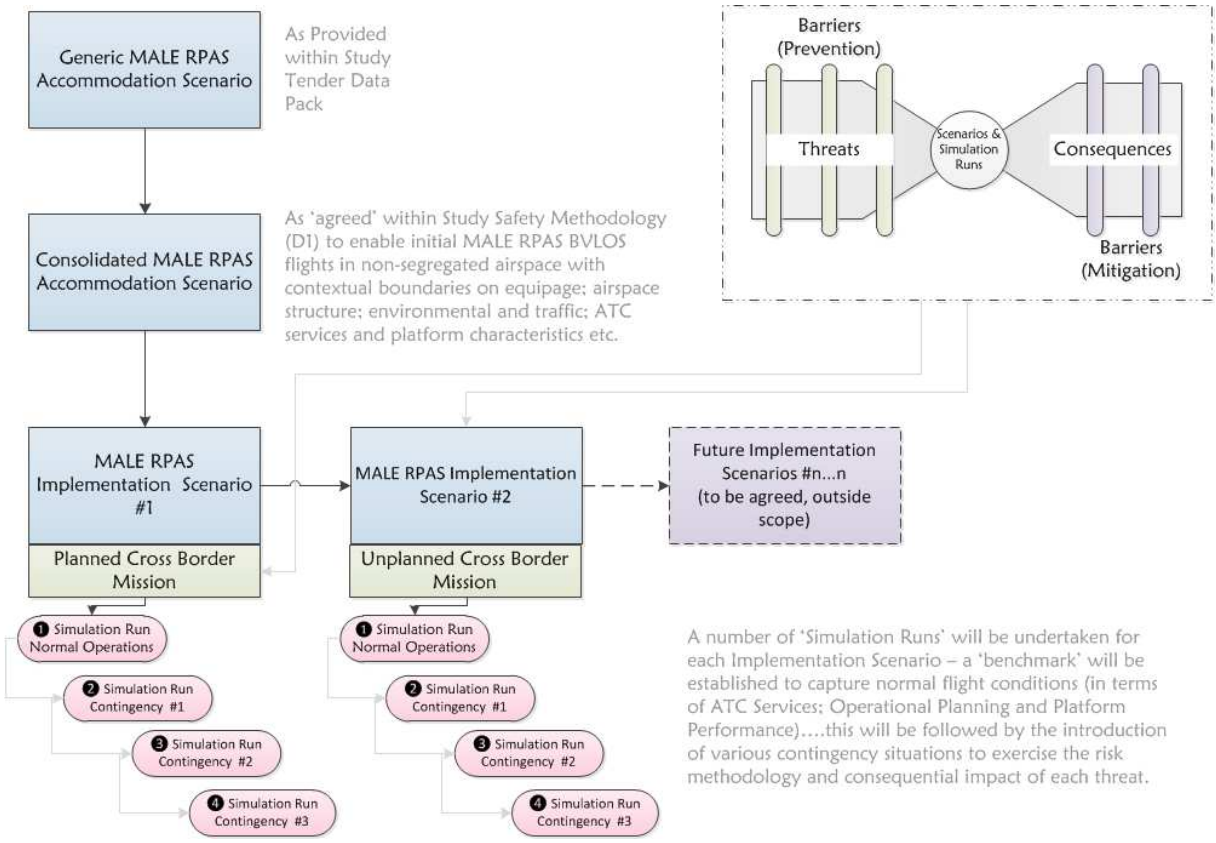


Figure 5 - Simulation Structure

3 Safety Case Assessment Consolidation

3.1 Introduction

The Safety Case Assessment methodology defined in Task 1 has been continually refined throughout the study through liaison with key stakeholders such as EDA and EUROCONTROL and through the assessment process underpinning the set-up of the Simulation Campaign. This section presents a consolidated view of the overall Air Systems Safety Case (ASSC) as described in task 1 to support the Implementation Scenario flights were they to be conducted in a real-world operating environment and not in a Synthetic Environment (SE).

The ASSC presented is in the form of a series of Safety 'Claims' backed-up by reasoned argument and, where possible, evidence to cover the broadest possible scope of the safety argument. This part exercises the assertion that the Safety Case Methodology provides sufficient rigor across all three principal elements of the holistic safety case.

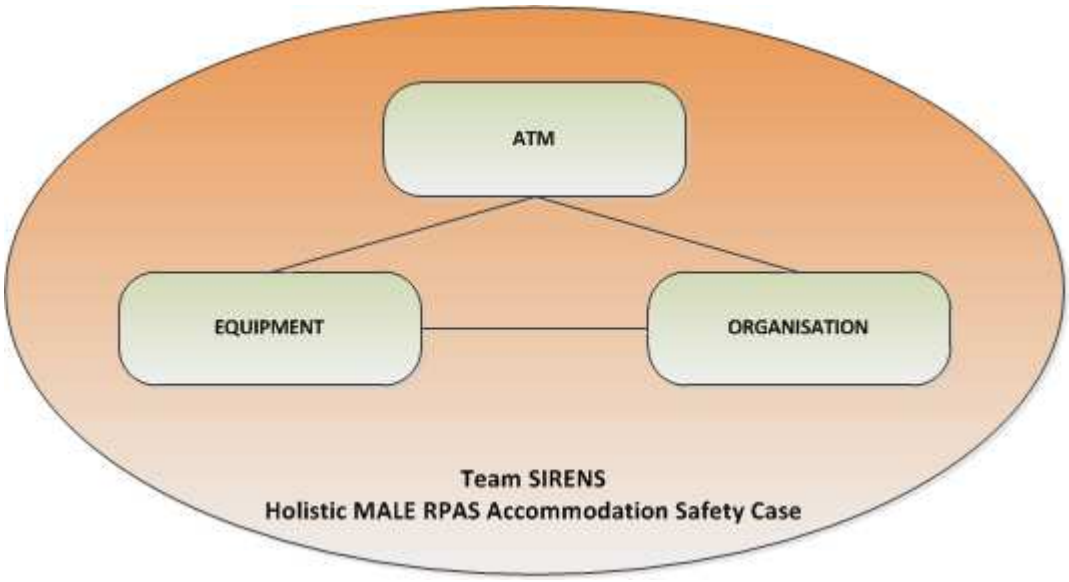


Figure 6 - Holistic Air Systems Safety Case

This treatment is then supplemented with a small number of 'deep dives' into the detail of how the methodology supports Risk Assessment and mitigation through a hierarchical set of Claim, Argument, Evidence (CAE) analyses culminating in the definition of a number of BowTies to illustrate the understanding and management of Risk to Life.

The following diagram (Figure 7) defines the terminology used throughout the 'Claim, Argument, Evidence' diagrams that follow.

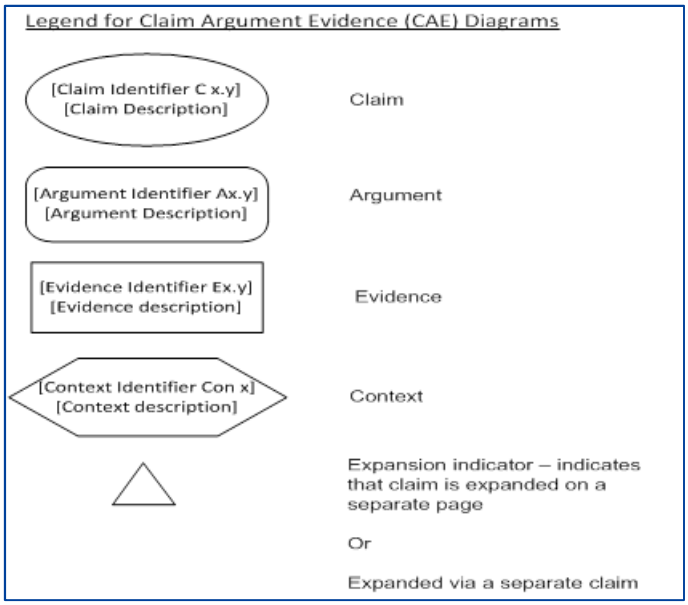


Figure 7 - Nomenclature for CAE Diagrams

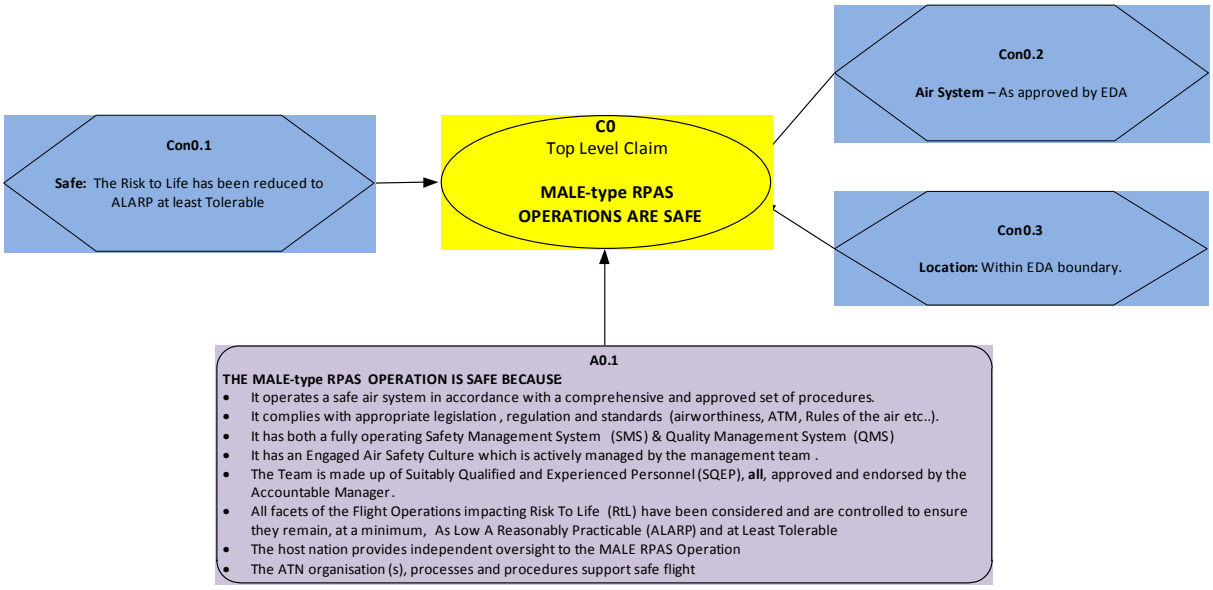


Figure 8 - Top Level Safety Case Claim

The top-level claim is that the planned MALE-type RPAS flight operations are safe because:

- The Risk to Life has been reduce to 'As Low As Reasonably Practicable (ALARP) and at least Tolerable ' by:
  - Ensuring the MALE-type RPAS 'Equipment' is safe
  - Ensuring that the MALE-type RPAS Operators are safe, and
  - Ensuring that the ATM organization, processes and procedures, support safe flight

Each of these sub-claims is hierarchically devolved to greater levels of detail ultimately captured using BowTie models. This has been expanded in Figure 9 and Figure 10 to show the Claim-

Argument-Evidence (CAE) Safety Case ds it develops. Figure 9 expands the Top level safety claim shown in Figure 8 to indicate how the structure will support the top-level safety claim. Figure 10 expands a specific element of the diagram further to illustrate how; typically the ATM evidence would be included in the umbrella of the Air System Safety Case (ASSC) safety artifacts.

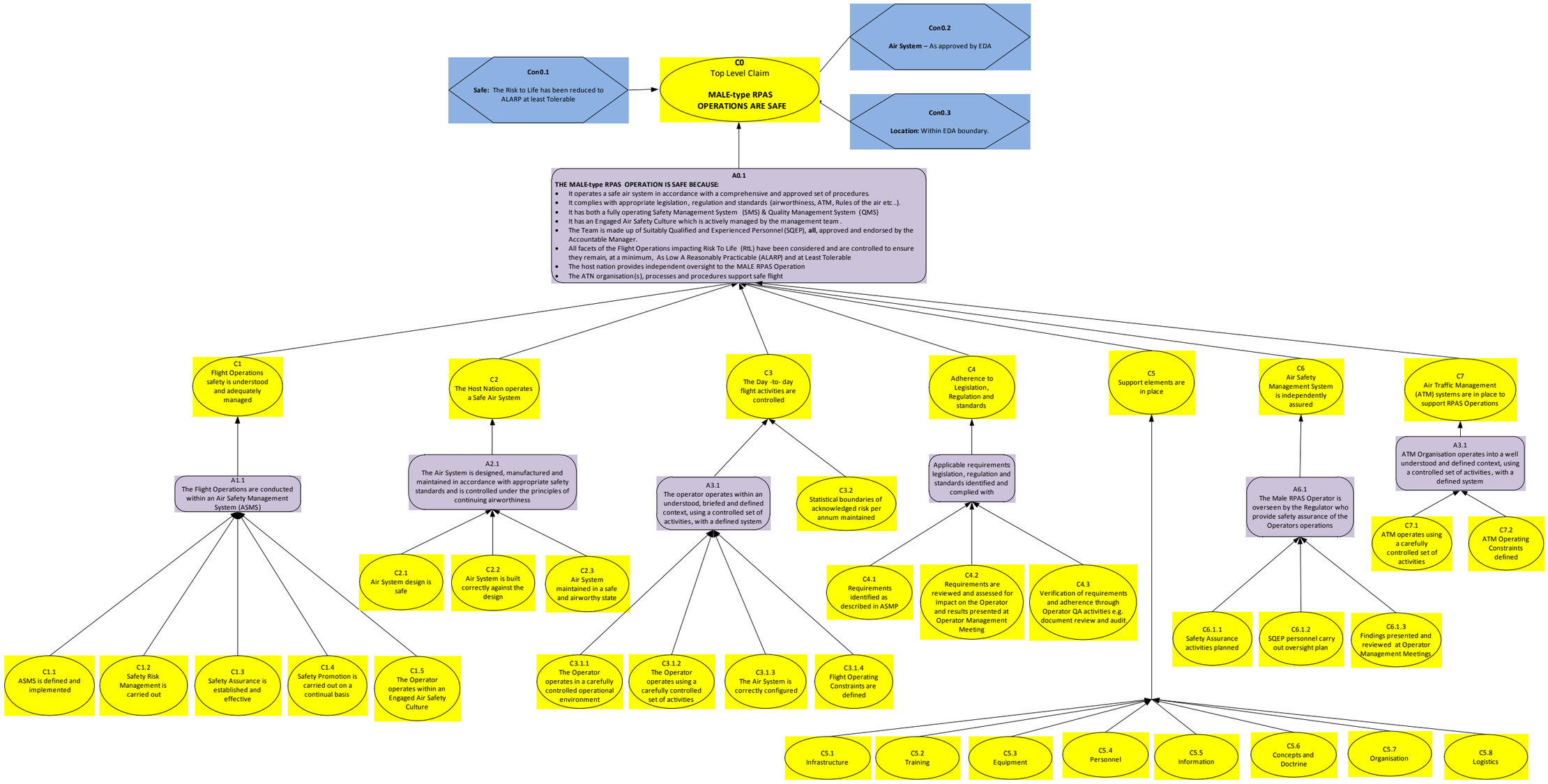


Figure 9 - Expanded Air Systems Safety Case

This page is intentionally left blank

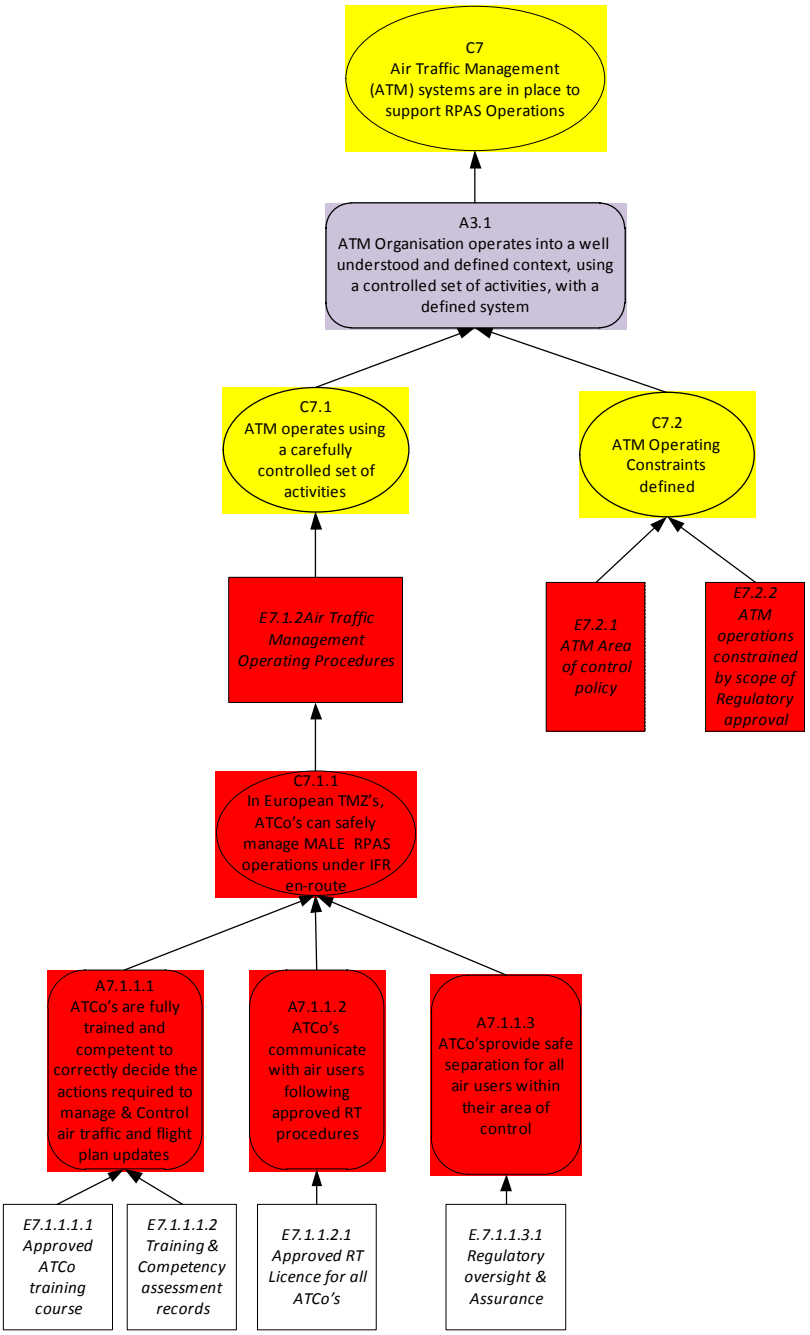


Figure 10 - Further Expansion to include ATM considerations

Whilst it was the intention to conduct a quantitative analysis within the BowTies it was not possible to give an accurate quantitative analysis due to the generic nature of the study. No specific MALE RPAS was used and assumptions over Human factors issues were not able to be sensitised to the platform and operating areas.

3.2 ATM Organisation & Separation Provision

To access controlled airspace pilots are required to obtain permission from Air Traffic Controllers (ATC) in the first instance, thereafter aircraft are mandated to follow ATC instructions - except in emergency situations. Furthermore and subject to submission and acceptance of an appropriate flight plan, aircraft will only be admitted into controlled airspace if they are equipped to a certain standard enabling controllers to provide separation assurance services and flight crews to maintain separation from other proximate aircraft and provide positional information to others.

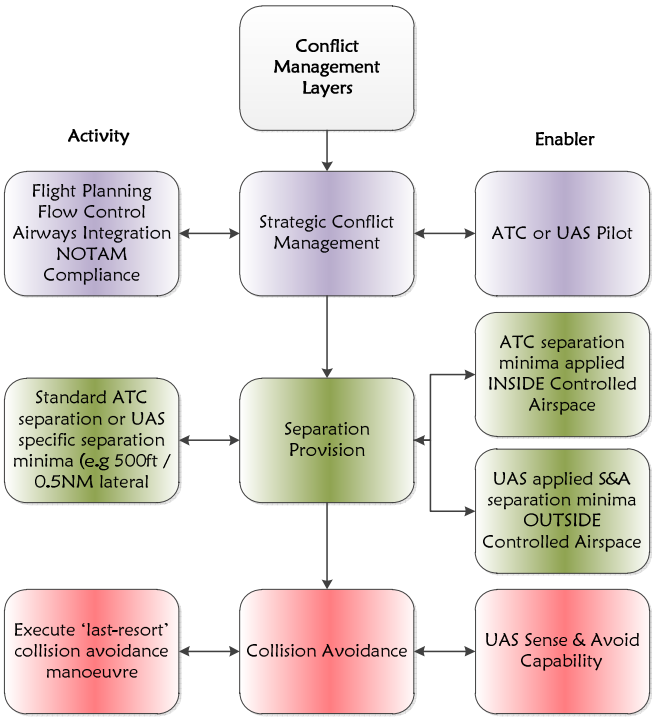


Figure 11 - ATC Provision of Separation

In general terms a layered approach is used to support conflict management requirements – this concept incorporates strategic flight planning; application of air traffic management services to achieve separation minima and also collision avoidance in situations where no ATC services are present or there has been a loss of separation for some reason.

The layered conflict management approach for RPAS is illustrated and highlights the need for RPAS pilots to ensure separation minima are maintained outside controlled airspace.

Future air traffic management concepts are largely based on a more flexible design use of airspace and 'free-flight' approaches enabling increased capacity, reduced congestion and environmental footprint. This may lead to additional requirements placed on RPAS operating in more complex traffic environments and future thinking exploring radical changes such as advocating delegation of the separation task to the pilot. This may lead to increased controller workload as well as additional equipage burdens in areas such as self-separation assurance systems as well as the ability to share ATM information with other stakeholders in accordance with SWIM (System Wide Information Management) principles.

3.3 Anatomy of a BowTie

3.3.1 Overview

Pictorially, a BowTie looks like the picture shown below.

Each identified 'Hazard', marked in rectangular yellow & black stripes is characterised by one or more 'Top Level Events (TLE)' marked in red & orange circles. Each TLE may be caused by one or more 'Threats' (blue rectangle) placed to the left and if the TLE occurs it may lead to one or more 'Consequences' (orange rectangle) placed to the right. Each 'Threat' may be prevented or each 'Consequence' mitigated by one or more 'Barriers' (green and white vertical rectangle) placed between the Threat and the TLE or between the TLE and the Consequence.

Threat barriers may also be dependent upon some other action or threat also known as an 'Escalation Factor' – these are shown in orange & white vertical rectangles. Similarly, each mitigation barrier may lead to a further 'Escalation Factor' or Consequence and these are shown in red and white vertical rectangles.

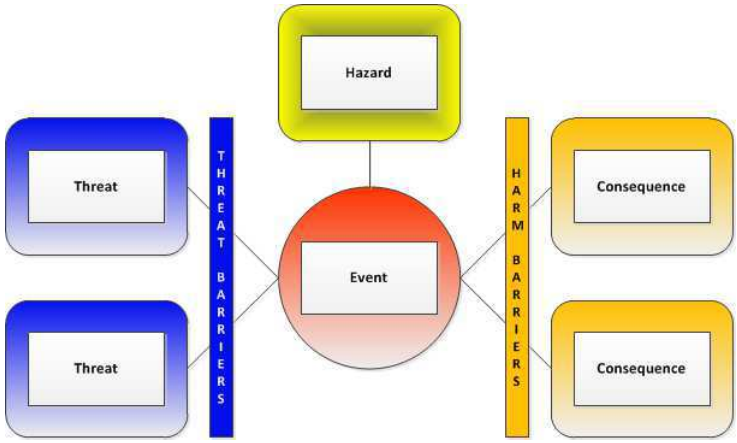


Figure 12 - Simple Bow Tie

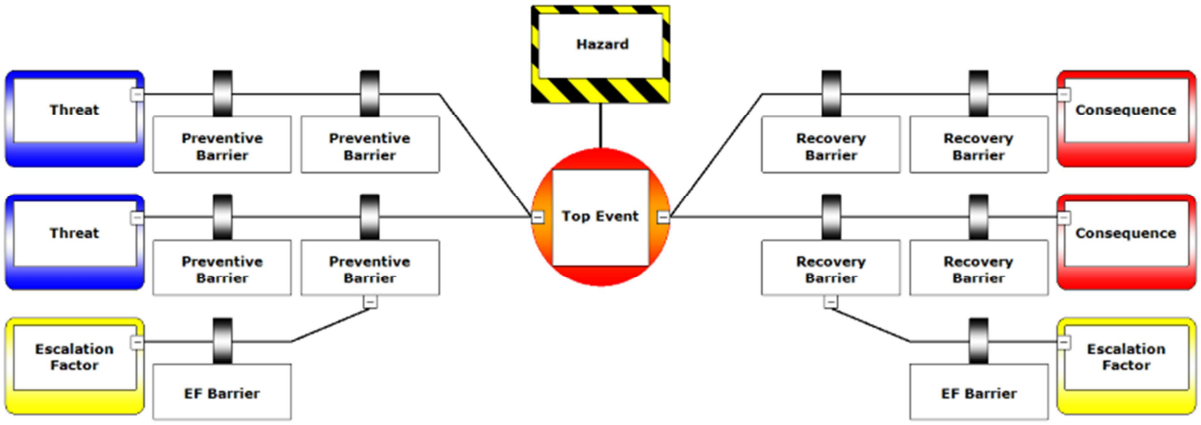


Figure 13 - Extended Bow Tie

3.3.2 Worked Example #1

To explain further how a BowTie should be read and used, we consider Hazard 'Air: Flying MALE RPAS' with the top event being 'Loss of Separation with Other Air Users (Mid Air Collision)'. This considers Injury/Fatality to 2nd & 3rd parties – Note: Passengers/crew on manned platform that may be involved in the MAC are considered as 2nd parties.

One of the threats to this TLE is Threat 005-5 which is the threat of the 'INS/GPS System Malfunction or loss of GPS signal' which could lead to a loss of separation with other air users and ultimately a Mid Air Collision.

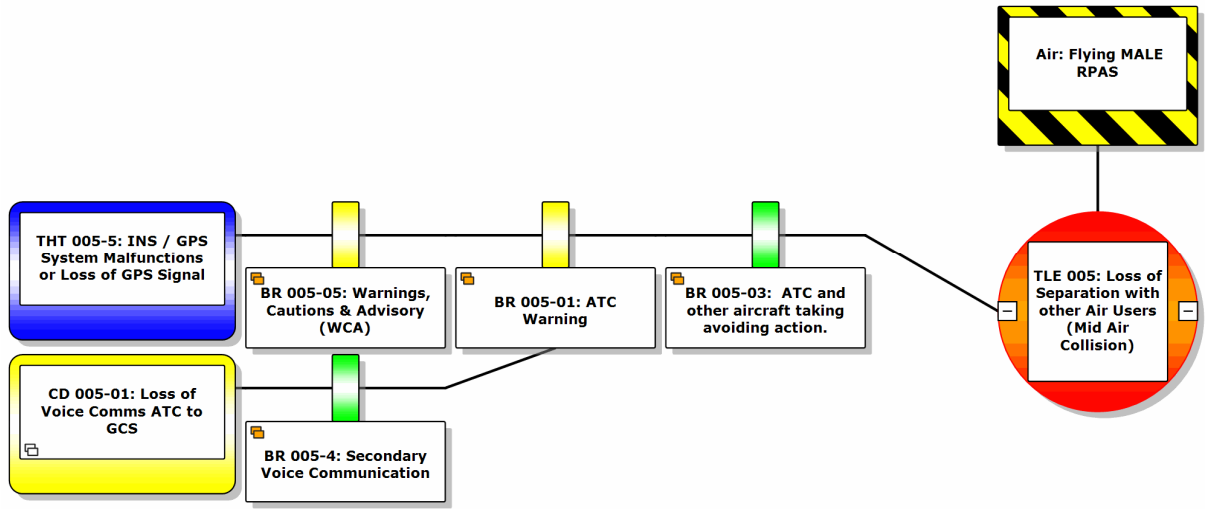


Figure 14 – Worked Example 1 (Threats)

Three barriers have been identified which could prevent this occurring:

a) BR 005-5: Failing to act appropriately to Warnings Cautions & Advisories (WCA). The WCA documentation is held in the Flight Reference Cards and the platform technical publications.
b) BR 005-01: ATC Warning of deviation from cleared track/position
c) BR 005-03: ATC & Other aircraft taking avoiding action. Includes ATC detection of potential collision and possibility of another aircraft taking avoiding action.

There are two 'risk to life' (RtL) consequences identified should this threat lead to the TLE:

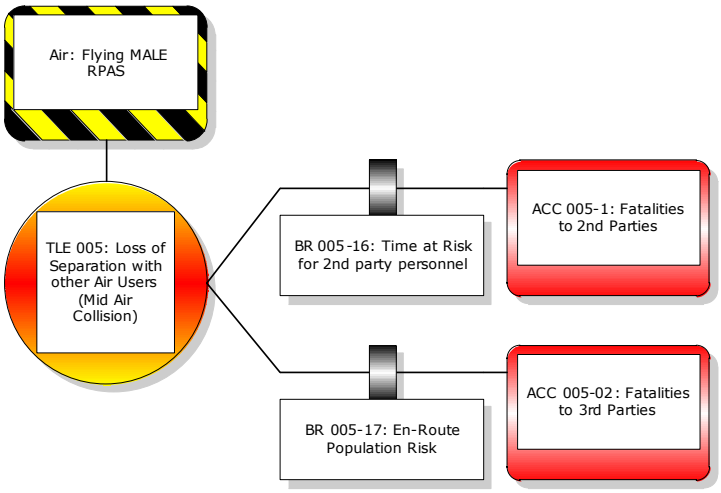


Figure 15 – Worked Example 1 (Consequences)

a) ACC 005-1 – Fatalities to 2nd party personnel – Mitigated by 'time at risk' based upon ATC reactions and maintenance of safe separation.
b) ACC 005-2 – Fatalities to 3rd parties – Mitigated by minimising flight over highly populated areas.

3.3.3 Worked Example #2

In our second example, we consider how Threat (THT) 005-2: Airspace Infringement – Pilot Error (outside cleared airspace) impacts the same top event ('Loss of Separation with Other Air Users (Mid Air Collision)'). The model is presented below.

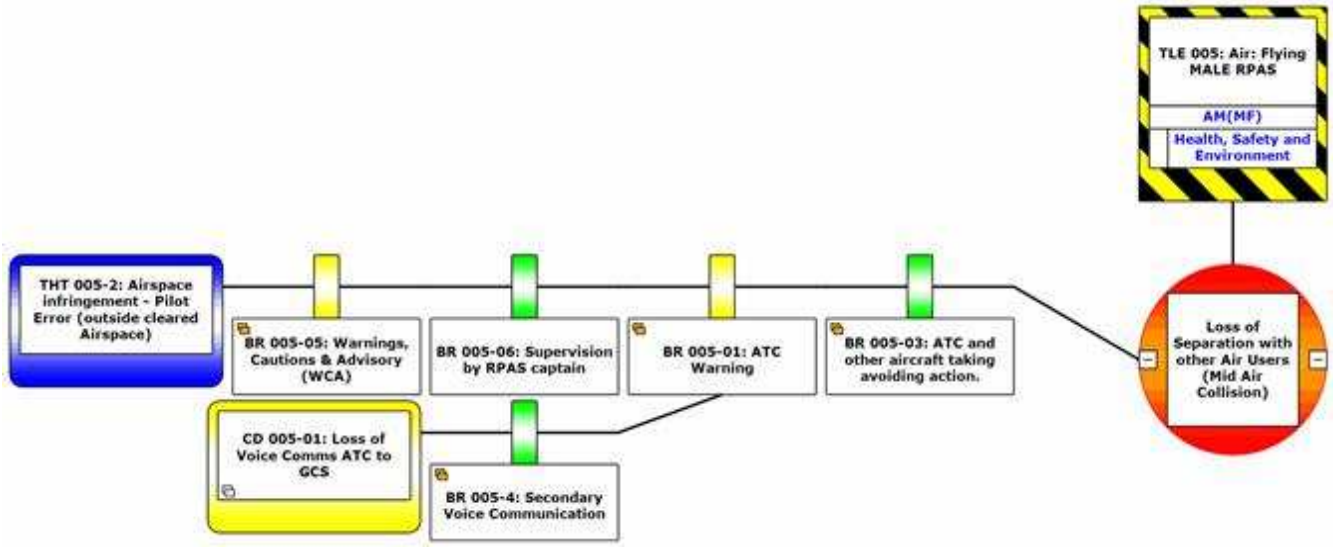


Figure 16 – Worked Example 2 (Threats)

There are four barriers identified to prevent this from occurring:

a) BR 005-05: Warnings, Cautions & Advisory (WCA) - Failing to act appropriately to WCAs. *The system will give notification if the aircraft is approaching segregated airspace. This is set-up by the crew through issuing a NOTAM. (This is equally applicable to the intruder/infringing aircraft).*
b) BR 005-06: Supervision by RPAS captain - GCS crew should notice flight outside airspace. *The system will give notification if the aircraft is approaching segregated airspace. This is set-up by the crew on initialisation of each GCS*
c) BR 005-01: ATC Warning - ATC warnings should/would be given regarding conflicting traffic and resolution course & speed
d) BR 005-03: ATC and other aircraft taking avoiding action - *includes ATC detection of aircraft incursion and ensuring the AV & Aircraft are kept separated to avoid potential collision and possibility of another aircraft taking avoiding action.*

There are three 'risk to life' (RtL) consequences identified should this threat lead to the TLE:

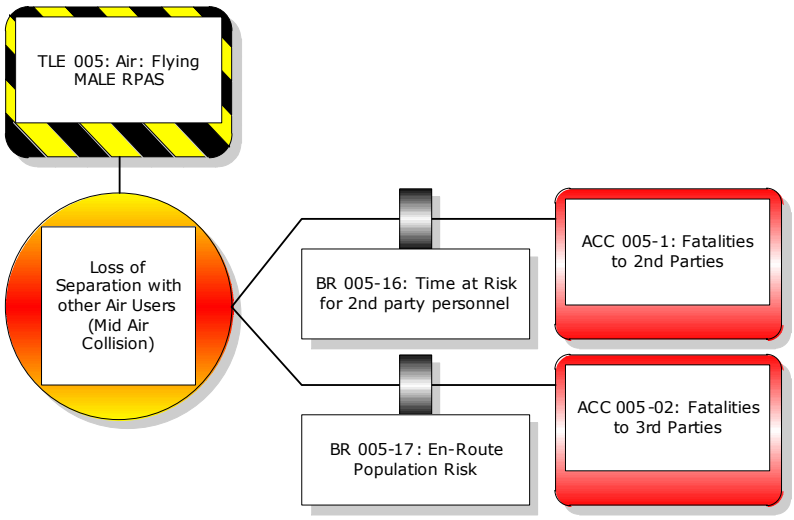


Figure 17 – Worked Example 2 (Consequences)

a) Fatalities to 1st parties – Mid-Air Collision with manned aviation
b) ACC 005-1: Fatalities to 2nd parties - Mid-Air Collision over the airfield where 2nd parties may be working. Mitigated by BR 005-16 Time at Risk for 2nd party personnel.
c) ACC 005-2: Fatalities to 3rd parties - Injuries to people on ground as a result of Mid-Air Collision. Mitigated by managing the en-route population risk – *avoiding high population densities if not necessary for mission completion.*

3.4 RPAS Accommodation Study BowTie Descriptions

In this section we analyse two of the BowTies in more detail in order to provide the reader with confidence in the application of the methodology and sufficient knowledge to understand the others.

3.4.1 Top Level Event: TLE 001 – Loss of Separation with Ground (During Emergency Recovery)

This BowTie is relevant to airborne operations only.

Hazard: Loss of separation with the ground (During Emergency Recovery) – This hazard relates to the potential of a crash following an in-flight emergency resulting in an Emergency Recovery procedure being invoked.

Threats:

THT 001-1: Engine Failing (Fault) – This Includes:

- Engine fire,
- Fuel starvation/blockage,
- AV Vehicular Management System command idle due to other system failures,
- Any other failure that leads to an engine stopping/lack of thrust

BR 001-1: Engine Monitoring - GCS crew monitor the engine performance throughout flight. This is done by:
- Monitoring fault indicators within the system (Warnings, Cautions & Advisories)
- Regular engine indication sweeps (typically every 15minutes) for any anomalies. Note: If pilot is alerted to problems early enough then it is possible to land before the engine fails.

BR 001-2: Live & Post Flight Data Analysis - Live flight data analysis by pilot or flight engineer identifying faults and trends during flight. Post flight data analysis to give early indication of developing faults/issues.

THT 001-2: Engine Failing (Low Fuel) - The cause is that there is not enough fuel due to either Pilot error, as there is not enough fuel to land, or lack of fuel due to a leak. Weather conditions are ignored in this threat.

BR 001-3: Supervision by RPAS Crew: This includes:
- Flight Planning (pre-flight & during-flight)
- FREDA checks – (Fuel, Radio, Engine, Direction Indicator, and Altimeter)
- WCA's Monitoring

BR 001-4: System Low Fuel Warning: The Vehicle Management System gives a warning of Minimum Fuel remaining.

THT 001-3: Engine Fail (Manual Engine Cut): Inappropriate use of the manual engine cut function.

BR 001-5: System Design (Manual Engine Cut Function): The Engine Cut switch is a guarded switch which prevents accidental selection of the engine cut.

BR 001-6: Engine Cut Procedures: Engine Cut procedures as detailed flight Reference Cards:
- Appropriate check & confirmation of system parameters.
- RPAS Captain approval to cut engine.

THT 001-4: Contaminated Fuel: AV refuelled with contaminated fuel.

BR 001-7: Ground Fuel checks: CAP 748 - Fuel checks

BR 001-1: Engine Monitoring: GCS crew monitor the engine performance throughout flight. This is done by:
- Monitoring fault indicators within the system (Warnings, Cautions & Advisories)
- Regular engine indication sweeps (typically every 15minutes) for any anomalies. Note: If the pilot is alerted to problems early enough then it is possible to land before the engine fails.

THT 001-5: Bird Strike: A bird strike is strictly defined as a collision between a bird and an aircraft which is in flight or on a take-off or landing roll. The term is often expanded to cover other wildlife strikes - with bats or ground animals.
90 % of Bird strikes occur in the vicinity of aerodromes (ICAO) during the Take-off and landing phase.

BR 001-8: BirdTAM: Bird Hazard Measures covered at 'out-brief' - information is gathered from an ANSP website along with NOTAMs.
BR 001-9: Airport Bird Control: Airport Bird Hazard control Measures i.e. Bird Scaring.
BR 001-13: **The likelihood of bird strike damaging the AV such that it becomes un-airworthy**: CAP673 (Aviation Safety Review) Ch. 14 Bird strikes - Provides evidence to support the frequency of reported bird strikes in UK aviation. Notably; 70% of Bird strikes occur below 500 Ft AGL and only 3% occur below 80Kts. Therefore this risk is most likely in and around the bounds of the airfield (Note: take-off climb is a 500ft/min).

THT 001-6: No-Comm with UAV and Autoland not set: UAV loses data-links and does not complete an automatic GTOL (**G**PS **T**ake-**o**ff & **L**anding) recovery to airfield due to Lost Link Procedure (LLP) settings. Autoland is normally selected in the LLP but may not be for short periods of flight during specific activities such as controllability checks.
Pilot error may also result in autoland being un-ticked.

BR 001-10: Design Failure Rate: Design safety case data should be used.
BR 001-11: Pre-Flight Maintenance activities: Maintenance activities carried out in accordance with approved maintenance data.
BR 001-12: Equipment reset (Data-Link): The Data Links can be reset and/or keys reloaded. Notwithstanding this, the RPA has the ability to carry out a 'no-Comm' landing - therefore if both data links are lost the AV will return to base

Consequence: ACC 001-1: Fatalities to 3rd Parties: UAV crashes at the Emergency Recovery Location (ERL).

BR 001-14: Glide Using UAV Battery: This is when there is an automatic recovery to an ERL. The battery gives minimum battery performance (in minutes - typically 40 mins) of power to control the basic flight control elements.
BR 001-15: Operation near/over Sea & Emergency Recovery Location (ERL) Population risk: Significant proportions of flights are over the sea. Standard ERPs are set to be over the sea in a safe area.

3.4.2 TLE 005 – Loss of Separation with other Air Users (Mid-Air Collision)

Hazard: Loss of Separation with other Air Users (Mid-Air Collision) – This hazard relates to a MALE Type-RPAS collision during flight perpetrated by either the RPAS or other Air user.

Threat: THT 005-1: Airspace Incursion by unauthorised aircraft - An aircraft that comes into the controlled airspace without permission/Clearance from the controlling ATC.

Barrier: BR 005-01: ATC Warning - Airspace area controllers monitor and control in, during transit and out of their allocated airspace.

Control Decay Mechanism: **CD 005-01: Loss of voice Comms ATC to GCS** – Primary Comms fails – Relying on Secondary & Tertiary comms.

BR 005-4: Secondary Voice Communications - Communications Plan to include revisionary modes – Both secondary and Tertiary.

BR 005-02: RPAS Pilot taking avoiding Action - Upon notification from the Air traffic control provider or if an aircraft is seen via the Electro Optic (EOP) device (Camera) then the RPAS pilot will initiate avoiding action.

BR 005-03: ATC & Other aircraft taking avoiding action - Includes ATC detection of aircraft incursion and ensuring the AV & Aircraft are kept separated to avoid potential collision and possibility of another aircraft taking avoiding action.

BR 005-04 to be inserted to cover RPAS Straying outside volume of cleared Airspace (or something similar)

THT 005-2: Airspace infringement - Pilot Error (outside cleared Airspace) - Human Error leading to Flight outside cleared & allocated Airspace.

BR 005-05: Warnings, Cautions & Advisory (WCA) - Failing to act appropriately to WCAs. The WCA documentation is held in the Flight Reference Cards (FRC's) and Technical Publications. The system will give notification if the aircraft is approaching a 'Stay out zone' this is set-up by the crew on initialisation and navigation set-up of each GCS. (Note this refers to Airspace and not Separation)

BR 005-6: Supervision by RPAS Captain - GCS crew should notice flight outside airspace.

Barrier: BR 005-01: ATC Warning - Airspace area controllers monitor and control in, during transit and out of their allocated airspace.

Control Decay Mechanism: **CD 005-01: Loss of voice Comms ATC to GCS** – Primary Comms fails – Relying on Secondary & Tertiary comms.

BR 005-4: Secondary Voice Communications - Communications Plan to include revisionary modes – Both secondary and Tertiary.

BR 005-03: ATC & Other aircraft taking avoiding action - Includes ATC detection of aircraft incursion and ensuring the AV & Aircraft are kept separated to avoid potential collision and possibility of another aircraft taking avoiding action.

THT 005-3: Pilot Error – Incorrect attitude - Pilot Error causing incorrect altitude/position entry.

BR 005-07: Altitude Checking – RPAS Captain would routinely supervise the P1/P2 during altitude transitions.

BR 005-08: Supervision by UAV P2 and/or UAC Cdr – Cooperative crew supervision.

BR 005-09: Flight Computer Flight Plan Validation – Ground Flight Control Computer checking of flight plan against airspace & terrain.

Barrier: BR 005-01: ATC Warning - Airspace area controllers monitor and control in, during transit and out of their allocated airspace.

Control Decay Mechanism: **CD 005-01: Loss of voice Comms ATC to GCS** – Primary Comms fails – Relying on Secondary & Tertiary comms.

BR 005-4: Secondary Voice Communications - Communications Plan to include revisionary modes – Both secondary and Tertiary.

BR 005-03: ATC & Other aircraft taking avoiding action - Includes ATC detection of aircraft incursion and ensuring the AV & Aircraft are kept separated to avoid potential collision and possibility of another aircraft taking avoiding action.

THT 005-4: Loss of Communications - This relates to either/both Primary & Secondary Comms failures.

BR 005-4: Secondary Voice Communications - Communications Plan to include revisionary modes – Both Secondary and Tertiary.

THT 005-5: INS/GPS system malfunction or loss of GPS Signal - Navigation system error produces unreliable position estimate.

BR 005-05: Warnings, Cautions & Advisory (WCA) - Failing to act appropriately to WCAs. The WCA documentation is held in the Flight Reference Cards (FRC's) and Technical Publications. The system will give notification if the aircraft is approaching a 'Stay out zone' this is set-up by the crew on initialisation and navigation set-up of each GCS.

Barrier: BR 005-01: ATC Warning - Airspace area controllers monitor and control in, during transit and out of their allocated airspace.

Control Decay Mechanism: **CD 005-01: Loss of voice Comms ATC to GCS** – Primary Comms fails – Relying on Secondary & Tertiary comms.

BR 005-4: Secondary Voice Communications - Communications Plan to include revisionary modes – Both secondary and Tertiary.

BR 005-03: ATC & Other aircraft taking avoiding action - Includes ATC detection of aircraft incursion and ensuring the AV & Aircraft are kept separated to avoid potential collision and possibility of another aircraft taking avoiding action.

THT 005-6: Pilot Incapacitation/GCS evacuation - Pilot/Flight crew incapacitation during the period of operation & GCS evacuation during flight.
Considerations:
1, There are a minimum of 2 pilots in the GCS for each flight. So if one pilot becomes incapacitated the 2nd pilot can take over or command the AV into a loiter. The Crew will be able to, via the Authoriser, bring another pilot into the crew to assist to recover the AV back to base.
2, If the incapacitation is due to smoke/fumes in the GCS and the crew are forced to evacuate then the AV should be put into a 'loiter' while a 2nd GCS is set-up to take over **or** a no-Comm landing is initiated.

BR 005-10: Aircrew medicals and fitness to fly – Aircrew (Pilots) are to be in date for annual medicals i.a.w. appropriate regulations. Flight Crews are responsible for declaring their fitness to fly prior to flight. During the Authorisation process the authoriser is satisfy him/herself to ensure that the crew is fit to conduct the briefed sortie. Nonetheless, if a crew member (pilot) should become incapacitated during flight the 2nd pilot will follow the FRC's to put the AV into a 'loiter' and then deal with the situation.

BR 005-11: Other GCS Crew Member available - Minimum GCS crew will be two pilots. Common cause incapacitation is very unlikely to be at the same time. Therefore second crew member should be able to follow the FRC's and put the aircraft into a 'loiter' and then deal with the crew situation.

BR 005-12: Active Monitoring & Action by ATC – It is often the norm for military flight that "ops normal" calls between the ATC & GCS Crew every 10-15 minutes are made as a matter of course.

BR 005-13: 2nd GCS (Standby) - 2nd GCS (Standby GCS) to be available in the event of an emergency.

CD 005-02: Availability of 2nd GCS Crew – SQEP crew availability to bring the 2nd GCS on-line. A minimum of 2, qualified, crew would be required to bring up the GCS ready to acquire the AV. Note: A GCS would take approximately 20 mins to bring up providing all goes well

BR 005-14: Flight Line Team able to 'bring-up' a 2nd GCS - Flight Line/Engineering Team able to 'bring-up' a 2nd GCS to the point of being able to attempt UAV acquisition and then handover to any available qualified aircrew to take control of the UAV.

CD 005-03: Availability of 2nd GCS - GCS must be able to support the build standard of the airborne AV. Generally there is more than one GCS at the required Operating build standard.

BR 005-15: Configuration of spare GCS - Following SQEP discussion it was considered that a GCS in the correct configuration ready to be powered would be available for 75% of flights. Therefore 25% of the flights an appropriate GCS would be unavailable

THT 005-7: Environmental conditions (Ice) – This threat relates to the UAV being inadvertently operated outside of MFTP/MPTF limits. Potentially the UAV behaviour differs from indication within the GCS

BR 005-16: Pre Flight/Flight Planning including Met Forecast considerations - Planning flights to operate within the Approved limits. Met forecast, delivered an approved Forecaster and used during the pre-flight planning phase. Flight Authoriser monitors Met conditions during flight and highlights any MET changes to the GCS crew. In particular if the Wind is within 20% of the allowable limit the Authoriser should monitor the wind from ATC and inform the GCS crew as required.

BR 005-05: Warnings, Cautions & Advisory (WCA) - Failing to act appropriately to WCAs. The WCA documentation is held in the Flight Reference Cards (FRC's) and Technical Publications. The system will give notification if the aircraft is approaching a 'Stay out zone' this is set-up by the crew on initialisation and navigation set-up of each GCS.

BR 005-03: ATC & Other aircraft taking avoiding action - Includes ATC detection of aircraft incursion and ensuring the AV & Aircraft are kept separated to avoid potential collision and possibility of another aircraft taking avoiding action.

THT 005-08: Environmental conditions (Wind) – This threat relates to the UAV being inadvertently operated outside of MFTP/MPTF limits. Potentially the UAV behaviour differs from indication within the GCS

BR 005-16: Pre Flight/Flight Planning including Met Forecast considerations - Planning flights to operate within the Approved limits. Met forecast, delivered an approved Forecaster and used during the pre-flight planning phase. Flight Authoriser monitors Met conditions during flight and highlights any MET changes to the GCS crew. In particular if the Wind is within 20% of the allowable limit the Authoriser should monitor the wind from ATC and inform the GCS crew as required.

BR 005-05: Warnings, Cautions & Advisory (WCA) - Failing to act appropriately to WCAs. The WCA documentation is held in the Flight Reference Cards (FRC's) and Technical Publications. The system will give notification if the aircraft is approaching a 'Stay out zone' this is set-up by the crew on initialisation and navigation set-up of each GCS.

BR 005-03: ATC & Other aircraft taking avoiding action - Includes ATC detection of aircraft incursion and ensuring the AV & Aircraft are kept separated to avoid potential collision and possibility of another aircraft taking avoiding action.

THT 005-9: Loss of IFF – Visibility & Identification to ATC and other air users is significantly impacted by the loss of IFF.

BR 005-17: ATC communications with RPAS crew - ATC will call GCS crew to provide regular updates of current position and provide controlling vectors as appropriate.

BR 005-18: ATC - Increased separation with other air users – ATC providing instructions to other air users to be aware and to Increase separation appropriately.

BR 005-19: RPAS Crew initiates loss of IFF procedures –
- Switch IFF on/off
- Identify current position to ATC
- Identify speed/altitude/heading
- Pass intentions
- RTB

THT 005 –10: Non-compliance or incorrect response with ATC separation instructions – ATC Instructions not complied with correctly.

BR 005-20: Pilot confirmation/read-back of ATC instructions – SOP's for pilot read-back and thus confirmation of ATC instructions.

Barrier: BR 005-01: ATC Warning - Airspace area controllers monitor and control in, during transit and out of their allocated airspace.

Control Decay Mechanism: **CD 005-01: Loss of voice Comms ATC to GCS** – Primary Comms fails – Relying on Secondary & Tertiary comms.

BR 005-4: Secondary Voice Communications - Communications Plan to include revisionary modes – Both secondary and Tertiary.

BR 005-21: Pilot Mayday call – Pilot has a problem which requires a Mayday call to be made.

THT 005-11: Incorrect information from ATC – Confusing/incorrect information from ATC

BR 005-20: Pilot confirmation/read-back of ATC instructions – SOP's for pilot read-back and thus confirmation of ATC instructions.

BR 005-22: Warnings from other Air Users – Other Air users monitoring the ATC frequencies and identifying issues and giving warnings.

Consequences: ACC 005-01: Fatality to 1st parties - AV hits manned platform potentially with passengers.

BR 005-22: Avoiding action being taken – Action taken to avoid the Mid-Air Collision.

ACC 005-02: Fatalities to 2nd Parties - Mid-Air Collision over the airfield where 2nd parties may be working.

BR 005-23: Time at Risk for 2nd party personnel - This relates to the time at risk to the 2nd parties when the AV is within the bounds of the airfield.

ACC 005-3: Fatalities to 3rd Parties – Injuries, resulting in fatalities, to people on ground as a result of Mid-Air Collision

BR 005-24: En-Route Population Risk – Where possible Flight planning will plan routes to avoid areas of high population density.

3.5 Air Systems Safety Case Linkages to Simulation Runs

The complete set of BowTies produced for the study, are detailed in Annex B. The BowTies have been considered as risks against accommodating MALE-type RPAS into controlled airspace and the following shows how and where critical elements have been linked to the simulation scenarios and simulation runs to enable verification exercises to be undertaken.

Table 1 – TLE & Threat to Scenario Mapping

#	TLE	THREATS	DESCRIPTION
001	Loss of separation with ground (during emergency recovery)	1. Engine failure (fault) 2. Engine failure (low fuel) 3. Engine failure (manual engine cut) 4. Contaminated fuel 5. Bird strike 6. No communications with UAV and Auto-land not set	Catastrophic equipment failure – not simulated as part of MALE RPAS Accommodation exercises
002	Loss of separation with ground (unintentional CFIT[3])	1. Pilot error – Incorrect altitude 2. Corruption of Speed & Altimetry Information	Catastrophic equipment failure – not simulated as part of MALE RPAS Accommodation exercises
003	Loss of separation with Ground (uncontrolled descent)	1. Environmental conditions out of limits 2. Vehicle Management System computer failure 3. UAV flight system control	Catastrophic equipment failure – not simulated as part of MALE RPAS Accommodation exercises

[3] Controlled Flight into Terrain

#	TLE	THREATS	DESCRIPTION
		failure 4. Structural failure (RPAS) 5. UAV fire 6. Manual engine cut during take-off, route &/or landing phases of flight	
004	Debris falling from UAV in flight	1. Loose panels 2. Structural failure leading to detachment of panels/structure 3. Ice shed from UAV	Not simulated as the simulation focus was on UAV pilot / ATC interaction
005	Loss of separation with other Air users (mid-air collision)	1. Airspace incursion by unauthorised aircraft 2. Airspace infringement – Pilot error 3. Pilot error – incorrect altitude 4. Loss of communications 5. INS/GPS System malfunction of loss of GPS signal 6. Pilot incapacitation/GCS evacuation 7. Environmental conditions (Ice) 8. Environmental conditions (Wind) 9. Loss of IFF 10. Non-compliance or incorrect response with ATC separation instructions 11. Incorrect information from ATC	Scenario 7 Scenario 8 Scenario 9 Scenario 10 Scenario 11
006	No communications due to irrecoverable loss of data link/Sat Comms	1. Technical failure of GCS 2. Failure of both data links/Sat Comm (ground) 3. Failure of both data links/Sat Comm (air) 4. Pilot Error 5. Loss of GCS electrical power 6. Electromagnetic interference 7. Shutdown of GCS due to fire or fumes 8. Loss of power to GDTS 9. Loss of GCS/GDT connection	Scenario 2 Scenario 4 Scenario 5 Scenario 9

Table 2 – Scenario to Simulation Run Mapping

SCENARIO	RUN	DESCRIPTION	EXPECTATIONS
1	1 & 5	Benchmark MALE-type RPAS flight without TLE	This scenario was designed to give all participants[4] some insight to the accommodation of a MALE-type RPAS in controlled airspace under 'normal' ATC, in order to create a 'baseline' system from which the issues encountered in the remaining simulations runs could be assessed and the behaviours of the participants judged.
2	3 & 11	R/T voice communication failure on return while in UK airspace	This scenarios was designed to exercise the ATCOs to safely return the RPAS to its home airport dealing with failed voice communications and the negotiation of a border-crossing leading to ATCO hand-over
3	2	Re-routing in-flight due to change of mission objective	This scenario was designed to exercise the participants with a change of mission mid-flight
4	6	Diverting manned aircraft & single C2 link failure	This scenario was designed to exercise the ATCOs to de-conflict (i.e. maintain separation) between a manned aircraft and a MALE-type RPAS and was made more challenging for the ATCOs by introducing a C2 data link failure
5	4 & 12	Diverting manned aircraft and single C2 link failure & poor quality of R/T voice communication	This scenario was designed to build on scenario 4 and make life even more difficult for the participants by reducing the quality of the voice communications between them
6	Not Simulated	RPAS unsafe landing gear indication	This scenario was designed to challenge the participants with a serious (potentially catastrophic) equipment failure prior to landing

[4] RPAS pilot(s) and ATCOs

SCENARIO	RUN	DESCRIPTION	EXPECTATIONS
7	7 & 10	Impact of slow RPAS speed – loss of horizontal separation)	This scenario was designed to challenge the ATCOs to maintain separation between the (relatively) slow-moving RPAS and a faster manned aircraft overtaking and climbing past the RPAS
8	7	Loss of vertical separation (because of emergency descent of a higher aircraft)	This scenario was designed to challenge the participants to maintain separation in an emergency situation
9	8 & 9	Two MALE-type RPAS (with simultaneous R/T voice communications failure in UK airspace)	This scenario was designed to challenge the participants by flying two MALE-type RPAS and investigate the issues and solutions generated when voice communications is lost between the ATCOs and the RPAS pilot(s)
10	3 & 11	Transponder failure	This scenario was designed to challenge the participants with an RPAS transponder failure whereby the ATCO workload increases in line with a requirement to ensure other air users are kept informed of the RPAS position and flight vector by verbal communications
11	4 & 12	Navigation System failure	This scenario was designed to challenge the participants with an RPAS transponder failure whereby the ATCO workload increases in line with a requirement to ensure other air users are kept informed of the RPAS position and flight vector by verbal communications. The RPAS pilot is reliant on the ATCO for a navigation solution sufficient to ensure a safe return to base

Notes:

Scenario 1 was developed as the baseline scenario to benchmark ‘normal operations’ in which no hazards were encountered.

Scenario 3 was developed to investigate participant behaviours and workload if the mission was changed mid-flight, it was not designed to support the analysis of a TLE.

Scenario 6 was developed as part of the study but was not simulated because the main thrust of the simulation campaign was to exercise the interaction between the RPAS Pilot and ATM, the scenario may be used (along with others) to support future experimentation campaigns.

4 Simulation Campaign Analysis

This chapter provides an overview of the simulation campaign and details the results achieved from questionnaires and discussions with the participants.

4.1 Introduction

The simulation campaign has been set up to evaluate the Safety Analysis Method as developed by team SIRENS and described in D1 – ***"Task 1 - General Approach and Safety Assessment Method Definition"*** [Ref. 27]. Details of the scenarios used and the evaluation method are described in D2 ***"Task 2 – Simulation Readiness Report"*** [Ref.28], and the schema showing the connection between the developed MALE-type RPAS accommodation scenario, the simulation runs and the safety case methodology is also shown in D2 at Figure 5.

The simulations have been performed, using the NARSIM (NLR ATC Research Simulator); a real-time man-in-the-loop simulation facilities, connected to MUST (Multi UAS Supervision Testbed); a generic RPAS ground control station.

Figure 18 - NARSIM in use for SIRENS simulations

Figure 19 - MUST in use for SIRENS simulations

Simulations have been set up to enable evaluation of the Safety Assessment Method, as described in D2 [Ref. 28]. Figure 20 illustrates the flight profile for the simulations. The flight profile for the return flight follows these steps inversely.

The following flight phases can be identified:

- Take-off from an aerodrome, under civil ATC in segregated airspace;
- Standard IFR Departure under the control of ATC;
- Climb in the CTR;
- Transit/cruise in Class A, B or C airspace, under civil ATC;
- Transit into the mission operations area, in segregated airspace, under civil ATC.

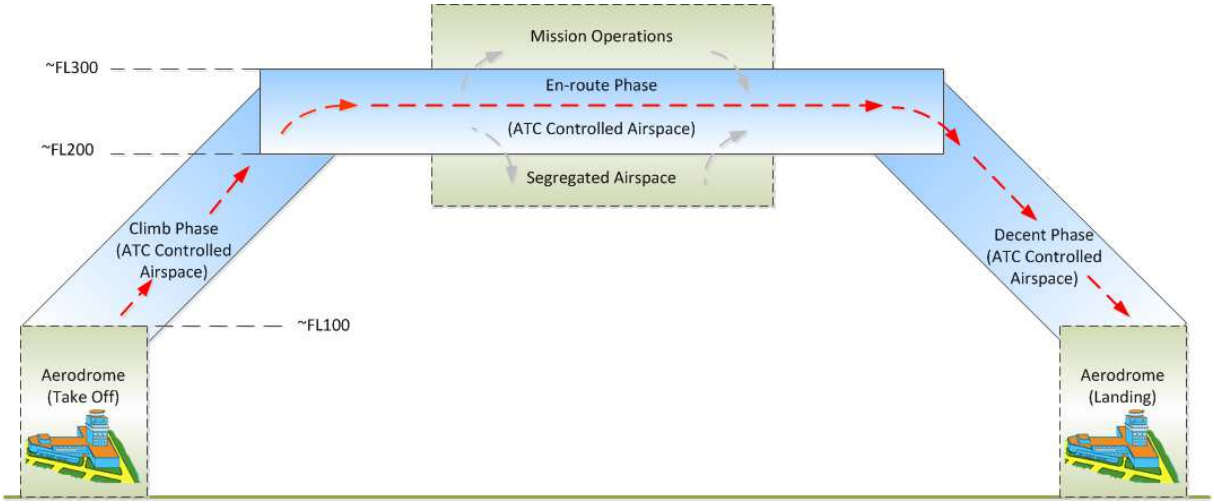


Figure 20 - Flight profile for the RPAS simulation

This flight profile assumes that the MALE RPAS only flies in normal airspace where ATC is responsible for separation assurance from all other VFR (Visual Flight Rules) and IFR (Instrument Flight Rules) traffic.

Furthermore, the project addressed normal cross-border operations, something that has not yet been explored in earlier RPAS projects. The cross-border operations in civil airspace concern missions that take place in the airspace of different European countries, where the RPAS is sequentially under control of the respective ATC-organisations and is crossing the border through a hand-over procedure at some moment during flight. The flights took place in the FIRs (Flight Information Regions) of The Netherlands (Amsterdam FIR) and that of the United Kingdom (London FIR); airways are indicated in the figures below.

Figure 21 - Airways in the London FIR

Figure 22 - Airways in the Amsterdam FIR

The Simulation runs were performed on 16th, 17th and 24th of July 2018, using NARSIM and MUST (see Figure 18 and Figure 19). In each simulation, two air traffic controllers, one MALE RPAS pilot and three pseudo pilots (for other, interfering, traffic) participated. Furthermore, each controller and the ground control station pilot was accompanied by an observer from team SIRENS. After each session, the air traffic controllers filled out a questionnaire on the specific events that occurred in the session. All participants then participated in detailed discussions to further evaluate the event and to consider suggestions on how to best deal with a number of specific events and particular situations. The suggestions have been recorded and will be discussed in the remainder of this chapter.

4.2 Qualitative Observations

A total of seven events have been evaluated during the simulation runs. Some events have been simulated several times, where the controllers switched positions to ensure that all controllers that participated in the simulations were faced with different situations each time. The specific events evaluated were:

- R/T (Radio Telephone) communications failure
- Loss of horizontal separation
- Two RPAS with simultaneous communications failure
- Navigation System Failure
- Single C2 (Command and Control) failure
- Loss of vertical separation
- Transponder failure

This section will further motivate the choice for these events and describe the general observations form the observers from team SIRENS and the high level results from the discussions with all

participants (air traffic controllers, ground control station pilot, pseudo pilots and observers). It can be seen that some of the events have been combined in one simulation run; the respective sections will only describe one event and refer to the other section for explanation of the remainder of the simulation run.

4.2.1 R/T Comm failure

An R/T failure leads to not being able to establish contact between the controller and pilot through VHF (Very High Frequency) radio. The contingency is to set up contact by phone. The flight performed is indicated in Figure 23 below.

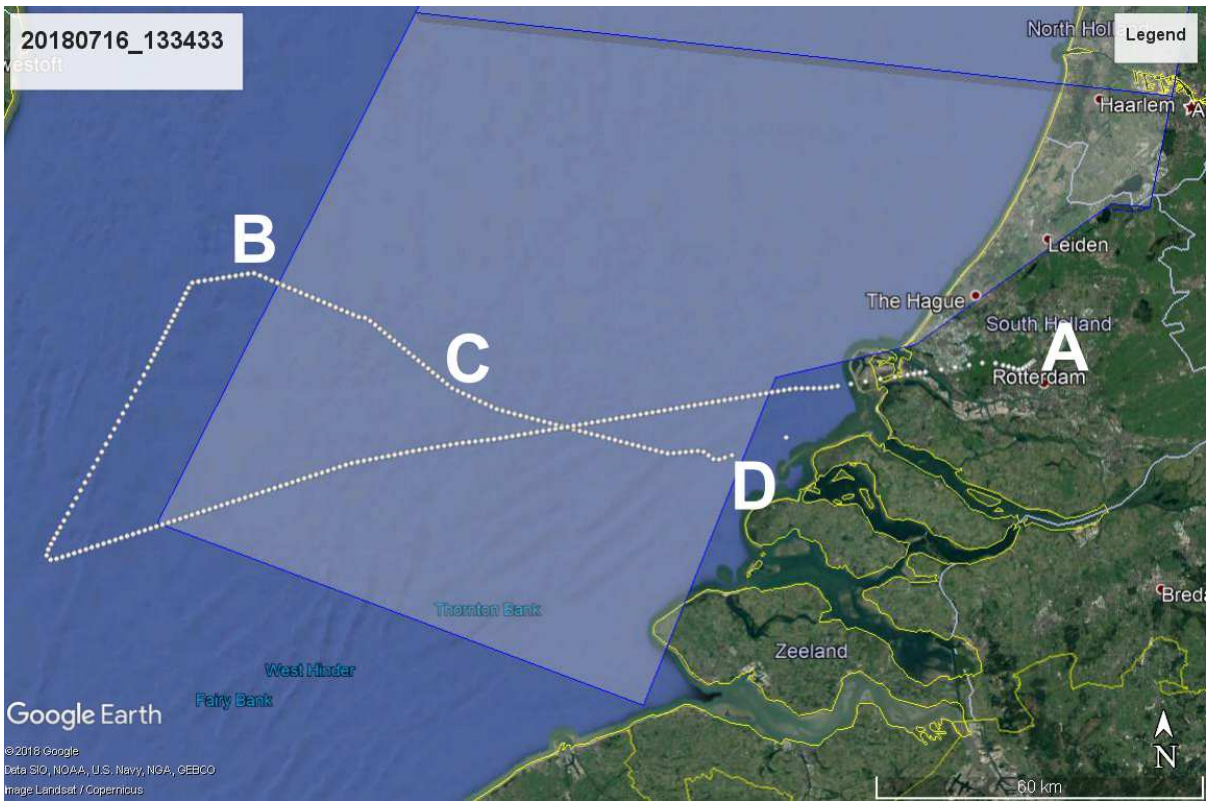


Figure 23 – Simulation Flight Path (R/T Comm Failure)

Point A: Start of simulation
Point B: R/T communication fails
Point C: Transponder fails (see other scenario)
Point D: End of simulation

Observations:

- RPAS will automatically switch to squawk 7600
- Air traffic controller remembers last clearance and will assume the RPAS will continue on this clearance
- The controller will normally ask his assistant to take over the actions for the RPAS

- A good phone procedure is necessary, e.g. to define who will initiate contact between controller and pilot
- A good phone strategy is necessary to defined where to find the appropriate phone numbers (probably, there will be a need to define this in the flight plan)
- At first contact by phone: confirm last clearance and ask for intentions

4.2.2 Loss of horizontal separation

The loss of horizontal separation has been simulated through an overtaking aircraft that is handed over from the APP-sector too early. The simulated ACC-sector needed to solve the issue. The flight performed is indicated in Figure 24 below.

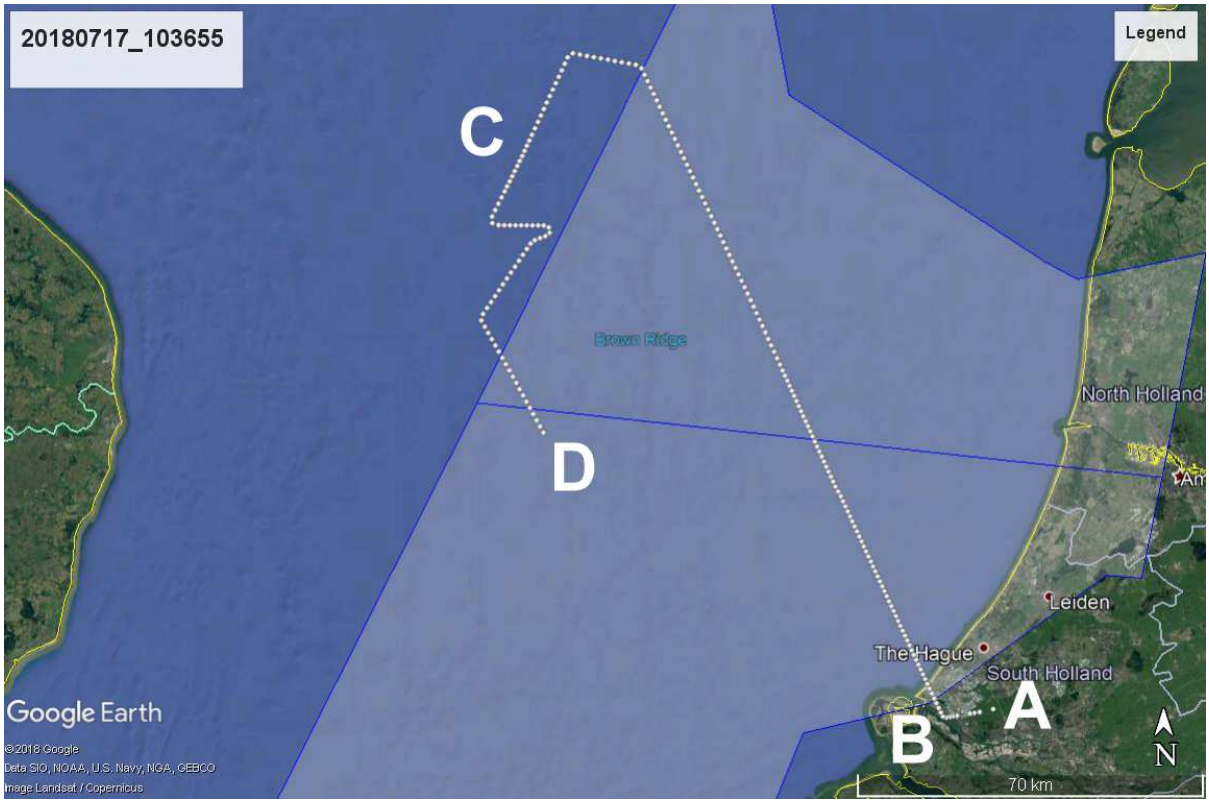


Figure 24 - Simulation Flight Path (Loss of horizontal separation))

Point A: Start of simulation
Point B: Imminent loss of horizontal separation
Point C: Emergency descent of another aircraft (see other scenario)
Point D: End of simulation

Observations:

- Controllers do not consider this a major problem (“it’s my job”)
- In case of another simultaneous emergency, a larger problem may arise
- In case of another error, e.g. from the pilot, a larger problem may arise

4.2.3 Two RPAS with simultaneous R/T communication failure

Two RPAS will both be experiencing an R/T comm failure simultaneously. The controller will need to open two phone lines (thus doubling the effort to establish communications and to check clearances and intentions). The flight performed is indicated in Figure 25 below.

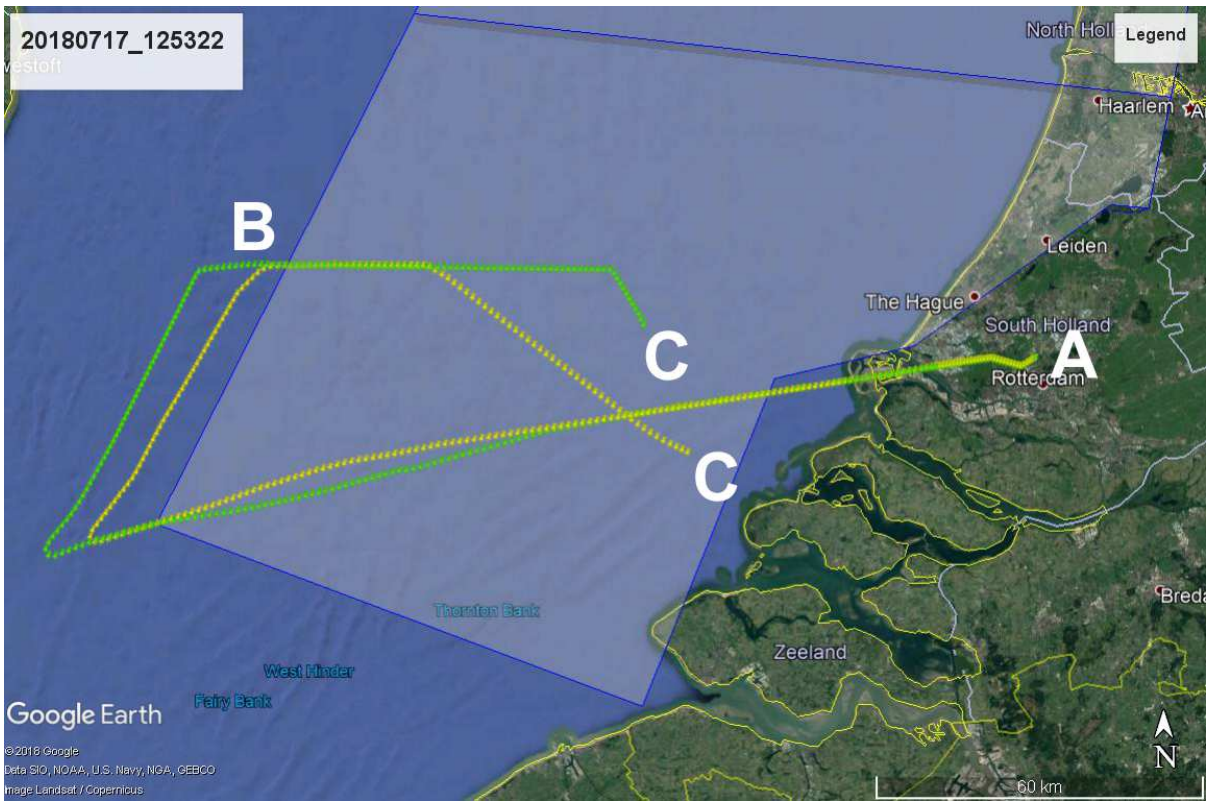


Figure 25 - Simulation Flight Path (Two RPAS with simultaneous R/T communication failure)

Point A: Start of simulation
Point B: R/T communication of both RPAS fails
Point C: End of simulation

Observations (apart from those already mentioned with the single R/T comm failure):

- When the two RPAS are operated as a formation flight of two RPAS, the controller may link both flights (if they are flying in the same area), thus giving instructions to the first and asking the second to follow. This will make it possible to give just one clearance for both aircraft simultaneously
- Two open phone lines will require additional attention, because of the switch necessary

4.2.4 Navigation system failure

A GNSS (Global Navigation Satellite System) failure cause the drone to lose own navigation. It will need to receive vectors from the controller in order to continue its course. The flight performed is indicated in Figure 26 below.

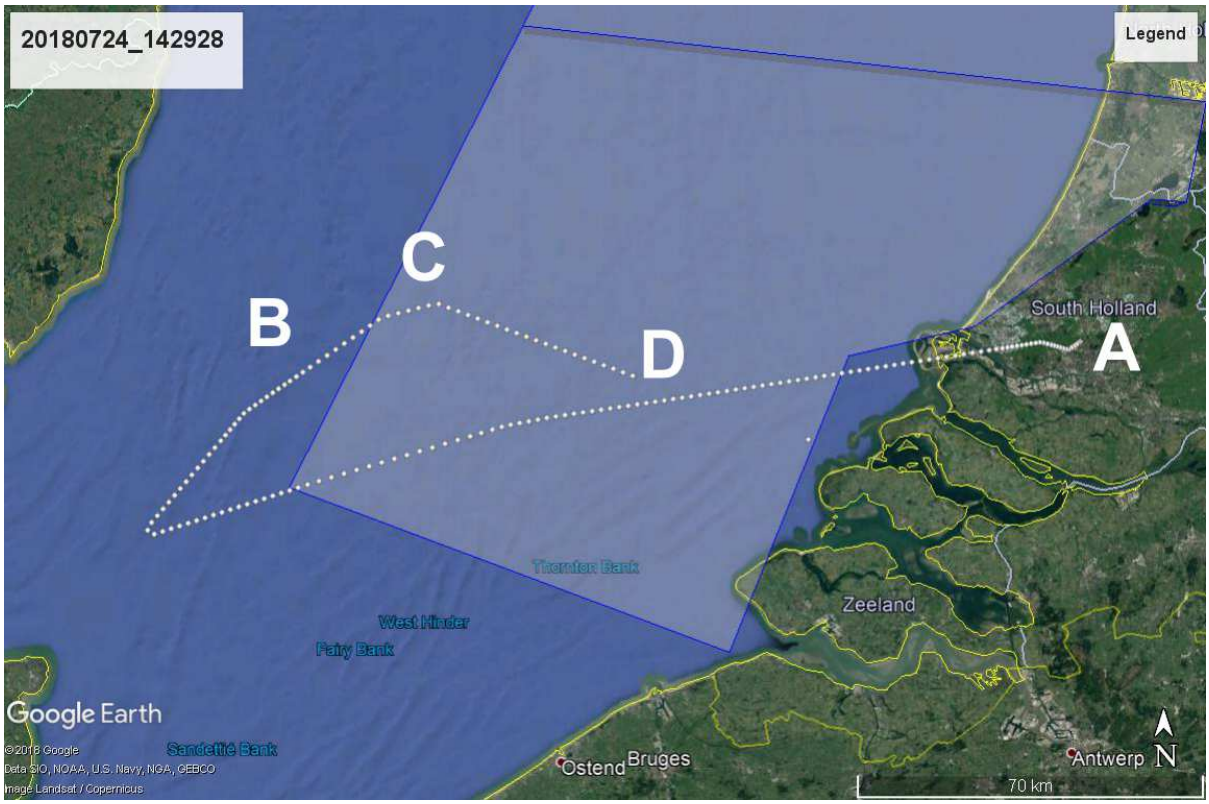


Figure 26 - Simulation Flight Path (Navigation System failure)

Point A: Start of simulation
Point B: Single C2 link fails + begin of poor R/T reception (see other scenario)
Point C: GNSS fails
Point D: End of simulation

Observations:

- Controller asks GCS pilot several questions to find out what is still possible concerning navigation ("can you fly towards a waypoint (answer = no)" and "are you able to determine your heading (answer is yes))
- Controller asks about the effect on the performance of the RPAS
- Other traffic in the vicinity is informed about the problem with the drone
- Amsterdam ACC has usually several aircraft flying vectors; one other aircraft to do so is no problem.

4.2.5 Single C2 failure

ICAO has determined that the command and control datalink is made of two independent datalinks, one being redundant (i.e. a back-up) to the primary link – thus the term 'single C2 link failure' means losing either the main data-link or the back-up. One single C2 failure occurs, which will require the

aircraft to return home. This will avoid a larger problem if the only one remaining C2-line gets lost as well. The flight performed is indicated in Figure 27 below.

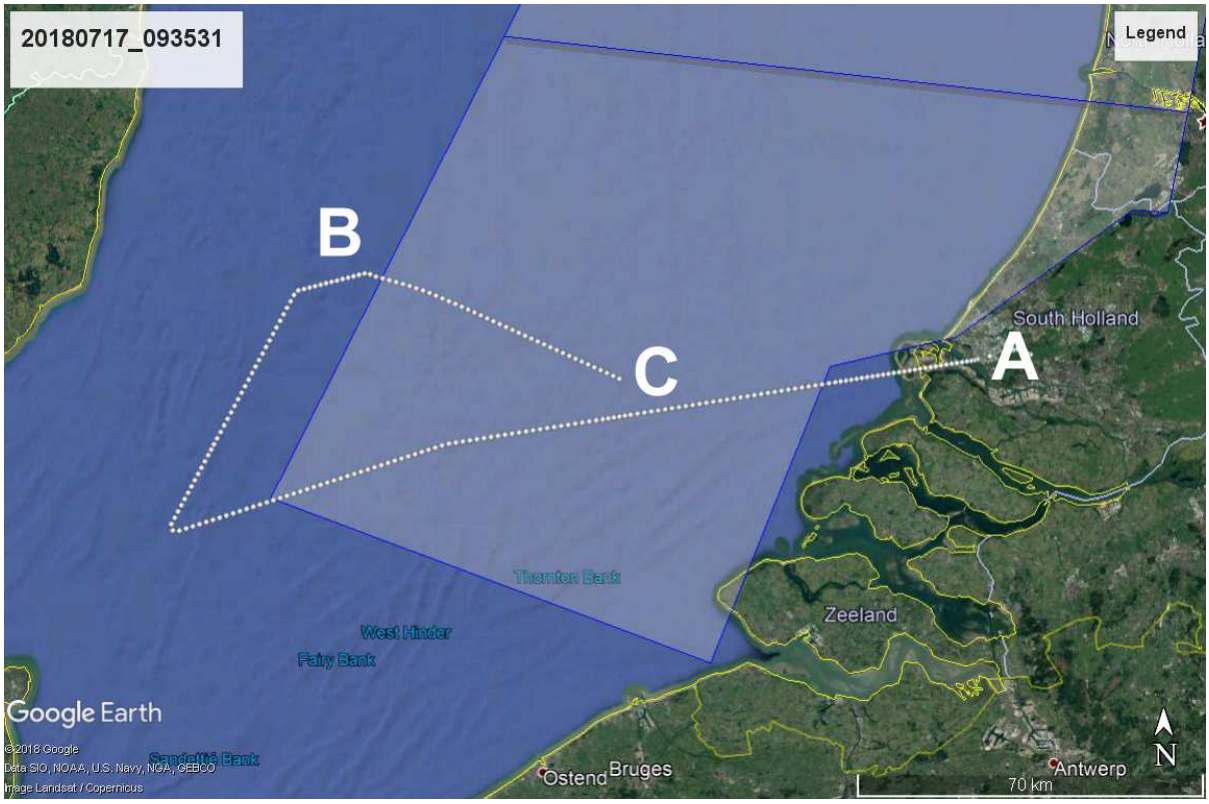


Figure 27 - Simulation Flight Path (Single C2 failure)

Point A: Start of simulation
Point B: Single C2 link fails
Point C: End of simulation

Observations (observations from a similar event see previous section, have been included):

- Controllers handled the RPAS to land as soon as practicable
- Neither controllers nor GCS pilot considered the situation an emergency
- Call on the lost C2-comm was considered as “information on”

4.2.6 Loss of vertical separation

In the simulations, this event was set up through a decompression of an aircraft that was flying above the aircraft, after which it made an emergency descent. The event is difficult to simulate as it requires good timing. It did not work out well and the results of this part of the simulations cannot be further analysed.

4.2.7 Transponder failure

A transponder failure causes the RPAS to disappear from the radar screen. In our case, the primary radar was not able to detect the RPAS and the controller needs to build the picture of the situation himself. The flight performed is indicated in Figure 28 below.

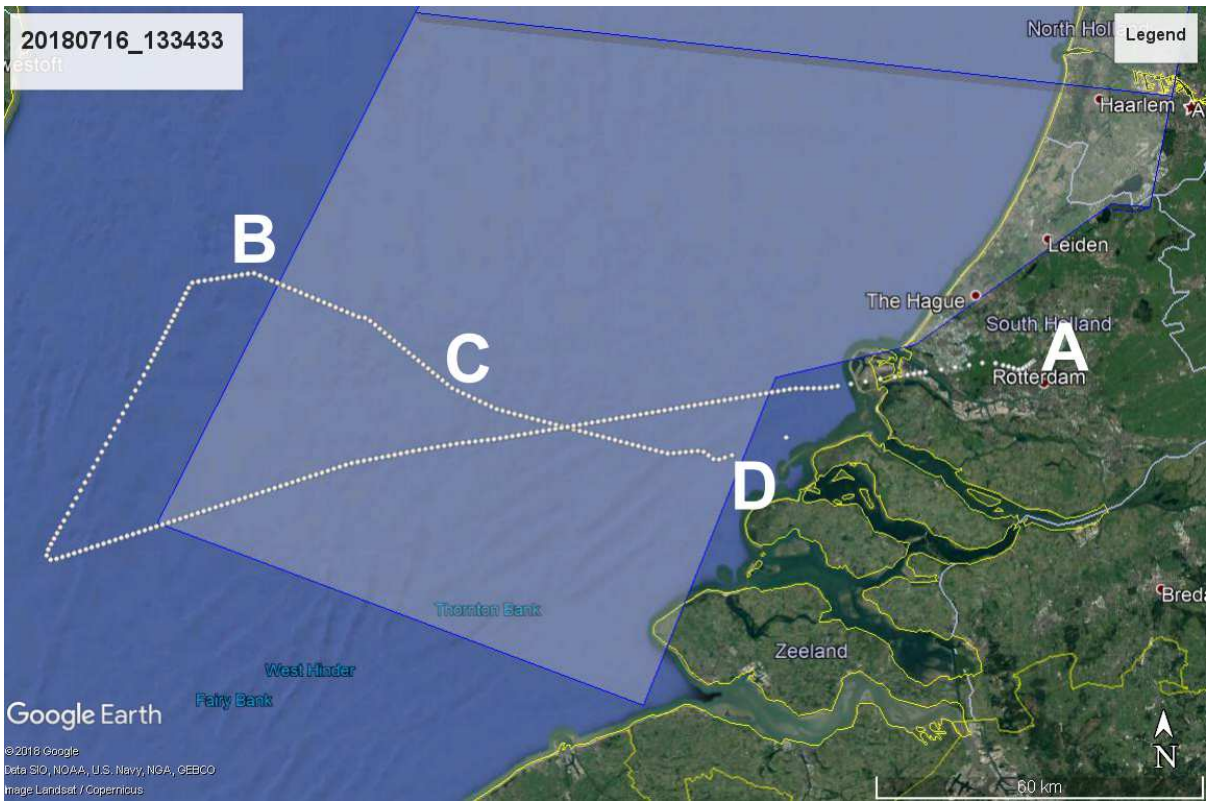


Figure 28 - Simulation Flight Path (Transponder failure)

Point A: Start of simulation
Point B: R/T communication fails (see other scenario)
Point C: Transponder fails
Point D: End of simulation

Observations:

- Controller directly notices the missing transponder at the screen
- Controller ask GCS pilot to confirm position and asks to state intentions. This will be done on a regular basis
- The controller will normally ask his assistant to take over the actions for the RPAS
- Controller will increase separation with other traffic significantly

4.3 Evaluation of the questionnaires

Completed questionnaires from the air traffic controllers have been captured and analysed.

Table 3 gives an overview of the answers provided. The mean score indicates the average answer given, where the second figure indicates the scale. Note that for some answers, a high score is positive, while for others the lower values indicate a well acceptable figure. This is indicated with "never", "very low" indication behind the questions.

Table 3 - Questionnaire: Mean Scores

#	Question	Mean Score
1.	I was able to handle the traffic in the simulation efficiently (never .. always)	5.2 / 7
2.	I was satisfied with my level of control in the simulation (never .. always)	5.4 / 7
3.	I did not experience interference with my work as controller (never .. always)	3.9 / 7
4.	I experienced safety during the simulation as (very low .. very high)	5.5 / 7
5.	I was able to plan and organise my work as I wanted (never .. always)	5.5 / 7
6.	What is the impact of RPAS on Situation Assessment? (no impact .. very high)	2.7 / 5
7.	What is the impact of RPAS on your workload? (no impact .. very high)	2.6 / 5
8.	What is the impact of the RPAS emergency procedure? (no impact .. very high)	2.8 / 5
9.	What is the impact of RPAS on Problem solving and Decision making? (no impact .. very high)	2.8 / 5
10.	What is the impact of RPAS on required controller actions? (e.g. system inputs, RT calls, coordination) (no impact .. very high)	2.9 / 5
11.	I was surprised by an event I did not expect (never .. always)	3.3 / 7

From the table, it can be observed that no very high or very low scores were given. One clear conclusion cannot be drawn from the scores; they need to be considered in the context of the simulations and the experience from the controllers. Some remarks were made by the observers and from evaluating the questionnaires in more detail:

- Controllers were not familiar with the UK airspace, though the MALE RPAS was flying in this part of the airspace. This influenced their capability to handle the traffic efficiently (question 1), but on the other hand, it caused them to be very busy and making the RPAS integration more interesting;

- The level of control that the air traffic controllers indicated in the simulations (question 2) was reasonably low in some of the simulation runs. These were the runs where controllers used the phone connection the first time; later in the simulations, the phone connection between the controller and the ground control pilot became more standard a part of their working procedures;
- The concerns on safety of the situation (question 4) correlate with the answer to question 2 on the level of control the air traffic controllers experienced. The same applies for their ability to plan and organise the work as they wanted.
- The impact of the MALE RPAS that controllers indicated on situation assessment (question 5) and on their workload (question 6) was mostly concerned with the need to give the RPAS a different route and the effect of the slow speed. In one occasion, where the impact was considered severe, the written statement from the controller stated that the RPAS had no impact on other traffic.
- Four questions concerned the impact the RPAS (questions 7, 8, 9 and 10) has on different aspects of the controller's task. The answers to these questions need to be evaluated in the context of the answers to the open questions.
- The relative high score to the question on whether the controller was surprised or not (question 11) is due to the lost position information events. The controller was not aware of the remaining capability of the MALE RPAS and needed a few iterations with the pilot to find out about the remaining navigation possibilities of the RPAS.

Table 4 gives an overview of the answers to the open questions. The cases where the controllers did not answer the questions, no bullet (not even an empty one) is provided.

Table 4 - Questionnaires: answers to open questions

During normal operation of the RPAS, did something interfere with your work as controller? If yes, please specify. • It was on a level which causes adjustment of handling traffic • No, besides normal separation • Not specifically, the low speed and ROC/ROD does cause some interference, but this is the case for any slow aircraft • Yes, mayday call • Yes, special separation at boundary which applies on handling
Were contingency procedures applied? If yes, which problems did occur? • Position lost, vectoring needed but due to relatively slow speed no read impact on situation of traffic • Yes, no radio contact • Lost comm. Very good to be able to use phone. • Lost transponder. Separation much more difficult because of no radar contact. Good to be able to use pilot phone • Yes, lost comms • C2 link failure + R/T failure

- Yes, L1 failure immediate RTB
- Yes, lost comms
- Lost comm (2x)
- Comm failure and loss of transponder
- Lost comm 7600
- Lost comm and lost position / GPS failure
- Lost comm, 1st stage transmitter failure

Which modifications or improvements do you suggest for contingency procedures?

- Normal performance should be mentioned
- Same lost comm procedures as for IFR traffic; ability for RPAS pilot to give bearing and distance when asked
- It would be much easier to be able to communicate with the RPAS without having to use a telephone. But then again: we are not able to communicate with regular traffic that has lost comms at all. Most important would be to have a direct line with the ground stations ASAP.
- The possibility to have an extra person take care of the emergency (planning) reduces the workload
- (translated) I would prefer one clear and concise lost comm procedure, similar to the ICAO/SERA procedures for IFR traffic

Please provide any comments or suggestions here

- The RPAS had no significant impact on workload or complexity. The only thing different from “normal” traffic was the routing
- In case of two RPAS (original text “Cronus’s” the call sign of the RPAS) at the same time: plan two different requested cruising levels
- (translated) Nice exercise :-)

4.4 Results from the Simulation Campaign

From the observations, questionnaires and discussions with all participants following each simulation run, a number of conclusions can be drawn. They will be given below in the same order as the observations described above. Please note that all BowTies are relevant to all flights, but specific TLEs deal with specific measures, for example: TLE 005 deals with a Communications Failure and Reversionary Communications Measures.

4.4.1 R/T communications failure

Conclusions:

- A good communications procedure needs to be established for the use of back up phone line. This includes strategic actions for example on how to find the pilot’s phone number by ATC and vice versa.
- The phone procedures take some training. After some time of using the phone, it became more easy to use

- Will it be necessary to keep a phone line open or can it be closed after each clearance and read back
- An assistant controller will be necessary to deal with the emergency situation of the MALE RPAS
- One suggestion was made to use the transponder or Mode-S (if available) for transmitting special messages to ATC
- If R/T failure is one direction, only from pilot to controller, it may be decided to cancel the need for read back
- A secondary frequency may be required

4.4.2 Loss of horizontal separation

Conclusions:

- Controllers need good briefing on routes from the RPAS
- This should be further investigated, maybe through other means as real-time simulations

4.4.3 Two RPAS with simultaneous communication failure

Conclusions:

- When two RPAS simultaneously have a loss of R/T voice communications with the same controller and are flown from one RPS and by one pilot, and the pilot can separates these RPAS, then for the controller the situation would be equivalent to the loss of R/T voice communication of one RPAS.

4.4.4 Navigation system failure

Conclusions:

- Should this be a pan-call? In the discussion, the tendency was no
- It may be decided to define standard phraseology for this (or use “unavailable RNAV”, which is standard ICAO
- The RPAS pilot shall inform the controller about the consequences of a failure on the performance of the RPAS, not on the failure itself.

4.4.5 Single C2 failure

Conclusions:

- It is the responsibility of the RPAS operator and RPAS pilot to assess the consequences of loss of C2 redundancy, and inform the ATC according to the procedures which have been agreed upon with the competent authority, for his RPAS. Only if the RPAS declares an emergency, ATC will give it priority, else the ATC will treat the RPAS as ‘normal’ operations.

4.4.6 Loss of vertical separation

No conclusions from the simulations

4.4.7 Transponder failure

Conclusions:

- An assistant controller will be necessary
- If available: R/T with a DF (Direction Finder) can be used to localise the RPAS at each moment (although not very accurate)

4.5 Simulation Campaign Participants

The following participants took part in the Simulation Campaign:

Air Traffic Controllers:

- **Ernst Burggraaf**: Area Control (RADAR/PROC) Amsterdam with 38 years of experience and already familiar with NARSIM.
- **Roelof Meijer**: Tower and Area Control (TWR/APP) De Kooy with 25 years of experience.
- **Jonah Bekkers**: Area Control (ACC) Amsterdam with 3 years of experience.

All of these controllers agreed that the training provided on the Simulation Campaign was sufficient for our needs.

RPAS Pilot:

- **Tim Smith**: Ex Royal Air Force navigator and qualified UAS Pilot with over 30 years of experience in aviation. Tim was the lead pilot on Project CLAIRE (Ref. 20):
  - 27 years in the RAF as a Navigator
  - 5 years as a trials RPAS pilot with Thales
  - 4000 hours flying of which 300 hours flying RPAS
  - RAF Aircrew Instructor
  - Royal Australian Air force Aircrew Instructor
  - MAA endorsed Crew Training Post Holder
  - Central Flying School endorsed Aircrew Instructor
  - First RPAS pilot in Europe to fly in controlled airspace
  - First RPAS pilot to gain a RPAS Instrument Rating

5 Initial Conclusions

Please note that these are a set of initial conclusions drawn by team SIRENS up to this point in time. They will be analyzed further before the set of final conclusions are delivered in the Final Report.

5.1 Safety Case Analysis Conclusions

5.1.1 Claim, Argument, Evidence

Underpinning the application of the Air Systems Safety Case analysis methodology derived in D1, to the Implementation Scenarios developed in D2, team SIRENS make the following ***Claim"*** in support of the overall objectives of this study: ***It will be safe to fly a MALE-type RPAS from Rotterdam under Netherlands ATC out over the North Sea towards the UK, crossing the border into UK airspace and handing over ATC to UK ATCOs; for the MALE-type RPAS to then conduct a Military ISR Mission in UK airspace and when complete, returning back into Netherland airspace under Netherlands ATC to return to base in Rotterdam.*** Note that this analysis does not include take-off and landing or ground operations which outside the scope of this study.

Clearly this claim covers many and varied aspects but is supported by a number of "***Arguments"*** that apply to each scenario in support of the claim:

> In terms of '**Equipment'** we argue that flying either of the two ***Implementation Scenarios*** (as described in D2 and Section 2 of this document) will be safe because the RPAS has type certification, it is maintained by SQEP under a strict set of rules, procedures and supervision and that the correct flight permit has been granted by the relevant authorities. In detail, the Air system design is safe because:
>
> - The Design organisation are appropriately trained, assessed & approved
> - Air System – Type approval certificate/Flight permit/release to service (military)
> - Equipment – Robust qualification/testing process
> - Approved Maintenance provider – Licenced Engineers etc…
> - Continued Airworthiness oversight is provided by the organisation
>
> In terms of '**Operational Organization'** we argue that flying either of the two ***Implementation Scenarios*** will be safe because the organization is subject to a regulated Design Approvals process, that the team operate to strictly-controlled and regulated procedures and are all SQEP. In detail, the Operational Organisation is safe because:
>
> - Operators & Maintainers are appropriately trained, assessed & approved.
> - Terms Of Reference (TORs) are in place for all staff and the Staff are suitably Qualified & Experienced
> - The organisation is compliant to appropriate Regulations

- Risk to Life (RtL) is understood and managed within the organisation
- Appropriate processes are in place to support the claim the Operational Organisation is safe.

In terms of '**Air Traffic Management'** we argue that flying either of the two ***Implementation Scenarios*** will be safe because the ATCOs are SQEP and they follow strictly enforced and supervised procedures. In detail, the Air traffic Management Organisation is safe because:

- Air traffic controllers are appropriately trained, assessed & approved.
- Standardised Air Traffic Management processes are used.
- The ATM organisation is compliant with appropriate regulations including any additional RPAS Accommodation procedures.

5.1.2 Methodology

The methodology developed is sound and can be used to produce a robust, holistic Air Systems Safety Case. However, the level of detail is somewhat generic and so it would need to be made 'specific' to any particular platform being flown and the host nations' regulations and requirements in order to support live flying of RPAS accommodation flights.

5.2 Simulation Campaign Conclusions

The following conclusions were derived from analysis of the simulation results and of the questionnaires formally completed by the participants during the campaign (see sections 4.3 and 4.4).

5.2.1 Participant Workload

We found that the ATCO participants were able to spot potential 'loss of separation' events between aircraft represented in the Simulation runs a long time before they would occur and instigate avoidance procedures well in advance. This begs a numbers of questions:

- What happens as the level of background air traffic increases?
  - At what point would 'normal' ATCOs start to miss spotting and dealing with potential conflicts?
  - Is there a point where the level of traffic is so high that the ATCOs could get overwhelmed and this Barrier begins to fail?
  - What then is the potential for the hazard to occur leading to consequential risk to life?
- What happens if there are more RPAS for the ATCOs to manage? At what point would the same set of issues outlined above start to occur?

- What happens if RPAS pilots begin to fly more than one Aircraft each? Does their ability to liaise with ATC diminish and at what point does this represent a failure of the Barrier leading to the occurrence of the TLE/Hazard?
- What happens if all of these situations occur?

In addition, it was thought that additional manpower might be required to help deal with RPAS emergencies:

- An assistant controller will be necessary to deal with MALE RPAS emergency situations and ensure sufficient mitigation measures are implemented as necessary

Other workload issues that arose included:

- Controllers were not familiar with the UK airspace which influenced their capability to handle the traffic efficiently but on the other hand it caused them to be very busy thus making the RPAS integration more stressful. This was a consequence of the fact that the ATCO participants in the Simulations were all Dutch, clearly they coped well and in a real-life exercise we would not expect this situation to occur but it should be recognised in the planning of real-life, cross-border RPAS flights.

- In the event of a Transponder failure an assistant controller will be necessary to help handle the situation. This could be mitigated by the use of additional localising equipment such as ADS-B.

5.2.2 Back up Communications Procedures

In the Simulation runs a back-up communications set-up was used whereby the ATCOs could talk to the RPAS Pilots via a dedicated phone line in case of emergency (i.e. in case of radio relay failure on-board the RPA). This was considered a reasonable measure with the following caveats:

- A good communications procedure needs to be established for the use of back up phone line. This includes several important considerations such as how to routinely identify the pilot's phone number by ATC (and vice versa); maintenance of communications with other air traffic and workload implications
- The phone procedures take some familiarisation effort, after some time using the phone, it became easier to use
- Is it considered necessary to keep the phone line open or could it be closed after each clearance and read back as necessary?
    - One suggestion was to use the transponder or Mode-S (if available) for transmitting special messages to ATC
- If R/T failure is one direction, only from pilot to controller, it may be decided to cancel the need for read back
- A secondary frequency may be required for radio and/or data-link communications back up

5.2.3 Route Awareness

As RPAS are accommodated alongside manned aviation the ATCOs need to gain confidence that the RPAS will behave as expected. To help gain this level of confidence the ATCOs will need "good briefing on planned RPAS routes". This is really to ensure that RPAS flights are planned in the same way and to the same level of detail as manned flights are now.

5.2.4 Dual- RPAS flying & Communications Failures

In the fullness of time it is conceivable that an RPAS Pilot may take control over more than one RPA (for example, the UK tactical UAS is designed to allow the single 'UAV Pilot' to control up to three airborne UAVs simultaneously, although this has not yet been attempted). This situation was simulated during the Simulation campaign in order to present a new and difficult situation to all participants, in particular since they were challenged with simultaneous loss of communications o both RPAs. In the relevant simulation run (run 9) both the ATCOs and RPAS Pilots coped admirably and made the following observation:

- When two RPAS simultaneously have a loss of R/T voice communications with the same controller and are flown from one GCS and by one pilot and the pilot can separate these RPAS, then for the controller (ATCO) the situation would be equivalent to the loss of R/T voice communication of one RPAS.

5.2.5 Navigation System Failures

Specific conclusions arising from the examination of the effect of a failure in the RPAS navigation system include:

- Should this be a pan-call? In the discussion, the tendency was no
- It may be decided to define standard phraseology for this (or use "unavailable RNAV", which is standard ICAO terminology
- The RPAS pilot shall inform the controller about the consequences of a failure on the performance of the RPAS, not on the failure itself.
- To mitigate transponder failure and if available, R/T voice communications with a direction finding capability can be used to localise the RPAS (although it is recognised that this is not a very accurate localisation solution)

5.2.6 Overall Safety and Control

In general, the ATCOs were satisfied that they retained a level of control over the airspace and its inhabitants with a MALE-type RPAS present, with the following specific observations:

- The level of control that the air traffic controllers indicated in the simulations was reasonably low in some of the runs. These were the runs where controllers used the phone connection

the first time. Later on in the simulations the phone connection between the controller and the ground control pilot became a more standard a part of their working procedures.

- The concerns on safety of the situation correlate with the answers on the level of control the air traffic controllers experienced. The same applies for their ability to plan and organise the work as they wanted.
- The impact of the MALE RPAS that controllers indicated on situation assessment and on their workload was mostly concerned with the need to give the RPAS a different route and the effect of its slow (slower) speed. In one occasion, where the impact was considered severe (by team SIRENS), the written statement from the controller stated that the RPAS had no impact on other traffic.

Therefore we conclude that the accommodation of MALE-type RPAS as demonstrated in the simulation runs conducted under this study does not compromise ATCOs ability to maintain safe skies.

5.2.7 The 'Impact' of RPAS Accommodation

The participants were questioned about the overall impact of accommodating a MALE –type RPAS in the scenarios and their conclusion was that the RPAS had no significant impact on ATCO workload or scenario complexity. The only thing that was noted to be different from "normal" traffic was the way the RPAS was routed.

There were times during the simulation runs (particularly when positional information was compromised) where the ATCOs were not aware of or familiar with the remaining RPAS capabilities and it took them a few iterations to become comfortable with the ability of the RPAS to navigate as expected.

Controllers were not initially familiar with the capabilities of the RPAS and so it took them a few iterations to understand them. Such capabilities will need to be provided as part of the flight programme filed pre-flight.

6 Initial Recommendations

Please note that these are a set of initial recommendations made by team SIRENS up to this point in time. They will be analyzed further before the set of final recommendations are presented in the Final Report.

6.1 MALE-type RPAS Performance criteria

Team SIRENS recommends that a standardised set of minimum MALE-type RPAS performance characteristics are developed and agreed to aid ATM and to set the benchmark for type-certification for Integration into European Airspace alongside manned aviation. For example these should specify a minimum climb rate which will allow ATCOs to position the RPAS in such a way as to ensure swift compliance with anticipated separation directives. Similarly a minimum descent rate, transit speed, Loiter direction & radius (in the event of Loss of datalink) and manoeuvrability characteristics should also be considered to ensure safe separation is maintained even in adverse environmental conditions. It may be that MALE-type RPAS become classified into a range of 'classes'.

6.2 Fully Integrated Air Systems Safety Case Methodology

We recommend that a further study programme is conducted to ensure that the Safety Case Methodology, as proposed in this study, is complete and fully exercised integrating the three primary safety attributes of Equipment; Organisation and Air Traffic Management. The proposed methodology should be subject to further examination by independent experts outside of Team SIRENS in each of the three areas.

6.3 Complete Hazard Analysis

We recommend that each of the identified hazards is exercised in a subsequent set of simulation scenarios to fully test the Safety Case Methodology and ensure study completeness. This wide ranging hazard analysis may also include additional hazards and inputs from the EDA and wider community of experts supporting the study. This treatment will need to cover elements excluded from this study such as: take-off and landing, ground operations and flight over densely populated areas.

6.4 Accommodation Scenario Development

We recommend that the "Consolidated Generic Accommodation Scenario" be further developed to accommodate the lessons from this study aiming at turning it into an 'Integration Scenario' involving a heterogeneous set of MALE-type RPAS with differing performance characteristics.

This scenario also needs to be expanded to cover issues including:

- Flight over populated areas
- The utility of 'Detect And Avoid' technology additions
- Quantitative analysis (this will require the selection of a 'specific' RPAS instance in order to be able to define meaningful metrics and performance figures to support the analysis).

6.5 Live Flying

We recommend that the Safety Case Methodology developed in this study is exercised to the next level by applying it to a live flying RPAS exercise. This should be conducted opportunistically to reduce costs and to achieve flights as quickly as possible. Ideally these flights should be performed using a MALE-type RPAS in European airspace but benefit would still be gained from using other RPAS types and making use of segregated airspace (to de-risk exercises and refine initial operating procedures) before making the transition into various flight conditions within Controlled Airspace (e.g. benign to complex airspace structures; quiet to congested airspace; optimal to demanding environmental conditions).

ANNEXES

Annex A Acronyms and Abbreviations

ACC	Area Control Centre
ALARP	As Low As Reasonably Possible
APP	Approach
ASSC	Air Systems Safety Case
ATC	Air Traffic Control/Controller
ATCO	Air Traffic Control Officer
ATM	Air Traffic Management
C2	Command and Control
CAE	Claim, Argument, Evidence
CLAIRE	CiviL Airspace Integration of RPAS in Europe
CTR	Control Traffic Region
DF	Direction Finder
EASA	European Aviation Safety Agency
EDA	European Defence Agency
E-OCVM	European Operational Concept Validation Methodology
ESARR	EUROCONTROL Safety Regulatory Requirements
FIR	Flight Information Region
FOO	Flight Operations Organisation
FRC	Flight Reference Cards
GCS	Ground Control Station
GDT	Ground Data Terminal
GNSS	Global Navigation Satellite System
ICAO	International Civil Aviation Organization
IFF	Identification Friend-Or-Foe
IFR	Instrumental Flight Rules
JARUS	Joint Authorities for Rulemaking on Unmanned Systems
MALE	Medium Altitude Long Endurance
MAC	Mid Air Collision

MFTP	Military Flight Trial Permit (Permit to Fly)
MUST	Multi UAS Supervision Testbed
NARSIM	NLR ATC Research Simulator
NATO	North Atlantic Treaty Organization
NLR	Netherlands Aerospace Centre
OAT	Operational Air Traffic
ROC	Rate of Climb
ROD	Rate of Decent
RPAS	Remotely Piloted Aircraft Systems
RTB	Return to Base
RtL	Risk to Life
R/T	Radio/Telephone
SAM	Safety Assessment Methodology
SAME	Safety Assessment Made Easier
SERA	Standardised European Rules of the Air
SESAR	Single European Sky ATM Research
SORA	Specific Operations Risk Assessment
SIRENS	Simulations for Integrating RPAS into European Nations Safely
SQEP	Suitably Qualified and Experienced Person
SRM	SESAR Safety Reference Material
SWIM	System Wide Information Management
TLE	Top Level Events
UAS	Unmanned Aircraft System
UAV	Unmanned Air Vehicle
VFR	Visual Flight Rules
WCA	Warnings, Cautions and Advisory

Annex B Bow Tie Models

Figure 29 – TLE 001: Loss of Separation with Ground (during Emergency Recovery)

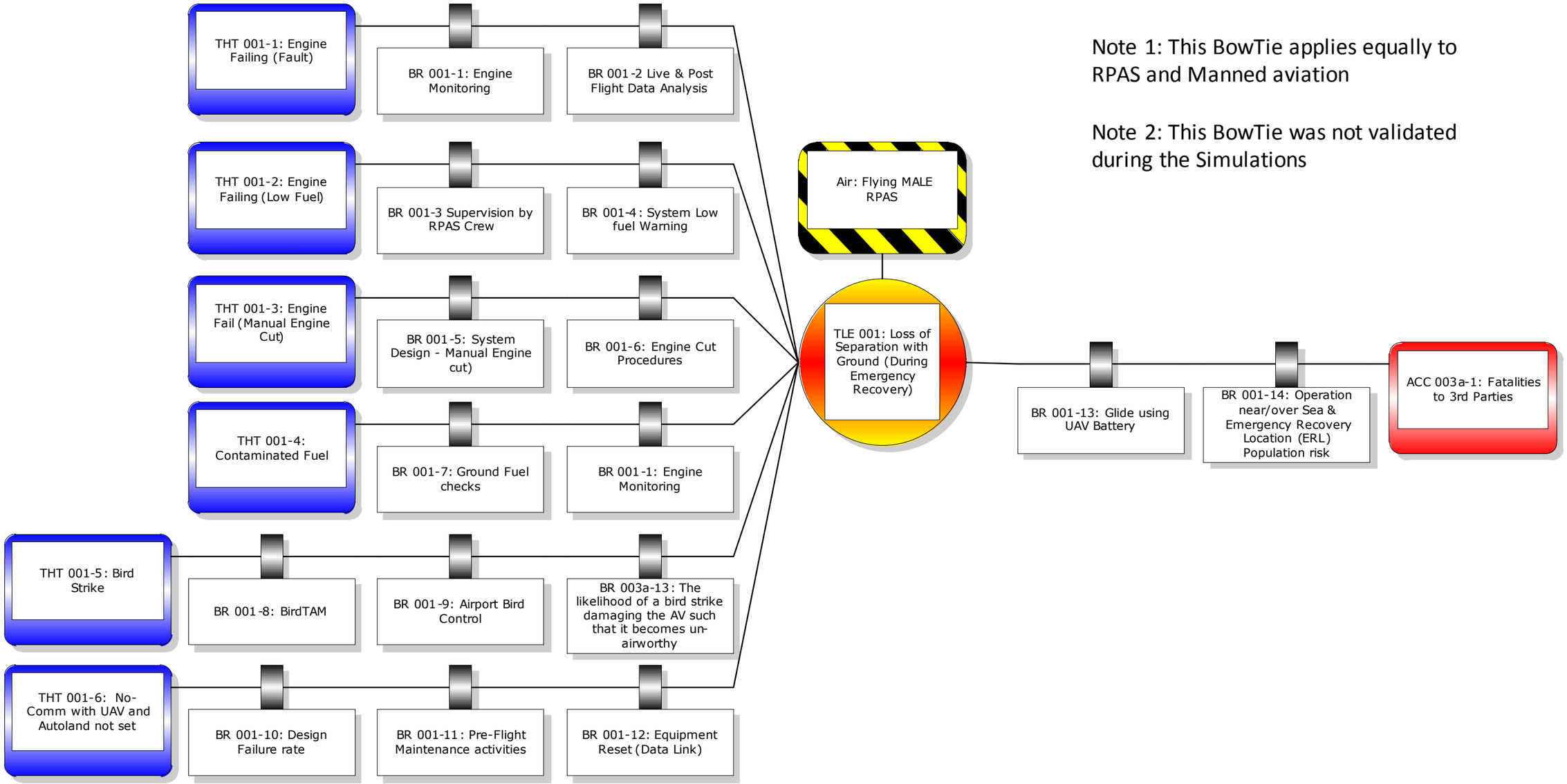


Figure 30 - TLE 002: Loss of Separation with Ground (Unintentional CFIT)

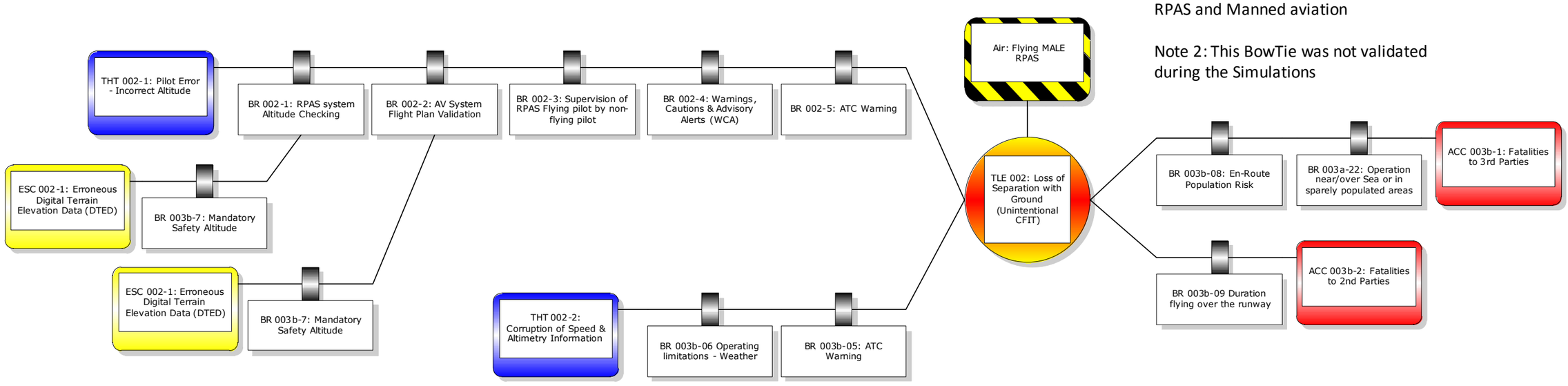
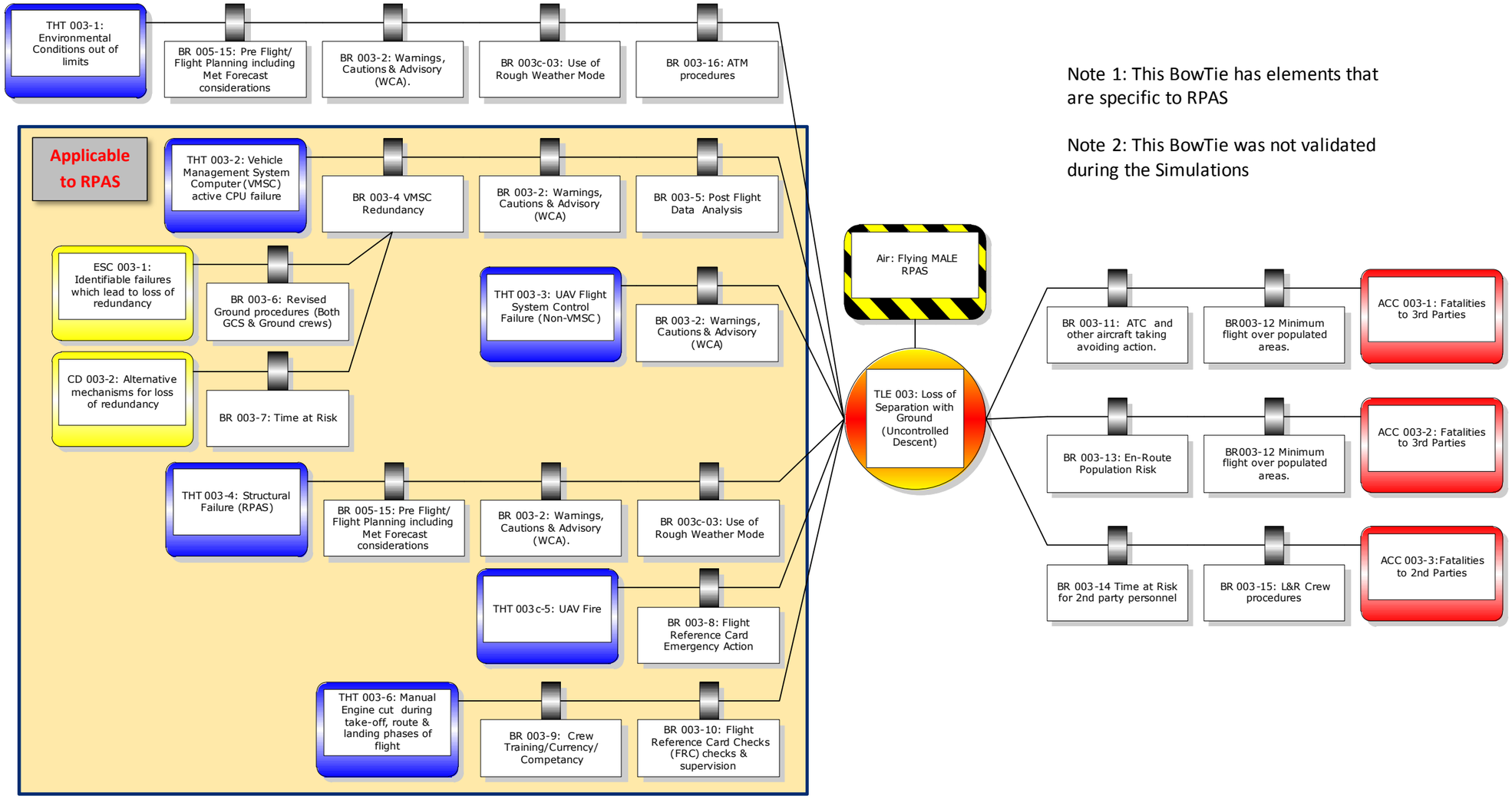


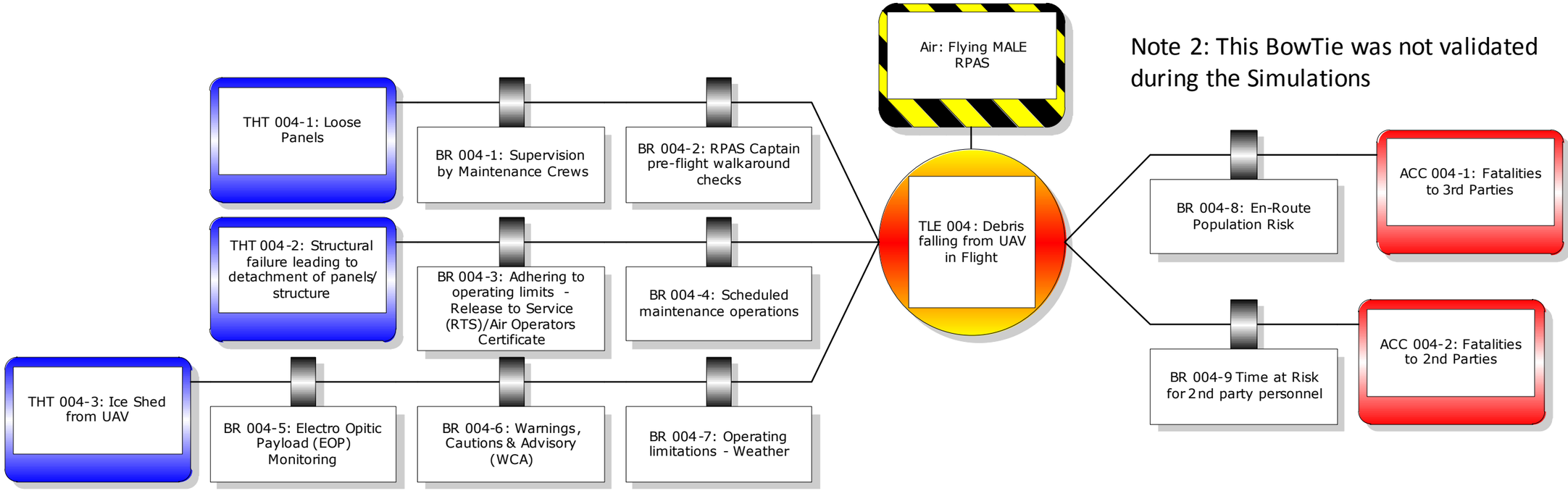
Figure 31 - TLE 003: Loss of Separation with Ground (Uncontrolled Descent)



Note 1: This BowTie has elements that are specific to RPAS

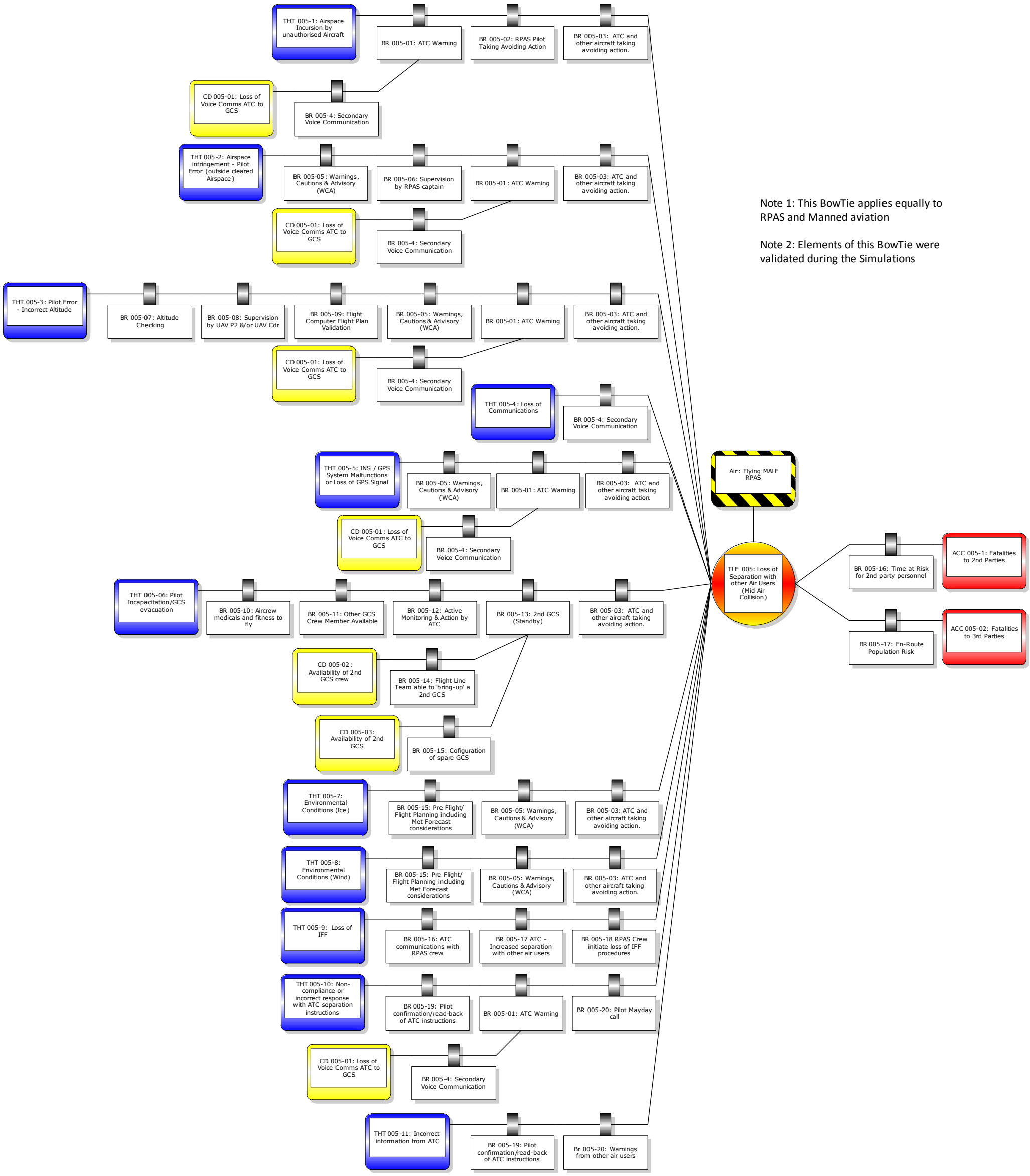
Note 2: This BowTie was not validated during the Simulations

Figure 32 - TLE 004: Debris falling from UAV in Flight



This page is left intentionally blank

Figure 33 - TLE 005: Loss of Separation with other Air Users (Mid-Air Collision)

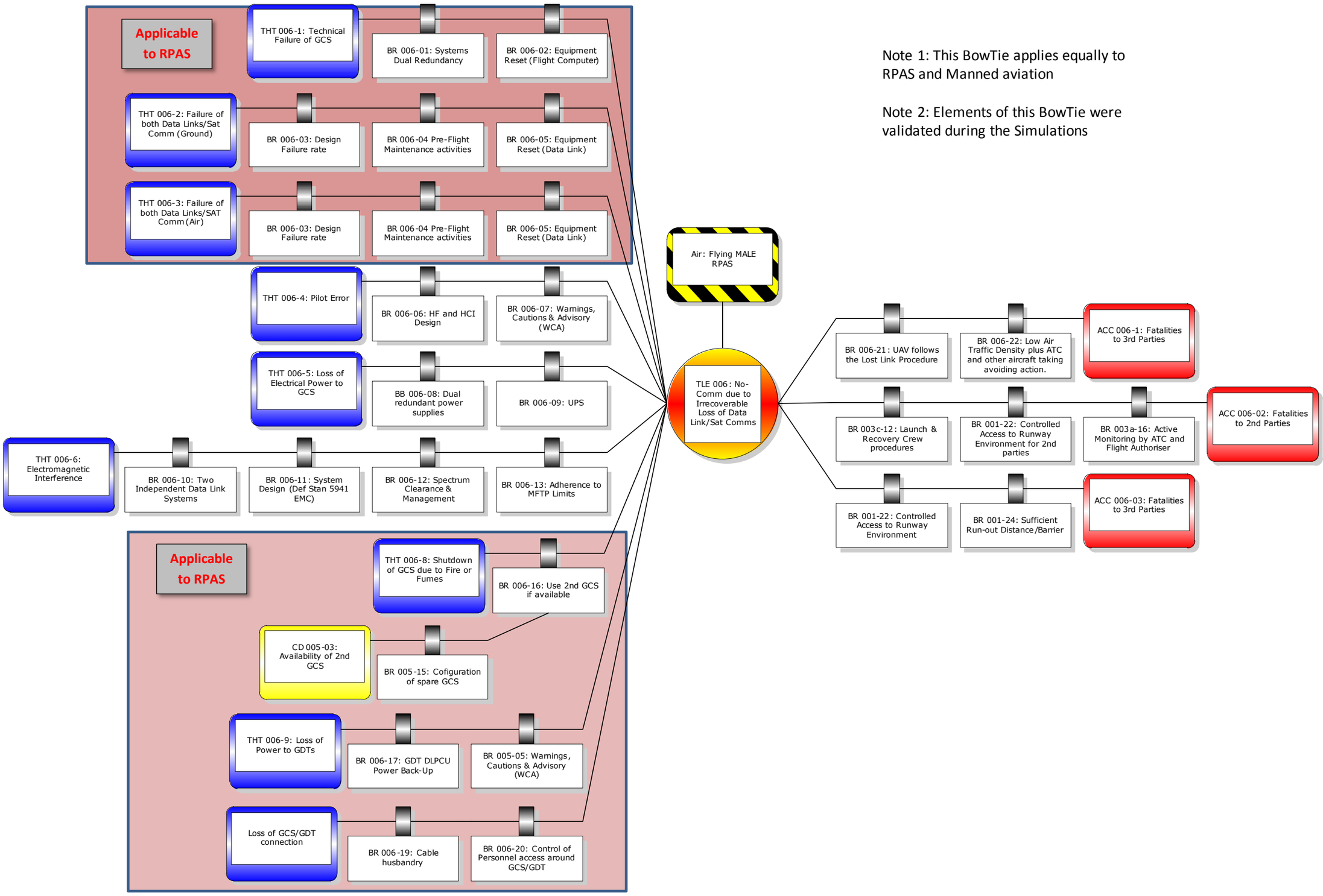


Note 1: This BowTie applies equally to RPAS and Manned aviation

Note 2: Elements of this BowTie were validated during the Simulations

Figure 34 - TLE 006: No-Comm due to irrecoverable loss of data Link/Sat Comms

(Blank space to accommodate legible diagram)



Note 1: This BowTie applies equally to RPAS and Manned aviation

Note 2: Elements of this BowTie were validated during the Simulations