Final Safety Assessment Report_4

Document information	
Project title	Conflict Detection, Resolution and Monitoring
Project N°	04.07.02
Project Manager	DSNA
Deliverable Name	Final Safety Assessment Report_4
Deliverable ID	D61
Edition	00.03.00

Task contributors
DFS, DSNA, NATS, Honeywell

Abstract

This document contains the Specimen Safety Assessment for a typical application of the 03.03.01 OFA Conflict Detection, Resolution and Monitoring in En Route Trajectory based environment, namely the operational services in SESAR P04.07.02: TRajectory Adjustment through Constraint of Time (TRACT) and Conflict Detection / Resolution (CD/R) aid to Planner Controller / Tactical Controller (PC/TC). The report presents the assurance that the Safety Requirements for the V2-V3 phases are complete, correct and realistic, thereby providing all material to adequately inform the 03.03.01 OFA SPRs, as part of solution #27.

2 Authoring & Approval

Prepared By		
[redacted] NATS	[redacted]	24/08/2016
[redacted] THINK RESEARCH on behalf of NATS		24/08/2016

3

Reviewed By - *Reviewers internal to the project.*		
Name & Company	Position & Title	Date
[redacted] DSNA	[redacted]	14/06/2016
[redacted] NATS		14/06/2016
[redacted] THINK RESEARCH on behalf of NATS		14/06/2016
[redacted] DFS		14/06/2016
[redacted] THALES		14/06/2016
[redacted] EUROCONTROL		14/06/2016
[redacted] HONEYWELL		14/06/2016
[redacted] AIRBUS		14/06/2016
[redacted] DSNA		14/06/2016
[redacted] DSNA		14/06/2016

4

Reviewed By - *Other SESAR projects, Airspace Users, staff association, military, Industrial Support, other organisations.*		
Name & Company	Position & Title	Date
[redacted] NATS	[redacted]	01/07/2016
[redacted] NATS		01/07/2016
[redacted] INDRA		01/07/2016
[redacted] HONEYWELL		01/07/2016
[redacted] THALES		01/07/2016
[redacted] SELEX		01/07/2016
[redacted] SELEX		01/07/2016
[redacted] EUROCONTROL		01/07/2016
[redacted] THALES		01/07/2016
[redacted] AIRBUS		01/07/2016
[redacted] DSNA		01/07/2016
[redacted] SICTA		01/07/2016
[redacted] DASSAULT		01/07/2016
[redacted] NOVAIR		01/07/2016
[redacted] MINISTERO DELLA DIFESSA		01/07/2016
[redacted] ELFAA		01/07/2016
[redacted] TURKISH AIRLINES		01/07/2016
[redacted] ATCEUC		01/07/2016
[redacted] HONEYWELL		01/07/2016
[redacted] DSNA		01/07/2016
[redacted] EUROCONTROL		01/07/2016
[redacted] EUROCONTROL		01/07/2016

Approved By		
Name & company	Position / Title	Date
<Name> / <company>	<Position / Title>	<Date>

Document History

Edition	Date	Status	Author	Justification
00.00.01	19/05/2015	Draft	[redacted]	Creation of new document.
00.00.02	26/05/2015	Draft		Updated after internal review.
00.00.03	17/06/2015	Updated Draft		Update following internal and external review.
00.01.00	19/06/2015	Issue		Update for issue to SJU.
00.01.01	18/08/2015	Updated Draft		Updated with the past validation exercises' results for internal review.
00.01.02	27/08/2015	Updated Draft		Updated following internal review ready to be sent out to external reviewers.
00.02.00	02/10/2015	Issue		Workshop updates added for issue to SJU.
00.02.01	29/01/2015	Update Draft		Updates following SJU comments.
00.02.02	14/06/2016	Update Final Draft		Update following VP-501 and VP-798
00.02.03	01/07/2016	Update Final Draft		Update following internal review
00.02.04	18/07/2016	Update Final Draft		Update following external review. Draft to be sent to WP10
00.03.00	25/10/2016	Final Version		Update following SJU comments and final resubmission.

IPR (foreground)

This deliverable consists of SJU foreground.

Table of Contents

EXECUTIVE SUMMARY **9**

1 INTRODUCTION **10**

1.1 BACKGROUND 10
1.2 GENERAL APPROACH TO SAFETY ASSESSMENT 11
1.2.1 A Broader Approach *11*
1.3 SCOPE OF THE SAFETY ASSESSMENT 11
1.4 LAYOUT OF THE DOCUMENT 12
1.5 GLOSSARY OF TERMS 12
1.5.1 Overview *12*
1.5.1 Safety Reference Material (SRM) *23*
1.5.2 Others *27*
1.6 ACRONYMS AND TERMINOLOGY 27
1.7 REFERENCES 31

2 SAFETY SPECIFICATIONS AT THE OSED LEVEL **32**

2.1 SCOPE 32
2.2 "CONFLICT DETECTION, RESOLUTION AND MONITORING" - OPERATIONAL ENVIRONMENT AND KEY PROPERTIES 32
2.2.1 Airspace Structure, Type and Boundaries *32*
2.2.2 Airspace Users (Flight Rules), Traffic Levels and complexity *33*
2.2.3 Aircraft ATM capabilities *33*
2.2.4 Communications, Navigation and Surveillance (CNS) Aids *34*
2.2.5 Separation Minima *35*
2.2.6 Operational services *35*
2.3 AIRSPACE USERS REQUIREMENTS 35
2.4 RELEVANT PRE-EXISTING HAZARDS 36
2.4.1 Pre-existing Hazards for TRACT *36*
2.4.2 Pre-existing Hazards for CD/R aid to PC *36*
2.4.3 Pre-existing Hazards for CD/R to TC *37*
2.5 SAFETY CRITERIA (SAC) 37
2.5.1 Introduction *37*
2.5.2 Scope *37*
2.5.3 Attendees of the Workshop *37*
2.5.4 Derivation of SAfety Criteria *38*
2.6 MITIGATION OF THE PRE-EXISTING RISKS – NORMAL OPERATIONS 42
2.6.1 Derivation of Safety Objectives for Normal Operations *42*
2.6.2 Analysis of the Concept for a Typical Flight *52*
2.7 CONFLICT DETECTION, RESOLUTION AND MONITORING OPERATIONS UNDER ABNORMAL CONDITIONS 56
2.7.1 Identification of Abnormal Conditions *56*
2.7.2 Potential Mitigations of Abnormal Conditions *58*
2.8 MITIGATION OF SYSTEM-GENERATED RISKS (FAILURE APPROACH) 66
2.8.1 Identification and Analysis of System-generated Hazards *66*
2.8.2 Derivation of Safety Objectives (integrity/reliability) *70*
2.9 IMPACTS OF CONFLICT DETECTING, RESOLUTION AND MONITORING OPERATIONS ON ADJACENT AIRSPACE OR ON NEIGHBOURING ATM SYSTEMS 72
2.10 ACHIEVABILITY OF THE SAFETY CRITERIA 72
2.10.1 TRACT *72*
2.10.2 CD/R aid to PC *73*
2.10.3 CD/R aid to TC *76*
2.11 VALIDATION & VERIFICATION OF THE SAFETY SPECIFICATION 81

3 SAFE DESIGN AT SPR LEVEL **81**

3.1 SCOPE 81
3.2 THE CONFLICT DETECTION, RESOLUTION AND MONITORING SYSTEMS SPR-LEVEL MODEL 81

3.2.1 Description of SPR-level Model *81*
3.2.2 Task Analysis *83*
3.2.3 Derivation of Safety Requirements (Functionality and Performance – success approach) *84*
3.3 ANALYSIS OF THE SPR-LEVEL MODEL – NORMAL OPERATIONAL CONDITIONS 107
3.3.1 Scenarios for Normal Operations *107*
3.3.2 Thread Analysis of the SPR-level Model – Normal Operations *109*
3.3.3 Effects on Safety Nets – Normal and Abnormal Operational Conditions *109*
3.3.4 Dynamic Analysis of the SPR-level Model – Normal and Abnormal Operational Conditions *109*
3.3.5 Additional Safety Requirements (functionality and performance) – Normal Operational Conditions *128*
3.4 DESIGN ANALYSIS – CASE OF INTERNAL SYSTEM FAILURES 128
3.4.1 Scenarios for the Failure Case Analysis *128*
3.4.2 Derivation of Safety Requirements (Integrity/Reliability) *129*
3.4.3 Thread Analysis of the SPR-level Model - Abnormal Conditions *135*
3.4.4 Additional Safety Requirements – Abnormal Operational Conditions *136*
3.5 ACHIEVABILITY OF THE SAFETY CRITERIA 136

APPENDIX A SUCCESS CASE SAFETY REQUIREMENTS DERIVATION 137

A.1 THREAD ANALYSIS 137
A.1.1 TRACT *137*
A.1.2 PC aid *142*
A.1.3 TC aid *149*

APPENDIX B FAILURE CASE SAFETY OBJECTIVES AND REQUIREMENTS DERIVATION 153

B.1 DETAILED PSSA RESULTS 153
B.1.1 TRACT *155*
B.1.2 CD/R aid to PC *170*
B.1.3 CD/R air to TC *195*
B.2 SYSTEM GENERATED HAZARDS – MAXIMUM TOLERABLE FREQUENCY OF OCCURRENCE CALCULATIONS 2

APPENDIX C TASK 20 – REVIEW SAFETY WORKSHOP 5

C.1 MAIN RESULTS 5
C.1.1 Suppressed Requirements *5*
C.1.2 Additional Requirements *7*
C.1.3 Changes in existing SPRs *7*

APPENDIX D DELETED REQUIREMENTS – TC AID 8

List of tables

Table 2 Pre-existing Hazards 36
Table 3 Task 20 workshop participants 38
Table 4 Operational Services & Safety Objectives (success approach) – TRACT 44
Table 5 List of Safety Objectives (success approach) for Normal Operations - TRACT 45
Table 6 Operational Services & Safety Objectives (success approach) – CD/R aid to PC 46
Table 7 List of Safety Objectives (success approach) for Normal Operations - CD/R aid to PC 49
Table 8 Operational Services & Safety Objectives (success approach) – CD/R aid to TC 50
Table 9 List of Safety Objectives (success approach) for Normal Operations - CD/R aid to TC 52
Table 10 Abnormal Conditions and Potential Mitigations 65
Table 11: System-Generated Hazards and Analysis for TRACT 67
Table 12: System-Generated Hazards and Analysis for CD/R aid to PC 69
Table 13: System-Generated Hazards and Analysis for CD/R aid to TC 70
Table 14: Safety Objectives (integrity/reliability) - TRACT 71
Table 15 Safety Objectives (integrity/reliability) - PC aid 71
Table 16 Safety Objectives (integrity/reliability) - TC aid 72
Table 17 SAC Quantification - TRACT 73
Table 18 SAC Quantification - CD/R aid to PC 76
Table 19 SAC Quantification - CD/R aid to TC 80
Table 20: Mapping of Safety Objectives to the SPR-level Model Elements – TC aid 86
Table 21: Derivation of Safety Requirements (success case) from Safety Objectives – TC aid 88
Table 22: Assumptions made in deriving the above Safety Requirements – TC aid 89
Table 23 Mapping of Safety Objectives to the SPR-level Model Elements – PC aid 92
Table 24 Derivation of Safety Requirements (success case) from Safety Objectives – PC aid 96
Table 25 Assumptions made in deriving the above Safety Requirements – PC aid 97
Table 26 Mapping of Safety Objectives to the SPR-level Model Elements – TRACT 99
Table 27 Derivation of Safety Requirements (success case) from Safety Objectives - TRACT 102
Table 28 Assumptions made in deriving the above Safety Requirements - TRACT 103
Table 29 Additional Success Case Safety Requirements following VP-798 106
Table 30: Operational Scenarios – Normal Conditions TRACT 108
Table 31 Operational Scenarios – Normal Conditions PC aid 109
Table 32 Operational Scenarios – Normal Conditions TC aid 109
Table 33 TC Aid Success Case Safety Requirements Verification 114
Table 34 PC Aid Success Case Safety Requirements Validation 120
Table 35 PC Aid Success Case Safety Requirements Verification 123
Table 36 TRACT Success Case Safety Requirements Verification 128
Table 37 Probability numbers calculation - Example 130
Table 38: Safety Requirements or Assumptions - abnormal conditions for TRACT 132
Table 39: Safety Requirements or Assumptions - abnormal conditions for PC Aid 134
Table 40: Safety Requirements or Assumptions - abnormal conditions for TC Aid 135
Table 41: TRACT: scenario 1 138
Table 42: TRACT: scenario 1: Alt Flow 1 138
Table 43: TRACT: scenario 1: Alt Flow 2 139
Table 44: TRACT: scenario 1: Alt Flow 3 139
Table 45: TRACT: scenario 2 140
Table 46: TRACT: scenario 2: Alt Flow 1 140
Table 47: TRACT: scenario 2: Alt Flow 2 141
Table 48: TRACT: scenario 2: Alt Flow 3 142
Table 49: TRACT: scenario 2: Failure Flow 1 142
Table 50: PC Aid scenario 1 143
Table 51: PC Aid scenario 1: alt flow 1 144
Table 52: PC Aid scenario 1: alt flow 2 145
Table 53: PC Aid scenario 2 146
Table 54: PC Aid scenario 2: Alt Flow 2 146
Table 55: PC Aid scenario 2: Alt Flow 3 146
Table 56: PC Aid: scenario 2: Alt Flow 4 147

Table 57: PC Aid: scenario 3 147
Table 58: PC Aid: scenario 4 148
Table 59: PC Aid: scenario 5 149
Table 60: TC Aid: scenario 1 150
Table 61: TC Aid: scenario 1: Alt Flow 1 150
Table 62: TC Aid: Scenario 1: Failure Flow 1 150
Table 63: TC Aid: scenario 1: Failure Flow 2 150
Table 64: TC Aid: scenario 2 151
Table 65: TC Aid: scenario 3 152
Table 66: TC Aid: scenario 3: Alt Flow 1 152
Table 67 Detailed PSSA Results – TRACT 167
Table 68 PSSA Analysis - Resultant Hazards for each failure case TRACT 167
Table 69 FHA Analysis - Hazard Tolerable Failure Rate TRACT 168
Table 70 PSSA Analysis - Resultant Hazards Selection for the FCSR TRACT 169
Table 71 Detailed PSSA Results - PC aid 191
Table 72 PSSA Analysis - Resultant Hazards for each failure case PC Aid 193
Table 73 PSSA Analysis - Hazard Tolerable Failure Rate PC aid 193
Table 74 PSSA Analysis - Resultant Hazards Selection for the FCSR PC aid 194
Table 75 Detailed PSSA Results TC aid 209
Table 76 PSSA Analysis - Resultant Hazards for each failure case TC Aid 1
Table 77 PSSA Analysis - Hazard Tolerable Failure Rate TC aid 1
Table 78 PSSA Analysis - Resultant Hazards Selection for the FCSR TC aid 2
Table 79 System Generated Hazards maximum tolerable frequency of occurrence calculations – TRACT 3
Table 80 System Generated Hazards maximum tolerable frequency of occurrence calculations - PC aid 3
Table 81 System Generated Hazards maximum tolerable frequency of occurrence calculations - TC aid 4
Table 82 TC Aid - Deleted Requirements 8

List of figures

Figure 1: Separation related Entities. 13
Figure 2: Encounter Management related Entities. 15
Figure 3: Planning Aircraft vs. Aircraft Encounters. 15
Figure 4: Tactical Aircraft vs. Aircraft Encounters. 16
Figure 5: Predicted Infringement Point vs Potential Infringement Point. 18
Figure 6 Mid-Air Collision Barrier Model 38
Figure 7 TRACT Sequence Diagram 53
Figure 8 CD/R aid to TC Sequence Diagram 54
Figure 9: TRACT SPR level model 82
Figure 10: PC Aid SPR level model 82
Figure 11: TC aid SPR level model 83
Figure 12: TRACT: scenario 1 137
Figure 13:TRACT: scenario 1: Alt Flow 1 138
Figure 14: TRACT: scenario 1: Alt Flow 2 138
Figure 15: TRACT: scenario 1: Alt Flow 3 139
Figure 16: TRACT: scenario 2 139
Figure 17: TRACT: scenario 2: Alt Flow 1 140
Figure 18: TRACT: scenario 2: Alt Flow 2 141
Figure 19: TRACT: scenario 2: Alt Flow 3 141
Figure 20: TRACT: scenario 2: Failure Flow 1 142
Figure 21: PC Aid scenario 1 143
Figure 22: PC Aid scenario 1: alt flow 1 144
Figure 23: PC Aid scenario 1: alt flow 2 145
Figure 24: PC Aid scenario 2 145

213 Figure 25: PC Aid: scenario 2: Alt Flow 4 146
214 Figure 26: PC Aid: scenario 3 147
215 Figure 27: PC Aid: scenario 4 148
216 Figure 28: PC Aid: scenario 5 149
217 Figure 29: TC Aid: scenario 1 149
218 Figure 30: TC Aid: scenario 1: Alt Flow 1 150
219 Figure 31: TC Aid: scenario 2 151
220 Figure 32: TC Aid: Scenario 3 152
221

Executive summary

This document contains the Specimen Safety Assessment for a typical application of the 03.03.01 OFA Conflict Detection, Resolution and Monitoring in En Route Trajectory based environment and it impacts the following Operational Improvement steps:

- CM-0207-A “Advanced Automated Ground Based Flight Conformance Monitoring in En Route”
- CM-0205 “Advanced Conflict Detection and Resolution in En Route" – which will be split in two OIs:
    - CM-02XX for TCT
    - CM-02YY for PC
- CM-0403-A "Early Conflict Resolution through CTO allocation in STEP 1"

The report presents the assurance that the Safety Requirements for the V2-V3 phases are complete, correct and realistic, thereby providing all material to adequately inform the 03.03.01 OFA SPR, as part of solution #27. The requirements were determined through the success and failure approach described in the Safety Reference Material [1] and Guidance to Apply Safety Reference Material [2].

1 Introduction

1.1 Background

The aim of the Operational Focus Area (OFA) 03.03.01 “Conflict Detection, Resolution and Monitoring” is to develop a system which provides real-time assistance to the En route controllers in conflict detection and resolution using trajectory data in Predefined Route environments and to provide resolution support information based upon predicted conflict detection and associated monitoring features.

The objective is to provide the controller (Planner / Tactical) with an automated Conflict Detection and Resolution aid tool using an enhanced Trajectory Prediction model through the use of improved data, e.g. extended flight plan data, real-time on board trajectory data, and met data. Trajectory data may be made available via extended flight plans and new Interoperability (IOP) capabilities.

The current document aims to present the results of the safety assessment, which took place under P04.07.02 (V2 and V3), focused on the current “Conflict Detection, Resolution and Monitoring” operational services, namely TRajectory Adjustment through Constraint of Time (TRACT) and Conflict Detection / Resolution (CD/R) aid to Planner Controller / Tactical Controller (PC/TC).

Note: The safety activities presented in this document are at a: **V2 maturity level for TRACT and CD/R aid to PC;** and **V3 maturity level for CD/R aid to TC**.

TRACT (V2) is a strategic de-conflicting service that adjusts 4D planning trajectories to optimise separation management for medium and/or long term conflicts (e.g. potential conflicts that will be apparent in the next 20 – 30 minutes). The trajectory adjustment relies, amongst others, on Flight Management System (FMS) generated trajectory which is based on more reliable information and will result in an improved computation of the solution. The computed speed adjustments are translated into a Controlled Time Over (CTO) which are transmitted to the aircraft via Datalink between the ground and airborne systems. No controller intervention is required but flights under TRACT “control” are highlighted on the controller display.

There are two main aspects to the **CD/R aid to PC (V2)**: conflict detection and conflict resolution. **Conflict Detection** may aim to support the PC by identifying and classifying potential interactions between flights at the various events associated with the inter-sector co-ordination process (e.g. receipt of an offer, selection of a suitable sector exit level etc.) and on a cyclic basis to identify whether the situation has changed significantly such that (Planning) Controller intervention is required to re-evaluate and amend as necessary. **Conflict resolution** in Planning terms may involve the identification of alternative co-ordination conditions (level, route, profile etc.) at either the entry and/or exit boundaries of the sector so that unacceptable workload for the Tactical Controller is avoided whilst offering as expeditious a flight profile as possible to the airspace user. The system may build upon the tools developed for the Planning Conflict Detection (CD) support. For example, it may allow the PC to ask “what-if” questions to the system which will respond with similarly classified interactions that are predicted to occur if the potential co-ordination plan were to be put in place. The PC may also use the “what-else” tool to directly be informed of the alternatives that the system evaluated on its own. Additionally, CD/R for PC includes a monitoring aid which assesses the achievability of exit levels based on aircraft performance and conformance to the agreed planning amendments (not following the agreed heading, for example). Deviation alerts that are identified are highlighted in the Track Data Block (TDB).

Just as in the case of the CD/R aid to PC, there are two main aspects to the **CD/R aid to TC (V3)** as well, conflict detection and conflict resolution. The Conflict Detection service supports the TC in assuring separation between (pairs of) aircraft and between aircraft and restricted airspace (based on tactical trajectories). It may aim to support the controller by identifying and classifying potential interactions between flights that are under tactical control within the Area of Responsibility. S/he will also address remaining conflicts which have been highlighted by the PC. Conflict Resolution in

tactical terms may involve the identification of different solutions, e.g. by modifying the trajectory laterally, vertically or in terms of speed adjustments. In the envisaged operational environment priority should be given to solutions which impose a minimum deviation from the RBT. Moreover, the solution should be closed loop as far as practicable, i.e. it should be clearly defined when and how the aircraft returns on RBT. Decision Support Tools may include "what-if" and/or "what-else" services. With this aid, it is up to the controller to identify the "best" conflict resolution with regards to the specific situation.

1.2 General Approach to Safety Assessment

1.2.1 A Broader Approach

This safety assessment is conducted as per the SESAR Safety Reference Material (SRM) [1] which itself is based on a two-fold approach:

- a success approach which is concerned with the safety of the "Conflict Detection, Resolution and Monitoring" operations in the absence of failure within the end-to-end "Conflict Detection, Resolution and Monitoring" System.
- a conventional failure approach which is concerned with the safety of the "Conflict Detection, Resolution and Monitoring" operations in the event of failures within the end-to-end "Conflict Detection, Resolution and Monitoring" System.

Together, the two approaches lead to Safety Objectives and Safety Requirements which set the minimum positive and maximum negative safety contributions of the "Conflict Detection, Resolution and Monitoring" System.

1.3 Scope of the Safety Assessment

This Safety Assessment is focused on the three "Conflict Detection, Resolution and Monitoring" operational services, more specifically TRACT, CD/R aid to PC and CD/R aid to TC.

This report is a proposed version for the final Safety Assessment Report (SAR), addressing safety related activities for V2 and V3. It includes the provision of the following results:

- Information defined at "Operational Service(s) Environmental Description (OSED) level" which includes:
    - The SAfety Criteria (SAC) which determine the expected level of safety for the "Conflict Detection, Resolution and Monitoring" services;
    - The Safety Objectives, which specifies what the "Conflict Detection, Resolution and Monitoring" services have to provide in terms of operational service in order to satisfy the SACs.

Two types of Safety Objectives are provided: the "Functionality" ones, describing the services required from the "Conflict Detection, Resolution and Monitoring" services, and the "Integrity" ones, specifying the integrity of the "Conflict Detection, Resolution and Monitoring" system to provide those services.

- Information defined at "SPR level" which includes:
    - The Safety Requirements which specify how the "Conflict Detection, Resolution and Monitoring" system is to provide the operational services defined by the Safety Objectives mentioned above.

Two types of Safety Requirements are provided as well at this level: the "Functionality" ones and the "Integrity" ones (as for the Safety Objectives).

Evidence on the completeness, correctness and realism of these results is provided in this assessment, either directly included in this report or providing the relevant cross-reference to the concerned project document where evidence can be found for a specific subject.

1.4 Layout of the Document

Section 1 is the current introduction to the safety assessment report for the “Conflict Detection, Resolution and Monitoring” services.

Section 2 documents the safety assessment of the “Conflict Detection, Resolution and Monitoring” system at the service level and provides its specification in terms of Safety Objectives.

Section 3 documents the safety assessment of the “Conflict Detection, Resolution and Monitoring” system at the design level and provides the corresponding specification in terms of Safety Requirements.

Appendix A shows the thread diagrams that were used to derive the safety requirements.

Appendix B documents the detailed Preliminary System Safety Assessment (PSSA) undertaken to derive the failure case safety requirements and the full calculus of the *Maximum Tolerable Frequency of Occurrence* rates for each system generated hazard.

Appendix C presents the changes that have been made to the safety assessment in light of the safety workshop that took place in September 2015.

1.5 Glossary of terms

1.5.1 Overview

The terms used in this document are consistent with those used in the OSED [4]. As a result, the following section is a direct copy of the same section within the OSED [4]. The terms are replicated here purely for the benefit of the reader.

Separation Related Terms.

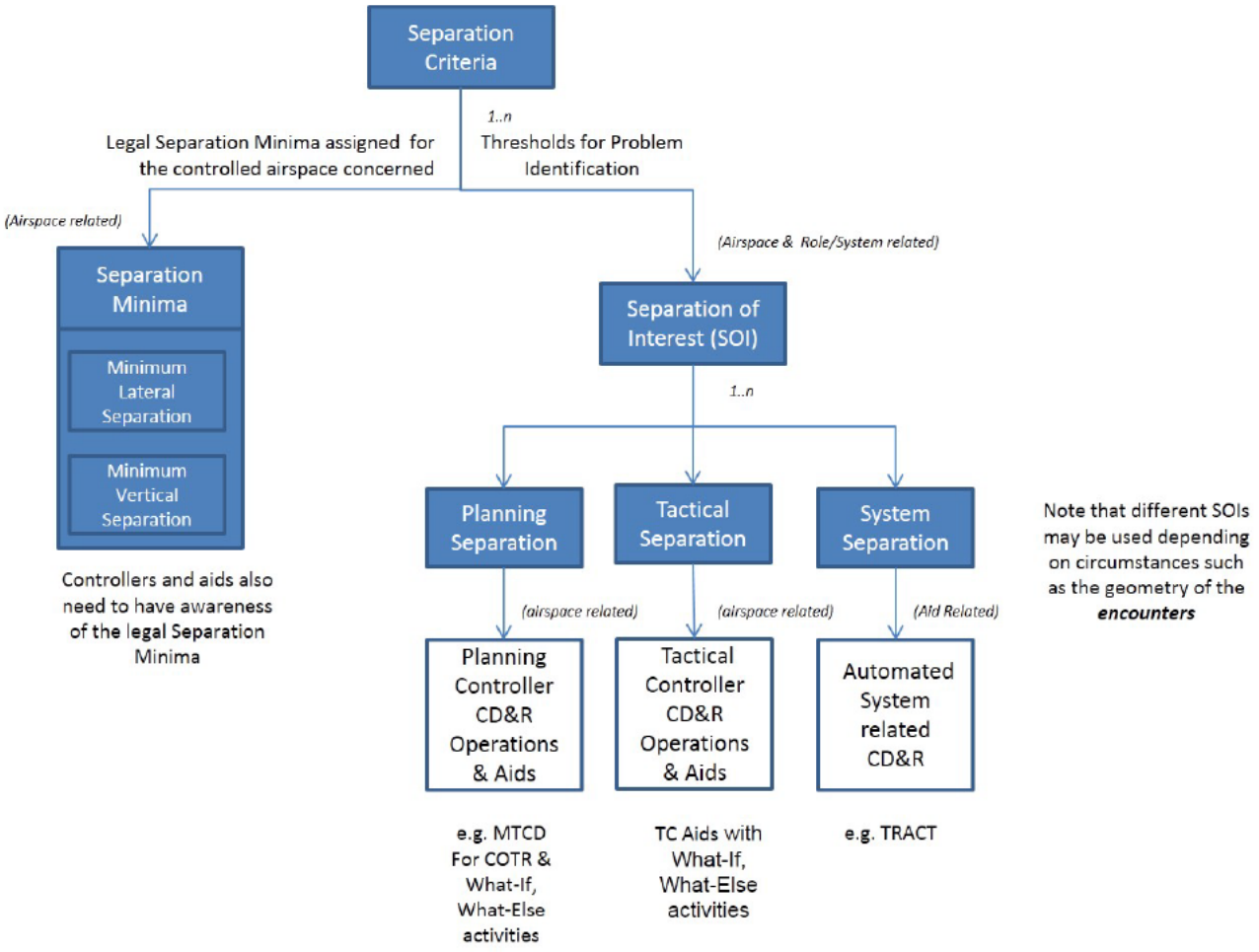
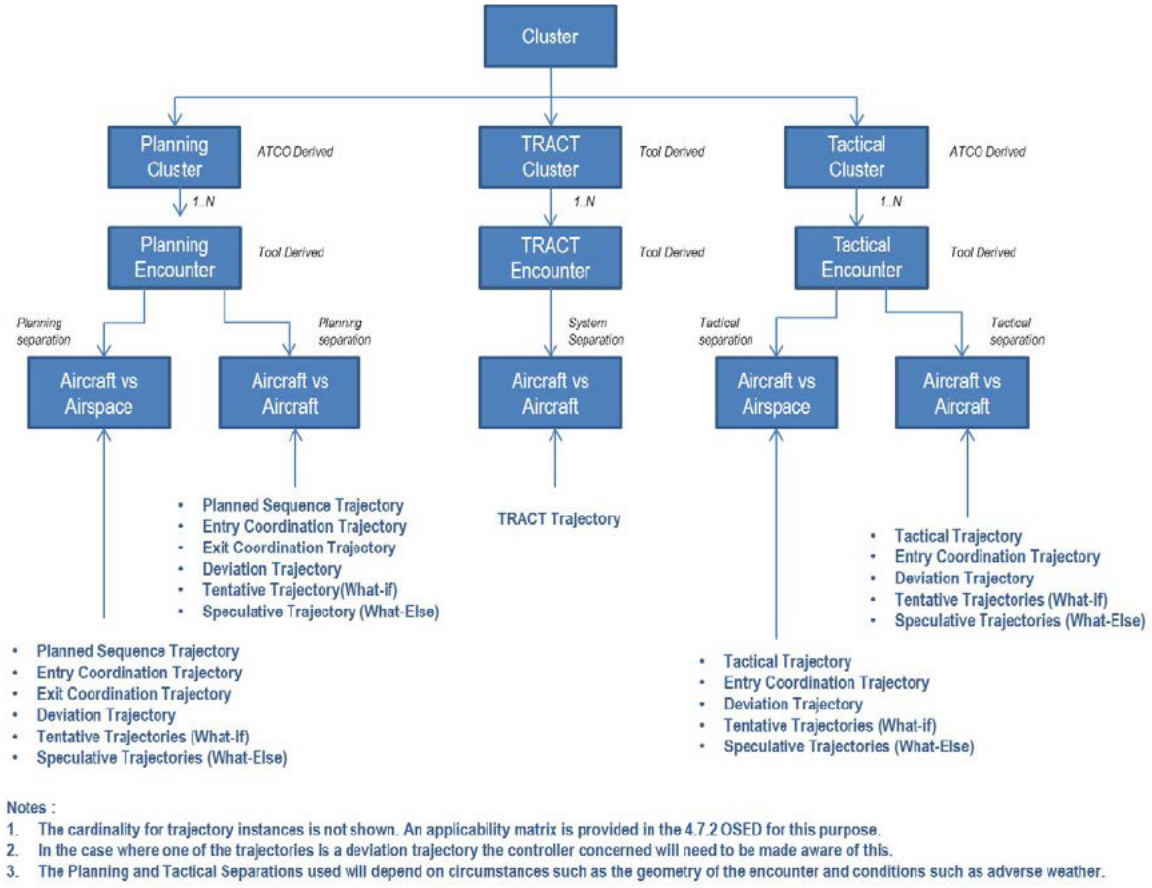


Figure 1: Separation related Entities.

Term	Definition
Separation Criteria	A generic term which covers the ***Separation Minima*** and the thresholds used for problem identification.
Separation	Spacing between an aircraft and a ***Hazard***.
Lateral Separation	***Separation*** expressed in terms of horizontal distance and function of angular convergence/divergence between tracks.
Vertical Separation	***Separation*** expressed in units of vertical distance.
Separation Minima Related Terms Note: that the separation minima define the legal separation between hazards in a controlled airspace.	
Separation Minima	The minimum displacements between an aircraft and a ***Hazard*** which maintain the risk of collision at an acceptable level of safety. Note: ICAO Doc 9689 describes the methodology to be used for the determination of ***Separation Minima***.
Minimum Lateral Separation	The ***lateral separation*** threshold above which the ***separation minima*** are fulfilled

Minimum Vertical Separation	The ***vertical separation*** threshold above which the ***separation minima*** are fulfilled Note: Different thresholds are applied above and below the ***RVSM*** limit. Any non-RVSM aircraft that is authorized to fly within an RVSM airspace shall be subject to the thresholds that are applied below the RVSM limit.
Reduced Vertical Separation Minimum (RVSM)	A reduction to 1000 feet ***vertical separation*** between flights, which is used at least in Europe and on the North Atlantic, between FL290 and FL410.
Separation of Interest	The ***separation*** threshold below which the proximity of a pair of aircraft is considered to be of interest to a controller, for the airspace and conditions concerned. Note: At this point there may be no actual risk that ***separation minima*** are infringed. The values chosen for the various controller activities and tools are larger than the separation criteria in order to provide an adequate margin of safety. The controller and the aids used need to have awareness of the applicable separation minima for the airspace concerned. Note: This is a generic term, independent of the planning or tactical layers of separation activity. Particular instances of the ***Separation of Interest*** may be applied for each level of separation activity. The actual ***separation*** values used will take into account aspects such as the type of clearance issued, the requested navigation precision and the airspace rules. They will also relate to the type of trajectory used at the specific layer of concern. They may vary according to circumstances such as the geometry of the ***conflicts***/***encounters*** and prevailing conditions such as adverse weather.
Planning Separation (of Interest)	A particular instance of the ***Separation of Interest*** which is applied during planning activities. Note: This is a generic term relevant to the planning layers of separation activity. Particular instances of this may be applied for each level of layered planning separation activity. The actual ***separation*** values used will vary according to the circumstances. For instance, in the case of Planner Controllers coordinating traffic into and out of sectors, it is the horizontal distance/time interval threshold below which the proximity of a pair of aircraft is considered to be of interest to a Planner Controller when determining the acceptability of sector entry or exit co-ordination. The TC may choose to increase this **Planning Separation**, in which case the PC must re-coordinate the relevant aircraft.
Tactical Separation (of Interest)	A particular instance of the ***Separation of Interest*** which is applied by Tactical Controllers when controlling traffic under their responsibility.
System Separation (of Interest)	A particular instance of the ***Separation of Interest*** which is applied by automated system tools for the detection of ***Encounters***. E.g. the ***separation of interest*** used by the TRACT tool.

Conflict management Related Terms



Notes :
1. The cardinality for trajectory instances is not shown. An applicability matrix is provided in the 4.7.2 OSED for this purpose.
2. In the case where one of the trajectories is a deviation trajectory the controller concerned will need to be made aware of this.
3. The Planning and Tactical Separations used will depend on circumstances such as the geometry of the encounter and conditions such as adverse weather.

Figure 2: Encounter Management related Entities.

		Subject Flight				
		Planned Sequence Traj.	Entry Coordination Traj.	Exit Coordination Traj.	Deviation Traj.	Context Traj.
Environmental Flight	Planned Sequence Traj.	Planned Sequence Encounter	--	--	--	--
	Entry Coordination Traj.	--	Planning Encounter	Planning Encounter	Planning Deviation Encounter	--
	Exit Coordination Traj.	--	Planning Encounter	Planning Encounter	Planning Deviation Encounter	--
	Deviation Traj.	--	Planning Deviation Encounter	Planning Deviation Encounter	Planning Deviation Encounter	--
	Context Traj.	--	--	--	--	Context Encounter

Figure 3: Planning Aircraft vs. Aircraft Encounters.

		Subject Flight		
		Tactical Traj.	Deviation Traj.	Entry Traj.
Environmental Flight	Tactical Traj.	Tactical Encounter	Tactical Deviation Encounter	Coordination Encounter
	Deviation Traj.	Tactical Deviation Encounter	Tactical Deviation Encounter	Coordination Encounter
	Entry Traj.	--	--	Coordination Encounter

Figure 4: Tactical Aircraft vs. Aircraft Encounters.

(note that speculative/tentative trajectories are not considered in Figure 3 and Figure 4 for the sake of simplicity)[1]

Hazard	The objects or elements that an aircraft can be separated from. Note: In En Route, these can be: other aircraft, airspace with adverse weather conditions, or airspace with incompatible airspace activity.

[1] There is scope for Planner What-If/What-Else probes to build Tactical Tentative/Speculative trajectories.
An example would be when the Planner performs a What-If on the XFL of FL350 with a heading coordination constraint of HDG090, while the Tactical has the flight currently cleared at FL330 flying on its own navigation. The PC Aid would show the results of the What-If and also (some components of) the Planner's TC Aid would show the results of a tentative tactical clearance of FL350, HDG090. When the Planner What-If ends (either by the Planner committing or cancelling the instruction) then the corresponding Tactical What-If shall end.

Additionally, it is possible to perform a What-Else on top of a What-If (therefore requiring speculative tentative trajectories). For example, during a heading What-If, there may be a simultaneous What-Else probing different levels along that tentative heading. This applies to both the PC Aid and the TC Aid.

The controller may also wish to perform multiple flight What-If/What-Else probes, for instance perform a heading What-If on one flight and then a heading What-Else on another. During a multiple flight What-If/What-Else, all existing primary, deviation, tentative and speculative trajectories shall be probed against each other:

- During a What-If, the subject flight's primary and deviation (if it exists) trajectories will be *replaced* by the tentative trajectory;
- During a What-Else, the subject flight's primary and deviation (if it exists) trajectories will be *augmented* by speculative trajectories.

A multiple flight What-Else could be performed when the controller selects an encounter and asks the PC Aid to suggest a solution. The PC Aid would then run heading What-Else probes on both flights and display a set of acceptable headings to the controller (i.e. either a pair of headings that require the minimum deviation to each flight's route, or a range of possible headings that are free of encounters).
This could also apply when the controller is performing a level What-If (so What-If plus a multiple flight What-Else). It may be possible to extend this to multiple flight What-If & What-Else probes, e.g. if two flights are involved in level What-Ifs and the PC Aid detects an encounter, then a multiple flight heading What-Else probe could then be run.
The controller may add additional flights into the probe set, e.g. if all solutions to one encounter cause (or fail to resolve) an encounter with another flight, then the controller could decide to perform a What-Else probe including that flight too (i.e. the system would then attempt to identify a set of clearances that would resolve the encounters between all flights in the probe set).

Separation Violation	A separation violation relates to a situation where the applicable ***separation minima*** have actually been infringed Note: e.g. Short Term Conflict Alert (STCA) or Minimum Safe Altitude Warning (MSAW). These situations are not within the scope of Separation Management as covered in the 4.7.2 OSED [4].
Conflict **Potential Conflict** **Predicted Conflict**	These terms relate to any situation involving aircraft and hazards in which the applicable ***separation minima*** may be compromised. Note**:** These terms are in general widespread usage and within the context of this glossary are synonymous. They relate to potential ***infringements of separation minima.*** More specifically they are used in the context of ATCO activities where actions are performed in order to anticipate and resolve conflicts (potential/predicted) for separation management purposes. This is in contrast to the situations detected and processed by CD&R tools where the terminology used is '***encounters',*** which relates to the applicable ***Separation of Interest*** used by the tool-set, rather than ***Separation Minima***.
Encounter	A situation where an aircraft is predicted to be below the applicable ***separation of interest*** with respect to another aircraft, or a designated volume of airspace, classified respectively as "aircraft-to-aircraft" and "aircraft-to-airspace" encounters. Notes: Encounters are related to the various detection tools and may work to different look-ahead time horizons with different separation criteria, using different trajectories. Different tool configurations can therefore be expected to yield different encounters. The ***Separation of Interest*** thresholds are considered with respect to any applicable ***uncertainty volumes*** around the predicted aircraft position(s).
TRACT Encounter	A specific instance of an ***Encounter*** which is predicted using the ***TRACT Trajectory*** and the particular ***System Separation.***
Planning Encounter	A specific instance of an ***Encounter*** which is predicted using any of the planning related ***trajectories*** and the ***Planning Separation***.
[Tactical/Planning] Context Encounter	To support the controllers' traffic management task, environmental flights which may be of interest due to their anticipated vertical and lateral profiles, known as **[Tactical/Planner] Context flights** (or alternatively "[Tactical/Planner] Traffic"), will be highlighted to controllers. Planner Context flights may not currently be involved in an encounter with the subject flight based on their current clearance or existing coordinated levels but may need to be considered by the Planner when making coordination choices for their sector. **Context Encounters** are detected between Context Trajectories. With Planner Context there is only one separation threshold, "Context Separation", and therefore no such concept as a "Context Conflict". When referring to **Context Encounters** operationally the environmental flights may just be labelled as "Traffic".
Tactical Encounter	A specific instance of an ***Encounter*** which is predicted using any of the tactical related ***trajectories*** or the ***Entry Coordination Trajectories,*** and the ***Tactical Separation.***
Planned Sequence Encounter	A specific instance of a ***Planning Encounter*** which is predicted between two ***Planned Sequence Trajectories***.
Coordination Encounter	A specific instance of a ***Tactical Encounter*** which is predicted between two ***Entry Trajectories.***
[Tactical/Planning] Deviation Encounter	A specific instance of a ***[Tactical/Planning] Encounter*** which is predicted using at least one ***[Tactical/Planning] Deviation Trajectory***.

Cluster	A set of one or more ***Encounters*** that should be treated as a whole when determining their resolution.
Planning Cluster	A ***Cluster*** of ***Planning Encounters***. Note: A ***Planning Cluster*** is an operational object that may be handled by ATCOs. The grouping of ***encounters*** is therefore likely to be an operational decision.
TRACT Cluster	A set of one or more ***TRACT Encounters*** that are treated as a whole when the TRACT determines their resolution.
Closest Point of Approach	The point on the ***Trajectory***, which is being evaluated, where the distance to the ***hazard*** is predicted to be minimal. Note: In some cases the evaluation may be made on the basis of a trajectory segment, e.g. when two aircraft join the same route at the same speed. Subsequent points along the trajectory being evaluated, beyond the closest point of approach are separated from the hazard by progressively increasing distance.
Predicted Infringement Point	The point on the ***Trajectory***, which is being evaluated, for a particular ***Encounter***, where infringement of the applicable ***Separation of Interest*** is predicted at respective flight positions for the trajectories concerned.
Potential Infringement Point	The point on the ***Trajectory***, which is being evaluated, for a particular ***Encounter***, where infringement of the applicable ***Separation of Interest*** may potentially occur within the ***uncertainty volumes*** for the trajectories concerned.

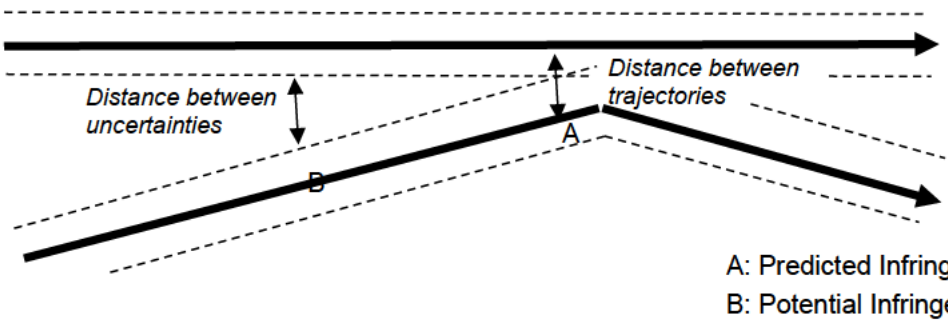
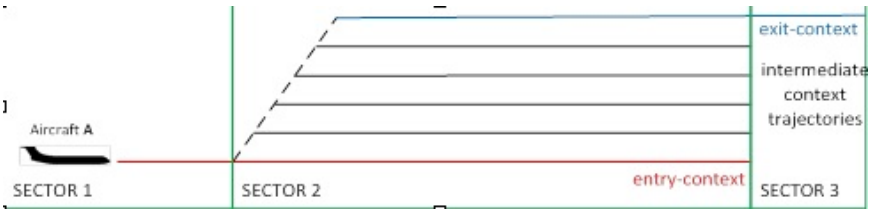
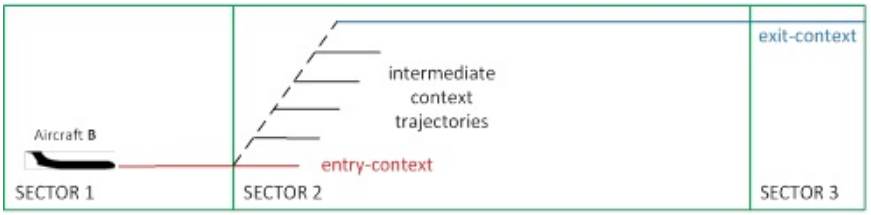


Figure 5: Predicted Infringement Point vs Potential Infringement Point.

What-if Probing	A process where a private copy of a ***Trajectory*** that is in operational use and associated data is taken and used as a ***Tentative Trajectory*** to check the impact of changes to the flight data on the occurrence of predicted ***Encounters***, without affecting the corresponding data for the actual flight. Note: On completion the what-if data and the ***Tentative Trajectory*** may be discarded or used to implement an update to the actual flight data and to construct the necessary clearance.
What-else Probing	A process where several ***Speculative Trajectories*** and associated data arising from ***What-If Probing*** are assessed for the impact on the occurrence of predicted ***Encounters***. The ***Speculative Trajectories*** utilise flight data other than that currently committed or tentatively selected (during ***What-If Probing*** operations) by the controller.
Trajectory and Flight Related Terms See Figure 1 for an overview of the trajectory usage.	
Uncertainty, Uncertainty Volume	The volume of airspace, around the nominal predicted future position of a flight, within which a flight is expected to be contained to a given statistical confidence (e.g. 95%) at the time to which the prediction relates. The uncertainty relates to the trajectory prediction and may therefore be considered as a property of the particular trajectory concerned.

	Note: The zone can be decomposed into along-track (longitudinal), across-track (lateral) and vertical dimensions.
Trajectory	The predicted behaviour of an aircraft. Note: the ***Trajectory*** is usually modelled as a set of consecutive segments linking waypoints and/or points computed by the aircraft avionics (e.g. FMS) or by the ground system to build the vertical profile and the lateral transitions. Note: Each point is defined by a longitude, latitude, a vertical distance and a time.
ADS-C EPP Report **EPP Data**	ADS-C EPP (Extended Projected Profile) report is the ADS-C report containing the sequence of 1 to 128 waypoints or pseudo waypoints with associated constraints and/or estimates (altitude, time, speed, etc.), gross mass and min/max speed schedule, etc. as defined in WG78/SC214 standards. Note: The aircraft's predicted trajectory is down-linked in accordance with its ADS-C contract parameters. The EPP Data can be used for variety of ATC services (e.g. TRACT).
Tentative Trajectory	Tentative ***trajectories*** are created from another trajectory that is in operational use (Tactical, Planning or otherwise). They reflect tentative what-if flight data selected by the controller. If these conditions are then committed the Tentative trajectory and the associated data will be used to establish the new operational trajectory. If the conditions are discarded then it will also be discarded. Note: Tentative trajectories support ***What-If probing*** and are created during this process.
Speculative Trajectory	A ***Trajectory*** that uses flight data other than those currently committed or tentatively selected (during a ***What-If Probing*** operation), by the controller. Note: Speculative Trajectories are produced for the purpose of ***What-Else probing***.
Tactical Trajectory	The ***Tactical Trajectory*** is calculated within a short look-ahead time (e.g. up to 15 minutes) during tactical ATC operations (sector planning layer). It therefore reflects an accurate view of the predicted flight evolution, starting from the current flight position (generally, as reported by surveillance), with low ***uncertainty*** and high precision. It is kept up to date with all clearances, including tactical instructions. During any open tactical manoeuvres it will also be reflecting those temporary conditions. It is usually determined with a fast update rate (e.g. 5 seconds) and with an optimised ***Uncertainty*** calculation; to maximise response and minimise the incidence of false alarms. Note: The Tactical Trajectory supports the tactical ATC operations when the flight follows its normal behaviour
[Tactical/Planning] Deviation Trajectory	The ***Deviation Trajectory*** provides the predicted profile of the aircraft based on the observed behaviour, extrapolated from the particular deviation from the current clearance (or deviation from coordination constraint for ***Planning Deviation Trajectories***). Note: ***Deviation Trajectories*** are necessary for situations where non-compliance with a flight's expected tactical or coordinated behaviour is observed, with respect to an applicable tolerance threshold. ***Deviation Trajectories*** support Tactical/Planner ATC operations when the flight has deviated from its predicted behaviour. The ***Tactical Deviation Trajectory*** is useful for a short prediction horizon (e.g. 3-5 minutes). A ***Planning Deviation Trajectory*** follows the cleared route of the flight, irrespective of any coordination constraints (as the flight has been observed to be deviating from these constraints). During periods where a ***Deviation Trajectory*** is necessary it may also be used by

	TC/PC CD&R Aid.
Subject Flight	A flight that has been explicitly selected by the Controller concerned.
Subject Trajectory	The ***Trajectory*** of the ***Subject Flight***
Environmental Flight	A flight of interest to the Controller which is not the ***Subject Flight***. The ***Subject Flight*** will be checked for ***encounters*** with all ***Environmental Flights***.
Context Flight	A flight that may need to be considered by the Planner ATCO when making coordination choices for the ***Subject Flight***, due to the flights' anticipated vertical and lateral profiles. ***Context Flights*** are those ***Environmental Flights*** that are involved in a ***Planning Context Encounter*** with the ***Subject Flight***. Note: ***Context Flights*** may not currently be involved in a ***Planning Encounter*** based on their current clearance or existing coordinated levels.
Environment Trajectory	The ***Trajectory*** of an ***Environmental Flight***
Context Trajectory	***Context Trajectories*** represent the expected utilisation of airspace by each flight. ***Context Trajectories*** are built for the ***Subject Flight*** and ***Environmental Flights***. Note: Context Trajectories are similar to ***Coordination Trajectories***. Each **Context Trajectory** maintains a single level and follows the lateral profile of the **Planned Trajectory**. **Context Trajectories** are built at every standard Flight Level from the entry-context level to the exit-context level. The identification of entry-context and exit-context levels is dictated by the information available in the system at the time of the probe. They represent the lowest and highest level at which the flight is anticipated to occupy in the sector. The Origin and Termination points on ***Context Trajectories*** depend on whether the flight is the ***Subject flight*** or an ***Environmental flight*** and on the flight's anticipated vertical profile. Example of Subject Flight **Context Trajectories**:  Example of Environmental Flight **Context Trajectories**: 
Eligible flight for TRACT	A flight to which the TRACT may send a CTO
User Preferred Route	A preferred route that is provided by an Airspace User during the flight planning and agreement phase. In Step 1 it may take advantage from ***Free Route Airspace (FRA)*** for optimum routings. Note: A User Preferred Route may include published as well as non-published

	points defined in latitude/longitude or point bearing/distance. Such waypoints are inserted in the FMS for trajectory computation
Planning Trajectory Related Terms *Since the needs of the PC and TC differ in many respects, the trajectories produced to support the planning and tactical roles are different.* *Planning Trajectories are used to predict encounters between flights that are of concern to the PC. They take account of the original flight plan, modified by agreed co-ordination constraints and standing agreements, but possibly unconstrained by tactical instructions.*	
Planned Trajectory	The ***Planned Trajectory*** represents the stable medium to long term behaviour of the aircraft but may be inaccurate over the short term where tactical instructions that will be issued to achieve the longer term plan are not yet known. It takes into account the planned route and requested vertical profile, strategic ATC constraints, ***Closed Loop Instructions/Clearances***, co-ordination conditions and the current state of the aircraft. Assumptions may be made to close ***Open Loop Instructions/Clearances*** issued by tactical controllers. It is calculated within the planning look-ahead timeframe, starting from the Area of Interest of the unit concerned, or the aircraft's current position (whichever is later). It is constrained during all phases of flight by boundary crossing targets (e.g. standing agreements between the Units concerned). Note: The ***Planned Trajectory*** supports the ATC planning operations. It is used primarily to support data distribution within the system and in the determination of the top of descent point. As such, uncertainty does not need to be calculated for this trajectory. It is also used as the starting point for derivation of more specific local ATC trajectories.
Planned Sequence Trajectory	A ***Trajectory*** that is derived from the ***Planned Trajectory*** as it follows the vertical and lateral profile of the ***Planned Trajectory***, truncated in time to an adaptable parameter (e.g. 25 minutes). ***Uncertainty*** is added (although the lateral uncertainty may be zero). Note: The Planned Sequence Trajectory is used for the determination of co-ordination levels and the sector penetration sequence. It is used for both manual coordination and integrated coordination purposes and may be used by the CD&R Aid (with the ***Planning Separation***) for traversals of the sector concerned (CD&R for entry and exit to the sector are covered by the ***Coordination Trajectory***).
[Entry/Exit] Coordination Trajectory Or **[Entry/Exit] Trajectory**	A ***Trajectory*** that is derived from the ***Planned Sequence Trajectory.*** It follows the lateral profile of the ***Planned Sequence Trajectory***[2] but maintains a specific coordination level relevant to the boundary between two sectors. It represents the expected behaviour of the aircraft according to the entry/exit co-ordination conditions. **Entry** = A ***Trajectory*** that is built at levels associated with the sector entry coordination for the flight. **Exit** = A ***Trajectory*** that is built at levels associated with ***the sec***tor exit coordination for the flight. Note: The ***Coordination Trajectory***: • Supports both lateral and vertical boundary co-ordinations; • Can have the origin and end truncated (e.g. at sector boundaries); • Is necessary for predicting ***encounters*** with flights that are co-ordinated with the sector but not yet in communication with that sector.

[2] It may be possible for the lateral profile of Coordination Trajectories to be altered from that of the Planning Trajectory to take into account relevant Coordination Constraints applied at the boundary between two sectors.

	Because it is only needed for boundary crossing conditions it can have a relatively short prediction horizon; typically up to the point where the flight is assumed by the sector concerned.
TRACT Trajectory	A ***Trajectory*** that is derived from the ***Planned Trajectory.*** It is similar to the ***Planned Sequence Trajectory*** in that it follows the vertical and lateral profile of the Planned Trajectory, truncated in time to an adaptable parameter (which is suitable for the TRACT process) and ***uncertainty*** is included. Note: It is used in support of the TRACT CD&R process.
Initial Reference Business Trajectory (iRBT for Step 1)	The representation of an airspace user's intention with respect to a given flight, guaranteeing the best outcome for this flight (as seen from the airspace user's perspective), respecting momentary and permanent constraints. The ***Reference Business Trajectory*** (RBT) refers to the Business Trajectory during the execution phase of the flight. It is the Business Trajectory which the airspace user agrees to fly and the Air Navigation Service Providers (ANSP) and Airports agree to facilitate (subject to separation provision) Note: The iRBT is the Step 1 attempt to move towards the full SESAR Reference Business Trajectory. It is shared between the Step 1 SWIM subscribers and is updated from down-linked aircraft trajectory updates. The extent to which this update, synchronisation and sharing is possible within Step 1 will depend on progress made by enabling projects. Likewise the extent to which guarantees can be made concerning best outcome will be subject to the same Step 1 development progress and validation.
Constraint and Target Related Terms	
CTO	An ATM imposed time constraint over a point. Note: This constraint is sent by the ground system to the aircraft.
CTA/RTA	An ATM imposed time constraint on a defined merging point associated with an arrival runway. Note: This constraint is sent by the ground system to the aircraft.
Active CTO/CTA/RTA	A ***CTO*** or ***CTA*** or ***RTA*** that is currently taken into account by both, the avionics (e.g. FMS) and the Ground Systems. Note: It is considered to be active from the moment when both the air and the Ground Systems have taken it into account, until the application point of the constraint is over-flown or until it is cancelled in the Air and the Ground systems.
Level Block	A level or a range of levels that is blocked off to other traffic, e.g. crossers
Target Time of Arrival	An Arrival Time which is not a constraint but a progressively refined planning time that is used to coordinate between arrival and departure management applications. It is an ATM computed time.
Clearance and Instruction Related Terms	
Open loop Instruction/Clearance	An ATC clearance or instruction where a full trajectory extrapolation beyond the point or segment(s) affected is not possible using the normal prediction process, i.e. without special measures to assert a closure condition (e.g. time limit on headings and most probable point of return to original routing). Open loop instructions/clearances can be cancelled by a Closed-loop instruction/clearance. Note: Most tactical instructions/clearances take this form; they include heading (including track offset), level, and speed restrictions and exceptionally could also cover rates of climb or descent.
Closed loop Instruction/Clearance	An ATC clearance or instruction where a full trajectory extrapolation beyond the point or segment(s) affected is possible using the normal prediction process. Note: A typical example is a direct route from one point to another on the original

	route.
NFL, SFL	The NFL is the cleared level that the aircraft will have when it will arrive in the sector. The NFL is given by the upstream sector. The NFL is equal to the TFL of the upstream sector. The SFL is the second level that permits to determine the interval of flight levels in which the aircraft will arrive in the sector. So when arriving in the sector the aircraft will be between the SFL and the NFL.
Data-Link Related Terms	
ETA	Estimated Time of Arrival. The ETA is usually used not only for the arrival (i.e. last point of the Trajectory) but also for the "arrival" on any given trajectory point. In such a case and for Ground systems use only the acronym ETO – Estimated Time Over – should be preferred. In the current document, it is used in Air aspects (e.g. as an item of EPP data) only, although Ground systems namely Ground TP may use this acronym too.
TOAC	Time Of Arrival Control - the function of airborne system providing automatic speed control as to overfly given point on trajectory within given time constraint.
reliable RTA interval	The range of arrival times at a specified lateral fix which are achievable using TOAC function, with a level of confidence of 95% assuming standard meteorological uncertainty as specified in appendix J of WG85 - addendum to document ED75, and margins. This corresponds to the raw [ETAmin,max] amended with margins, and it is downlinked in the ADS-C messages as "ETAmin,max" field.
RTA Tolerance	Time tolerance around CTO/CTA/RTA constrained point defined by ATC in which airborne system overfly this point with 95% probability.

352 ### 1.5.1 Safety Reference Material (SRM)

353 Many of the following definitions are taken from the SRM [1].

Term	Definition
SAfety Criteria	Explicit and verifiable criteria, the satisfaction of which results in acceptable safety following the change. They may be either qualitative or quantitative and either absolute or relative. They include not just specific risk targets but also safety (and other) regulatory requirements, operational and equipment standards and practices
Safety Objective	The functional, performance and integrity safety properties of the air navigation system, derived at the OSED level. Safety objectives describe what the air navigation system has to provide across the interface between the service provider and service user in order that the SAfety Criteria are satisfied. They provide mitigation of the pre-existing risks; and limit the risks arising from failures within the air navigation system. As objectives, they should specify what has to be achieved – how it is achieved is covered by safety requirements – from Article 2(11) of Regulation (EC) No 1035/2011
Safety Requirement	The necessary risk reduction measures identified in the risk assessment to achieve a particular safety objective. They describe the functional, performance and integrity safety properties at the system-design level as well as organisational, operational, procedural, and interoperability requirements or environmental characteristics – from Article 2(12) of Regulation (EC) No 1035/2011
Success Case	The examination of the system from the perspective of its operation under

Term	Definition
	normal and abnormal conditions.
Failure Case	The examination of the system from the perspective of its operation under failure conditions.
Hazard	Any condition, event, or circumstance which could induce an accident. This covers both pre-existing aviation hazards (not caused by ATM/ANS functional systems) and new hazards introduced by the failure of the ATM/ANS functional systems.
Normal conditions	Those conditions of the operational environment the ATM/ANS functional system is expected to encounter in day-to-day operations and for which the system must always deliver full functionality and performance
Abnormal conditions	Those external changes in the operational environment that the ATM/ANS functional system may exceptionally encounter (e.g. severe WX, airport closure, etc.) under which the system may be allowed to enter a degraded state provided that it can easily be recovered when the abnormal condition passes and the risk during the period of the degraded state is shown to be acceptable
Mitigation	Actions taken to alleviate or moderate the severity and/or the frequency of a risk
Functional model	An abstract representation of the design of the ATM/ANS functional system that is entirely independent of the design and of the eventual physical Implementation of the system. The Functional Model (FM) describes what safety-related functions are performed and the data that is used by, and produced by, those safety functions – it does not show who or what performs the safety functions
Implementation	The realisation of design in the form of the built and tested air navigation system prior to its transfer into operational service;
Impact Modification Factors (IM)	An Impact Modification (IM) factor can be applied to the maximum tolerable failure rate to reflect whether the hazard results in for example, impact to 2 aircraft (an IM of 2).
Providence	The 'luck' barrier in the AIM barrier model [3]. Where the conflict is resolved because the two aircraft just happened to miss each other.
Crew Collision Avoidance	The measures within the airborne domain for the resolution of conflicts in the AIM barrier model [3]. These include ACAS and See & Avoid.
ATC Collision Avoidance	The measures within the ground domain for the resolution of conflicts (losses of separation) in the AIM barrier model [3]. These include, ATC expedites, avoiding action and STCA.
Tactical Conflict Management	The measures in the ground domain for the prevention of losses of separation in the AIM barrier model [3] i.e. the tactical controller's role.
Traffic Planning & Synchronisation	The measures in the ground domain for the prevention of conflicts in the AIM barrier model [3] which are part of the planner controller's role.
Demand & Capacity	The measures in the ground domain for the prevention of conflicts which

Term	Definition
Balancing	include controller workload management, sector openings etc.
Airspace Design & Strategic Planning	The measures in the ground domain for the prevention of conflicts in the AIM barrier model. These measures include the design of the airspace and long-term planning of ATCO resource availability etc.
Pre-existing risks	The risks that are inherent in aviation. They are not associated with failure of the air navigation services / system - rather it is the primary purpose of air navigation services to reduce these risks wherever possible
Strategic conflicts	The event occurring when airspace design and strategic planning has failed to resolve the conflict
Pre-tactical conflicts	The event occurring when demand and capacity balancing has failed to resolve the conflict.
Planned conflicts	The event occurring when Traffic Planning and synchronisation has failed to resolve the conflict i.e. the Planner controller's role.
Imminent infringements	The event occurring when ATC tactical conflict management has failed to resolve the conflict i.e. the tactical controller's primary role.
Imminent collisions	The event occurring from the failure of the ATC Collision Avoidance Barrier. Where actions such as STCA, ATC Expedites and Avoiding Action have failed to resolve the conflict.
Collisions	The event occurring when Crew Collision Avoidance techniques such as ACAS, See & Avoid have failed to prevent the conflict.
ATC Induced pre-tactical conflict	A conflict created by an ATC planner action.
Induced conflict	ATM provision creates new risks, due to unplanned aircraft manoeuvres or as a result of ATC actions and these are termed induced conflicts. These are mainly created in the tactical operations and so they by-pass many of the safety barriers. These conflicts can be more difficult to detect and resolve due to their unexpected nature and the time pressure that they are created under.
ATC Induced Conflict	A conflict created by an ATC tactical action.
Pilot Induced Conflict	A conflict created by a pilot action.
Achievable	That safety requirements are capable of being satisfied in a typical ATM/ANS functional system implementation, *i.e.* they do not impose unrealistic expectations on the design comprising people, procedures, hardware, software and airspace design. This includes feasibility in terms of timescale, cost, and technical development
Argument	statement or set of statements asserting a fact that can be shown to be true or false (by demonstration and evidence)
Assurance	The results of all planned and systematic actions necessary to afford adequate confidence an air navigation service or ATM/ANS functional

Term	Definition
	system satisfies the SAfety Criteria – from Article 2(10) of Regulation (EC) No 1035/2011
Evidence	Information that establishes the truth (or otherwise) of an argument. Wherever possible, it should consist of proven facts – e.g., the results of a well-established process such as simulations and testing. Only where such objective information is not available should it be based on expert opinion
Integrity	The ability of a system, under all defined circumstances, to provide all the services (or functions) required by the users, with no unintended or un-commanded services (or functions). It is based on the logical completeness and correctness, and reliability, of the ATM/ANS functional system elements in relation to user / operator requirements
Rationale	The explanation of the logical reasons or principles employed in consciously arriving at a conclusion concerning safety. Rationales usually document (1) why a particular choice of argument was made, (2) how the basis of its selection was developed, (3) why and how the particular information or assumptions were relied on, and (4) why the conclusion from the evidence is deemed credible or realistic
Risk	The combination of the overall probability, or frequency of occurrence of a harmful effect induced by a hazard and the severity of that effect – as defined in Article 2(9) of Regulation (EC) No 1035/2011;
Risk Assessment	A sub-process in the overall safety management process to determine a priori the quantitative or qualitative value of risk related to the provision of air navigation services for a specific operational environment
Safety Performance	The performance of relevant and measurable safety indicators whereby the required SAfety Criteria will be fully achieved and maintained during the operational lifecycle
Specification	The ATM system has to provide across the interface between the service provider and service user in order that the User Requirements can be satisfied – *i.e.* a specification takes a "black-box" view of the system, at the OSED level
User Requirements	User(s) in this context are the user(s) of the air navigation service(s) concerned. In general, User Requirements are what the Users want to have happen in their domain of operation. From a safety viewpoint, the User Requirements are generally the SAfety Criteria
Validation	An iterative process by which the fitness for purpose of a new system or operational concept being developed is established (from E-OCVM 3)
Verification	Satisfaction of safety requirements can be demonstrated by direct means (e.g. testing, simulations, modelling, analysis, etc.), or (where applicable) indirectly through appropriate assurance processes

354

355

1.5.2 Others

Term	Definition
Open loop clearance	A clearance is an open loop clearance when it is not possible to determine the complete new trajectory from the instruction issued. A further instruction is needed to complete the information necessary to determine how the flight will resume its normal, planned navigation.
Closed loop clearance	A closed loop clearance is the opposite of an open loop clearance. It allows the trajectory to be determined beyond the end of the constraint as the duration of the constraint is known.
Environmental Trajectory	The [generic] trajectory of an Environmental Flight.
Airspace of interest	Airspace covered by the group of sectors using the PC aid.
Eligible Sector	The sector which currently has eligibility to make tactical inputs for a particular flight.
Background Track	A radar track for a flight that is known to the system and has not been identified as of interest at a sector or sector combination. The sector will not be identified on the co-ordination sector sequence.

356

357

1.6 Acronyms and Terminology

Term	Definition
2D, 3D, 4D	*Two Dimensional, Three Dimensional, Four Dimensional*
4D TM	*Four dimensional Trajectory Management*
4DTRAD	*Four Dimensional TRAjectory Data link*
A/C	*Aircraft*
ACARS	*Aircraft Communications Addressing and Reporting System*
ACAS	*Airborne Collision Avoidance System*
ADS-B	*Automatic Dependent Surveillance-Broadcast*
ADS-C	*Automatic Dependent Surveillance-Contract*
AIM	*Accident Incident Model*
AMAN	*Arrival MANager*
ANSP	*Air Navigation Service Provider*
AOC	*Airlines Operations Centre*
ATC	*Air Traffic Control*

Term	Definition
ATCO	*Air Traffic Controller*
ATIS	*Automatic Terminal Information Service*
ATM	*Air Traffic Management*
ATN	*Aeronautical Telecommunications Network*
ATSAW	*Air Traffic Situational Awareness*
CD/R	*Conflict Detection and Resolution*
CDPS	*Central Data Processing System*
CFL	*Cleared (Current) Flight Level*
CNS	*Communications, Navigation and Surveillance*
CPDLC	*Controller-Pilot Data Link Communication*
CTA	*Controlled Time of Arrival*
CTO	*Controlled Time Over*
CMT	*Monitoring Aid*
CRD	*Conflict Risk Display*
CWP	*Controller Working Position*
DCB	*Demand and Capacity Balancing Barrier*
DFS	*Deutsche Flugsicherung GmbH (German ANSP)*
DSNA	*Direction des Services de la Navigation Aérienne (Directorate Air Navigation Services) (French ANSP)*
DSNA	*French Aviation Authority*
EC	*European Commission*
E-OCVM	*European Operational Concept Validation Methodology*
ECAC	*European Civil Aviation Conference*
EPP	*Extended Projected Profile*
ETA	*Estimated Time of Arrival*
EUROCAE	*EURopean Organization for Civil Aviation Equipment*
FCSO	*Failure Case Safety Objective*

Term	Definition
FDPS	*Flight Data Processing System*
FHA	*Functional Hazard Assessment*
FIS	*Flight Information Service*
FL	*Flight Level*
FMS	*Flight Management System*
FPM	*Flight Path Monitoring*
FRA	*Free-Route Airspace*
GA-VLJ	*General Aviation - Very Light Jet*
HDG	*Heading*
HMI	*Human-Machine Interface*
HP	*Human Performance*
i4D TM	*Initial 4-Dimensional (Trajectory Management)*
iFACTS	*interim Future Area Control Tools*
IBP	*Industrial Based Platform*
ICAO	*International Civil Aviation Organisation*
IFR	*Instrument Flight Rules*
IOP	*Interoperability*
iRBT	*initial Reference Business Trajectory*
IRM	*Interim Risk Module*
iTEC	*interoperability Through European Collaboration*
JAR	*Joint Aviation Requirements*
MASPS	*Minimum Aviation System Performance Specification*
MAC-ER	*Mid-Air Collision En Route*
MET	*METeorological services*
MONA	*MONitoring Aids*
MTCD	*Medium-Term Conflict Detection*
NATS	*National Air Traffic Services (UK ANSP)*

Term	Definition
NFL	*eNtry Flight Level*
OFA	*Operational Focus Area*
OR	*Operational Requirement*
OSED	*Operational Service(s) Environmental Description*
PSSA	*Preliminary System Safety Assessment*
PXX.XX.XX	*Project PXX.XX.XX.*
PC	*Planning Controller*
RBT	*Reference Business Trajectory*
RNAV	*Area Navigation*
RNP	*Required Navigation Performance*
R/T	*Radio Telephony*
RTA	*Requested Time of Arrival*
RVSM	*Reduced Vertical Separation Minimum*
SAC	*SAfety Criteria*
SAR	*Safety Assessment Report*
SESAR	*Single European Sky ATM Research Programme*
SCSO	*Success Case Safety Objective*
SDPS	*Surveillance Data Processing System*
SFL	*Supplementary Flight Level*
SPR	*Safety and Performance Requirements*
SRM	*Safety Reference Material*
STCA	*Short-Term Conflict Alert*
SVFR	*Special Visual Flight Rules*
SWIM	*System Wide Information Management*
TAWS	*Terrain Awareness and Warning System*
TC	*Tactical Controller*
TC-SA	*Trajectory Control by Speed Adjustment*

Term	Definition
TDB	*Track Data Block*
TRACT	*TRajectory Adjustment through Constraint of Time*
TMA	*Terminal Manoeuvring Area*
TEMSI	*Temps Significatif (French weather forecasting map)*
TFL	*Transfer Flight Level*
TP	*Trajectory Prediction*
VALR	*Validation Report*
VFR	*Visual Flight Rules*
WG	*Working Group*
WX	*Weather*

1.7 References

[1]. SESAR P16.06.01, Task T16.06.01-006, SESAR Safety Reference Material, Edition 00.02.02, 10th February 2012

[2]. SESAR P16.06.01, Task T16.06.01-006, Guidance to Apply the SESAR Safety Reference Material, Edition 00.01.02, 10th February 2012

[3]. AIM model, v0.2 June 2012 (Note the original assessment was conducted using V0.1 and updated as part of the offline analysis).

[4]. WP4.07.02, OSED_4, D28, 00.01.00

[5]. D09.01_Aircraft and System Performance and Functional requirements, 05/09/2012

[6]. SESAR WP9.1 D07 Final Safety Assessment Report_4, 19/11/2012

[7]. RTCA DO-236B. Minimum Aviation System performance Standards: Required Navigation Performance for Area Navigation. October 2003.

[8]. JAA TGL6 Administrative and Guidance Material "Guidance Material on the Approval of Aircraft and Operators for Flight in Airspace above Flight Level 290 where a 300M (1,000 ft) Vertical Separation Minimum is applied

[9]. EUROCONTROL Initial 4D – 4D Trajectory Data Link (4DTRAD) Concept of Operations. December 2008.

[10].RTCA SC-214/EUROCAE WG-78. http://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/techops/atc_comms_services/sc214/current_docs/version_l_m/, September 2013.

[11].WP4.07.02, Development and Validation Plan_3, D27, 00.01.02

[12].WP4.07.02, V2 Validation Report (VALR), D05, 01.00.01

[13].WP4.07.02, V2 Validation Report Iteration 2 (VALR), D18, 00.01.01

[14].WP4.07.02, Project CATO – Requirements Specification Release 6/Final for Industrial Prototype, Version 1.0

[15].WP4.07.02, Validation Report_3, D09, 00.01.02

[16].WP4.07.03, Validation Report_4, D21, 00.00.03

[17].WP4.07.02, Final MTCD/TCT Safety and Performance Requirements_4, D23, 00.04.00

2 Safety specifications at the OSED Level

2.1 Scope

Section 2 addresses the following activities:

- Description of the key properties of the Operational Environment that are relevant to the safety assessment - section 2.2.
- Identification of the pre-existing hazards that affect traffic in the En Route environment and the risks of which services provided by the "Conflict Detection, Resolution and Monitoring" concept may reasonably be expected to mitigate to some degree and extent and the description of the airspace user requirements – sections 2.3 and 2.4.
- Derivation of suitable Safety Criteria – section 2.5.
- Description of the Air Traffic Services (ATS) to be provided by the "Conflict Detection, Resolution and Monitoring" systems and the derivation of Functional Safety Objectives in order to mitigate the pre-existing risks under normal operational conditions - section 2.6.
- Assessment of the adequacy of the services provided by the "Conflict Detection, Resolution and Monitoring" concept under abnormal conditions of the Operational Environment – section 2.7.
- Assessment of the adequacy of the services provided by the "Conflict Detection, Resolution and Monitoring" concept under internal-failure conditions and mitigation of the system-generated hazards – section 2.8.
- Assessment of the impacts of the "Conflict Detection, Resolution and Monitoring" operations on adjacent airspace or on neighbouring Air Traffic Management (ATM) systems – section 2.9.
- Achievability of the Safety Criteria – section 2.10.
- Validation & verification of the safety specification – section 2.11.

2.2 "Conflict Detection, Resolution and Monitoring" - Operational Environment and Key Properties

This section describes the key properties of the Operational Environment that are relevant to the safety assessment. This information is mainly obtained from the OSED [4], sections 4.1.1, 4.1.2, 4.1.3, 4.1.4 and 4.1.5.

2.2.1 Airspace Structure, Type and Boundaries

The Airspace considered by P04.07.02 is a **managed airspace** (free route and fixed route), where a separation service will be provided.

In such airspace the role of the separator may in some cases be delegated to the pilot. However, this capability is out of the P04.07.02 scope.

The vertical scope considered by P04.07.02 extends from FL195 up to FL660. The airspace in the Terminal Manoeuvring Area (TMA) is not considered by P04.07.02.

The airspace is Reduced Vertical Separation Minima (RVSM) up to FL410.

The Class of Airspace is "**Class C**" or above:

Operations may be conducted under Instrument Flight Rules (IFR), Special Visual Flight Rules (SVFR), or Visual Flight Rules (VFR). All flights are subject to Air Traffic Control (ATC) clearance. Aircraft operating under IFR and SVFR are separated from each other and from flights operating

under VFR. Flights operating under VFR are given traffic information in respect of other VFR flights. (ICAO definition).

The Airspace is divided into separate areas of responsibility (Sectors). The sectors may be grouped together when traffic is low enough and they will be de-grouped when traffic increases. This is operated by the Operational Supervisor on operational criteria.

2.2.2 Airspace Users (Flight Rules), Traffic Levels and complexity

Traffic characteristics will vary by airspace type:

- Upper Airspace e.g. above FL285: Mainly overflights with very little vertical change;
- Lower Airspace e.g. under FL285: A mix of overflights and descending/climbing aircraft depending on the sector. A higher proportion of airfield inbounds and outbounds to both airfields within and outside the sector of interest.

In the most-likely scenario there will be 16.9 million IFR movements in Europe by 2030, 1.8 times more than in 2009.

During the time frame of the Single European Sky ATM Research Programme (SESAR) Step 1, the future European airspace organisation will initially be based on current ICAO ATS airspace classifications, regulations and applicable rules, including VFR and IFR.

Classifications and rules will be adopted consistently by all States, thus ensuring uniformity of their application and a simplification of airspace organization throughout the whole European Civil Aviation Conference (ECAC) region.

This will provide a progress towards an airspace continuum where the only distinction is between two Airspace classes (i.e. Managed and Unmanaged Airspace). However, this will not be achieved in SESAR Step 1.

Airspace use will be optimised through dynamic demand and capacity management, queue management, flexible military airspace structures, free, direct and fixed routing and a reduced number of airspace categories. The objective is to have an airspace organisation that:

- Is as transparent and simple as possible with regard to user perception;
- Permits unambiguous rules for ATS service provision;
- Allows simple documentation of the requirements for aspects such as flight planning, airspace reservations, communication actions and minimum equipage.

2.2.3 Aircraft ATM capabilities

The aircraft capabilities will remain heterogeneous in the target environment. They will cover a range from existing capabilities and standards as described in the Minimum Aviation System Performance Specification (MASPS), to the initial four dimensional (i4D) capabilities as described in the P09.01 deliverables ([5] and [6]).

The EURopean Organization for Civil Aviation Equipment (EUROCAE) WG85 4D Navigation is currently working on an addendum version to DO236B/ED75 [7] for Estimated Time of Arrival (ETA) and Time Of Arrival Control (TOAC) functions. It will be further used as an addendum to the Minimum Aviation System Performance Specification (MASPS) for area navigation systems operating in a Required Navigation Performance (RNP) environment (limited to RNP-4 RNAV or smaller environments). The results from operational testing (namely in the P9.1 framework) are expected to be used as feedback for further Working Group (WG) 85 iterations before an official release.

It is assumed that the highest level of aircraft capabilities available in Time Based Operations (SESAR step1) can be summarized as follows:

- **Data link**:
  - Controller-Pilot Data Link Communication (CPDLC) and Automatic Dependent Surveillance-Contract (ADS-C) for ATC via Airborne Collision Avoidance System

(ACARS) (oceanic flights) and via Aeronautical Telecommunications Network (ATN) (continental flight) (ED122, ED 100A for FANS 1/A+, ED 110B/120 for continental Europe ATN B1);

- Flight Information Service (FIS): Automatic Terminal Information Service (ATIS) with ATC via ACARS;
- METeorological services (MET) data (winds/temperatures, TEMSI, etc.) with Airlines Operations Centre (AOC) via ACARS.

- **Navigation** (figures currently being assessed by WG85):
  - 2D RNP1 in en route and 2D RNP0.3 in approach (2D RNP means lateral containment i.e. not only a required accuracy but also a required integrity and continuity, e.g. the aircraft will remain within +/-1nm 95% of the time and within +/-2nm 99,99% (10^{-7}) of the time for RNP1);
  - Concerning the vertical dimension, the following is required in [8] section 7 "RVSM performance" JAR 25.1325(e) : "*Each system must be designed and installed so that the error in indicated pressure altitude, at sea-level, with a standard atmosphere, excluding instrument calibration error, does not result in an error of more than ± 30 ft per 100 knots speed for the appropriate configuration in the speed range between 1.3 VS0 with wing-flaps extended and 1.8 VS1 with wing-flaps retracted. However, the error need not be less than ± 30 ft*";
  - A time constraint (RTA) is achieved with an accuracy of at least +/-30 seconds for En RouteEn Route operations and at least +/- 10 seconds for arrival operations in the terminal area 95% of the time; with no wind and temperature error the time estimates accuracy is around 1% of Time To Go for open loop time control function, e.g. +/-15 seconds at 25 minutes. It is to be noted that these statements are guaranteed only in i4D operational conditions, i.e. end of cruise and descent approach (excluding fixes from decelerate to threshold runway).
- **Surveillance**:
  - ADS-B in/out via Mode S 1090 transponder and Air Traffic Situational Awareness (ATSAW) applications;
  - Terrain Awareness and Warning System (TAWS);
  - Airborne Collision Avoidance System (ACAS) for the safety net.

The focus here is mainly on Commercial aircraft (legacy, low fare, regional) and on Business aircraft[3].

There is generally less capability for General Aviation - Very Light Jet (GA-VLJ) Helicopter and Military aircraft (data link alike, FMS alike, ACAS for transport only).

2.2.4 Communications, Navigation and Surveillance (CNS) Aids

In P04.07.02, the key area of improvement within CNS is Communication. Voice and data exchanges between service actors within the system are expected to improve. For example, TRACT will reduce the number of voice communications between controller and the aircrew through automatic silent coordination.

Other items are less suited to P04.07.02:

- Navigation technologies that enable precision positioning are primarily designed for Lower Airspace. Of course, with RNP the ability to offset and design routes with reduced spacing between centrelines would benefit all airspace. However, it does not specifically impact the P04.07.02 concept;

[3] Mainline and BGA equipage level can be very different

519 • Surveillance technologies are globally important but no feature is specific for P04.07.02
520 matter.

521 2.2.5 Separation Minima

522 Separation minima are expected to continue to be based on guidance, regulations, and factors used
523 in today's environment (ICAO Doc 4444 Procedures for Air Traffic Management, especially
524 Chapter 5):

525 • Vertical separation: FL< 410 → 1000ft separation (RVSM);
526 • Horizontal separation: En Route Radar Separation: 5NM.

527 The radar separation standard may not be constant throughout the En Route sectors. Different
528 separation standards might be required e.g.:

529 - A non-RVSM flight that is authorized to fly within a RVSM airspace remains subject to separation
530 standard that is applicable below the RVSM limit (i.e. in a non-RVSM airspace);

531 - At the edges of multi-radar cover or in the case of a reduction in radar service where the radar
532 separation minimum may be increased to 10 NM;

533 - The TMA sectors that interface the lower En Route sectors may be operating a lower radar
534 separation standard (procedures ensure that the separation is established prior to transfer of
535 control in this case).

536 Therefore the choice of separation standard is made on a case-by-case basis depending on both the
537 pair of elements to assess and the airspace where the separation is assessed, and it may not be
538 homogeneous throughout the whole controlled sector.

539 2.2.6 Operational services

540 P04.07.02 is based on a combination of the following separation services:

541 • Service "TRajectory Adjustment through Constraint of Time (TRACT)";
542 • Service "CD/R Aid to the PC";
543 • Service "CD/R Aid to the TC".

544 2.3 Airspace Users Requirements

545 P04.07.02 is based on a combination of the following separation services:

546 • TRajectory Adjustment through Constraint of Time (TRACT) – V2,
547 • Conflict Detection and Resolution Aid to PC (CD/R aid to PC) – V2,
548 • Conflict Detection and Resolution Aid to TC (CD/R aid to TC) – V3.

549 Any combination of these services may be rendered together. In the case where all three services
550 are combined, they would roughly articulate with each other as follows:

551 • The TRACT detects potential conflicts (e.g. 25 minutes ahead) and attempts to resolve them
552 through CTO that should be achievable though small speed changes of the relevant aircraft;
553 • The list of potential conflicts that have been resolved by TRACT is input into the CD/R aid to
554 PC tool for information. This service then detects encounters and it provides the PC with the
555 list of remaining potential encounters that should be handled by her/him and/or the TC. Using
556 her/his aid tool, the PC elaborates solutions that s/he either implements through the
557 Coordination process, or proposes to the TC or sends directly to the aircraft if s/he has the
558 ability to do so;
559 • The list of potential conflicts that have been resolved by the PC and TRACT are input into the
560 CD/R aid to TC tool for information. This service then detects encounters and it provides the
561 TC with the list of remaining potential encounters that s/he should handle. Using her/his aid
562 tool, s/he elaborates solutions and sends them to the relevant aircraft.

This safety assessment report will show the safety benefits the three operational services described above are bringing to the ATM system.

A detailed Benefit and Impact Mechanism study is included in the 4.7.2 VALP [11], appendix F.

2.4 Relevant Pre-existing Hazards

For an ATM system, the pre-existing hazards are those that are inherent in aviation and for which the ATM system needs to provide as much mitigation as possible. These pre-existing hazards are associated with pre-existing risks, which are the risks that would be associated with them in the absence of any ATM service.

Table 2 Pre-existing Hazards shows the pre-existing hazards identified for the "Conflict Detection, Resolution and Monitoring" system.

Pre-existing Hazard [Hp]	Description
Hp#1	Conflicts between pairs of trajectories / clusters
Hp#2	Controlled flight towards terrain or obstacles
Hp#3	Aircraft entry into unauthorised areas
Hp#4	Aircraft encounters with severe weather conditions
Hp#5	Aircraft encounters with wake vortices

Table 1 Pre-existing Hazards

2.4.1 Pre-existing Hazards for TRACT

The impact of TRACT on the pre-existing hazards was examined and the results are recorded below.

Hp#1: TRACT will have a clear safety impact on conflicting pairs of trajectories and if implemented as conceived it should result in an overall safety benefit.

Hp#2: The adjustments made by TRACT are limited to existing flight plans so should have no impact on the likelihood of a controlled flight towards terrain or obstacles.

Hp#3: There is a theoretical impact on the likelihood of an aircraft entry into unauthorised areas due to an aircraft arriving slightly later or earlier at the CTO. It was agreed, however, that these timing differences will be so small (in relation to the timescales of the airspace changes) such that they can be considered to have a negligible impact.

Hp#4: The TRACT speed adjustments would not have any impact on the likelihood of severe weather encounters. The avoidance of severe weather is not accounted for when computing resolutions.

Hp#5: The TRACT speed adjustments would not have any impact on the likelihood of aircraft encounters with wake vortices. Wake vortices or aircraft categories are irrelevant when computing resolutions.

As can be observed, only "Conflicts between pairs of trajectories" (Hp#1) is considered to be impacted by TRACT.

2.4.2 Pre-existing Hazards for CD/R aid to PC

The five pre-existing hazards described in section 2.4 were reviewed for CD/R for PC. It was agreed that CD/R for PC would only impact on conflicts between pairs of trajectories (Hp#1).

2.4.3 Pre-existing Hazards for CD/R to TC

The five pre-existing hazards described in section 2.4 were reviewed for CD/R for TC. It was agreed that CD/R for TC would only impact on conflicts between pairs of trajectories (Hp#1).

2.5 SAfety Criteria (SAC)

The safety activities performed in deriving the SACs were performed in accordance with 16.06.01 guidance material [2].

2.5.1 Introduction

As part of WP4.7.2 Task 20 (V2 phase), a workshop was held to review the material that was produced for the Task 8 (V1) Deliverable during the V1 phase, and to amend to the material where necessary.

The specific objectives of the workshop were as follows:

- To revisit the process and methodology behind the Safety Assessment
- To revisit the following for each of the 04.07.02 Concepts:
    - Assumptions and Architecture of the concept
    - Success Case Safety Objectives
    - Review of Hazard Identification
- Identification of Abnormal Scenarios and any additional Success Case Safety Objectives (SCSO's) required to mitigate against these (this was performed as a post workshop activity but has been recorded here)

The detailed descriptions of the identified SACs below make reference to events within the Accident Incident Model (AIM) [3].

Note the SACs were reviewed following the VP-501 (V3 – as part of P04.07.02) and VP-798 (V3 as part of P04.03) exercises. No changes were necessary.

2.5.2 Scope

The initial workshop was conducted as part of Task 8 (V1) and the associated SACs were limited to the first build of 04.07.02 (denoted Build 1) which is dedicated to separation management with ATM service level 2 capabilities. As described above, a further safety workshop was conducted in the second iteration (Build 2) to review the SACs in light of the concept developments since the SACs were derived. As a result the SACs were updated.

It was expected that the output of this workshop (Build 2) be directly input to the validation activities so that a direct measure of the safety benefits or detriments of each separation service can be established during the exercises. However the validation plans were already mature before this task was undertaken.

2.5.3 Attendees of the Workshop

Name	Organisation	Role
[redacted]	Helios (representing NATS)	[redacted]
	Think Research (Representing NATS)	

[redacted]	DSNA	[redacted]
	NATS	
	NATS	
	DFS	
	DSNA	

Table 2 Task 20 workshop participants

2.5.4 Derivation of SAfety Criteria

Based on the list of pre-existing hazards, it can be concluded that the relevant type of accident is the Mid-Air Collision for all three operational services. This is depicted by SESAR Project 16.06.01 as an Accident Barrier Model, refer to Figure 6 Mid-Air Collision Barrier Model. The barriers were analysed further to identify the SACs for the change.

The SACs presented in sections 2.5.4.1, 2.5.4.2 and 2.5.4.3 were derived by analysing, with respect to each type of relevant accident:

- The contribution to aviation safety of the ATM services;
- The potential impact of the change on that contribution (indicated in red text for increased risk impact, green text for reduced impact, grey text for no impact); a SAfety Criteria is defined only when potential for impact is identified.

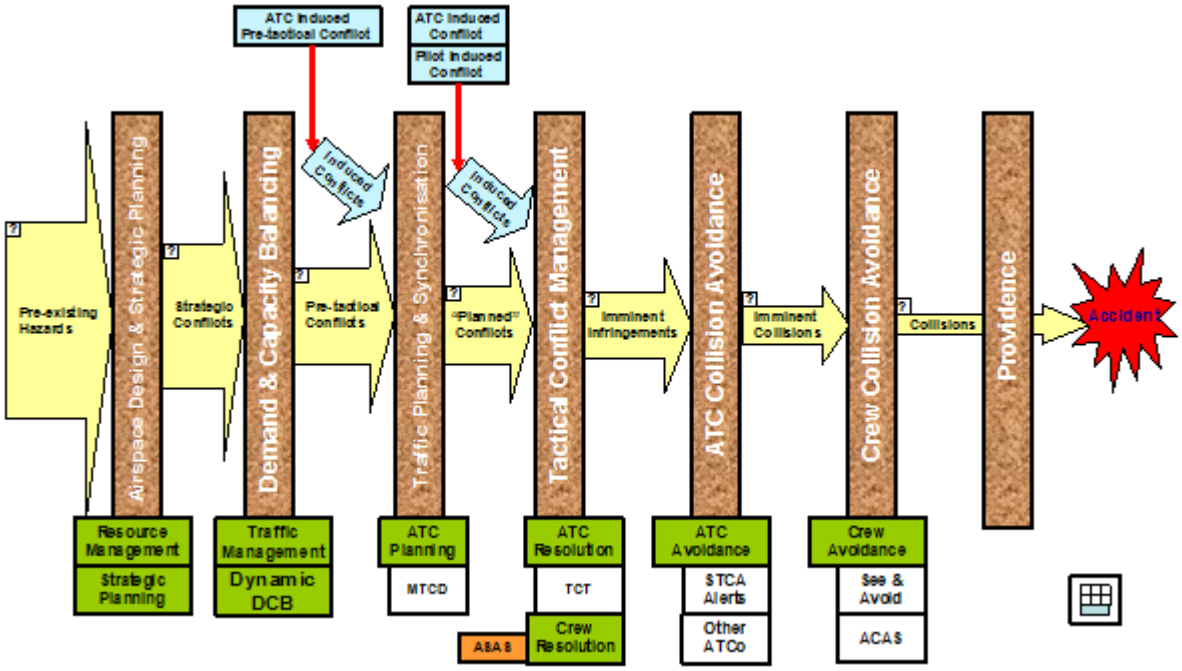


Figure 6 Mid-Air Collision Barrier Model

2.5.4.1 Safety Criteria related to TRACT

2.5.4.1.1 The Barrier Model (Service Level) – Mid-Air Collision

Airspace Design & Strategic Planning Barrier

No impact.

Demand and Capacity Balancing Barrier (DCB)

No impact for Build 1, provided dynamic DCB remains outside the scope of the Build 1 implementation of TRACT.

Traffic Planning & Synchronisation Barrier (TRACT introduces a new airborne pre-tactical de-confliction component within this barrier).

SAC31 – There shall be 3.3% reduction in the number of Pre-Tactical conflicts.

The primary objective of TRACT is to ensure that aircraft flights are adjusted and de-conflicted so that they do not require planner or tactical resolution. As a consequence, TRACT will have a safety benefit in the removal of pre-tactical conflicts. Reviewing the AIM [3] reveals that a new event MB9.2.2c "TRACT fails to resolve conflict" is required which will account for this safety benefit.

TRACT introduces additional uncertainty to the timings regarding aircraft trajectory (MB10.1.1.1.2)

ATC Induced Pre-Tactical Conflict

SAC32 – There shall not be an increase in the number of ATC Induced Pre-Tactical conflicts.

There is a risk that TRACT in some situations causes induced conflict because TRACT introduces additional uncertainty to the timings regarding aircraft trajectory, and there is a period where the instruction has been issued (from TRACT), but not accepted and displayed to the controllers. To be validated.

When solving a conflict, TRACT may fail to take into account all aircraft that are predicted to be within the wider region. This may create TRACT induced conflicts and result in a safety detriment. Additionally, the number of planner options immediately available to the controller is expected to be reduced as a result of TRACT. This may result in induced pre-tactical conflicts (despite the fact that aircraft under TRACT can be overridden). These safety detriments are expected to the very small in comparison to the improvements provided by the safety benefit above (except perhaps near to TRACT boundaries) therefore it was not considered necessary to identify affected events in the AIM model.

Tactical Conflict Management Barrier

SAC33 – There shall be no increase in the number of Imminent Infringements [losses of separation in NATS terminology]

Those conflicts remaining may be more difficult to resolve since those that are simple to solve will be the subject of TRACT resolutions. This will result in a safety detriment, the extent of which may be sector dependent and difficult to estimate. It is therefore important to ensure that TRACT does not result in the creation of any more conflict events (MB5.1.3.1 – "ATCO misjudgement of separation").

It is possible that aircraft under TRACT may be unpredictable due to the different speed adjustment options available to resolve the CTO which are dependent on when the speed adjustment is implemented and completed. This would result in a safety detriment that could be amplified by the pilot selecting manual mode. However, it is an assumption (Assumption 019 in Table 28 Assumptions made in deriving the above Safety Requirements - TRACT) that the FMS adjustments are implemented in such a way that they do not impede the predictability of aircraft trajectories which will aid controller situation awareness.

ATC Induced Tactical Conflict

SAC34 There shall be no increase in ATC induced Tactical Conflicts.

Less ATC interventions will be necessary. There is therefore less chance of either incorrect or untimely instructions or knock-on conflicts being generated. This should result in a reduced frequency of MF7.1.1 Conflict due to missing or incorrect timing of instructions,

MF7.1.3 – "Conflict due to bad Instructions given to pilot" and MF7.1.4 – "Conflict resolution leads to knock-on conflict".

Pilot Induced Tactical Conflict

No impact expected since CTO can only be applied in stable flight (Build 1)[4] and is therefore unlikely to result in high workload. The number of CTOs that can be initiated for a single flight is also limited. Furthermore, the ground systems validate the CTO from the FMS. No impact on pilot error is therefore expected.

ATC Collision Avoidance

No impact expected since the completion of the TRACT (by 6 minutes at the latest) is outside the collision avoidance window.

Crew Collision

No impact expected, pilots will continue to follow standard procedures.

2.5.4.2 Safety Criteria related to CD/R aid to PC

2.5.4.2.1 The Barrier Model (Service Level) – Mid-Air Collision

Airspace Design & Strategic Planning Barrier

No impact.

Demand and Capacity Balancing Barrier

No impact.

Traffic Planning & Synchronisation Barrier

SAC22 – There shall be 36% reduction in the number of Planned Tactical conflicts.

The "What-If" and "What-Else" tools provide the controller with medium term conflict detection and resolution functionality and improve the quality of planning data. These are expected to provide significant safety benefits through a reduction in the number of planned conflicts. This is expected to reduce the failure frequency of event MB9.2.2b.1 - "Failure to identify conflict or traffic peak".

It is also expected that the planner controller will be able to address planning conflicts much earlier than before and prioritise planning actions. This is expected to reduce the failure frequency of event MB9.2.2b.2 "Misjudge conflict resolution".

It should be noted that there may be the potential for the tactical controller to support the planner in undertaking the planning role. This would have the effect of further reducing planned tactical conflicts especially in the case when the planner has a high workload. However, this is likely to occur when the tactical controller is also under high workload due to the planner's inability to deal with the approaching traffic. It is currently unclear as to the extent that this merging of roles will be employed and as such no safety detriment or benefit has been envisaged.

ATC Induced Pre-Tactical Conflict

SAC21 – There shall be a 12% reduction in the number of ATC Induced Pre-Tactical conflicts.

The "What-Else" tool will also reduce the likelihood of misjudgement error since it provides support in the resolution of conflicts and will reduce the likelihood of a knock-on planned conflict. This is expected to reduce the failure frequency of events MF9.1.1 - "Pre-Tactical Conflict generated from other sector" and MF9.1.2 - "Conflict resolution leads to knock-on Pre-Tactical conflict".

[4] For example, far enough from the Top of Descent and before the 4D AMAN horizon (farther than 200-300NM from destination airport with 4D coordination).

Tactical Conflict Management Barrier

No impact, except that the tactical controller may also reduce the number of planned conflicts (see SAC22 justification).

ATC Induced Tactical Conflict

No impact.

Pilot Induced Tactical Conflict

SAC23 – There shall be 7% reduction in the number of Pilot Induced Tactical conflicts.

The Conformance Monitoring Tool (CMT) will detect whether exit conditions can actually be achieved based on aircraft performance. This is expected to reduce the failure frequency of crew induced conflicts; MF6.1.2.2 - “Conflict due to Lateral Deviation”, MF6.1.2.3 - “Conflict due to Speed Deviation” and MF6.1.2.4 - “Conflict due to V.Rate Deviation”.

ATC Collision Avoidance

No impact, existing procedures apply.

Crew Collision

No impact expected, pilots will continue to follow standard procedures.

2.5.4.3 Safety Criteria related to CD/R aid to TC

2.5.4.3.1 The Barrier Model (Service Level) – Mid-Air Collision

Airspace Design & Strategic Planning Barrier

No impact.

Demand and Capacity Balancing Barrier

No impact.

Traffic Planning & Synchronisation Barrier

No impact.

ATC Induced Pre-Tactical Conflict

No impact.

Tactical Conflict Management Barrier

SAC11 – There shall be 21% reduction in the number of Imminent Infringements

The What Else tool will improve the resolution of conflicts which is expected to reduce the failure frequency of event MB4.1.2.2 “Inadequate information for conflict management”.

The conformance monitoring tool will improve the detection of non-adherence to clearances which is expected to reduce the failure frequency of event MB4.3 “Inadequate Pilot Response to ATC”.

Furthermore, CD/R for TC will improve the team working between the planner and the tactical. This will mean that for sectors where there is a limited planning function the planner will be able to provide resolution advice to the tactical. This will reduce the failure frequency of events and MB4.2.1 - “ATCO misjudgement of separation” and MB4.2.2 - “ATCO failure to act”.

SAC12 – There shall be 30% reduction in the number of Tactical conflicts.

The “What if” and “What else” functions make the controllers more likely to identify conflicts and resolve them with better information about the nature of the conflict. Related aim barriers:

MBX1.3.1 ATCO misjudgement of separation

MBX.1.2.3 Failed to Detect Conflict

MBX1.1.1 Inadequate traffic picture

MBX.1.3.1 ATCO misjudgement of separation

MBX.1.3.2 ATCO failure to act

ATC Induced Tactical Conflict

SAC13 – There shall be 41% reduction in the number of ATC Induced Tactical conflicts.

The "What else" tool will also reduce the likelihood of induced conflicts since it provides the controller with a view of all the predictable knock-on conflicts. This is expected to reduce the failure frequency of event MF7.1.4. "Conflict resolution leads to knock-on conflict".

Pilot Induced Tactical Conflict

SAC14 – There shall be 28% reduction in the number of Pilot Induced Tactical conflicts.

The conformance monitoring tool will detect misjudgement error since it provides support in the resolution of conflicts and will reduce the likelihood of a knock-on planned conflict. This will strengthen the barrier "BY Ground/Air Trajectory Deviation Alerting".

ATC Collision Avoidance

SAC15 – There shall be no increase in the number of Near Collisions.

It should be noted that there could be a safety detriment to the "What else" tool if it was to overlap potential conflicts with STCA. The result could be two tools based on different data presenting a conflicting picture that could be confusing to the controller. Provided that STCA and CD/R for TC will be independent, this safety detriment can be discounted.

There may be some safety gain from the redundancy in the alerting which is introduced by having independent TC-Aid and STCA. However, this gain is believed to be offset by the confusion from inconsistency of alerting. This is reflected in the SAC which sets an expectation of 'no worse than today'.

Crew Collision

No impact expected, pilots will continue to follow standard procedures.

2.6 Mitigation of the Pre-existing Risks – Normal Operations

2.6.1 Derivation of Safety Objectives for Normal Operations

Following the SAfety Criteria (SAC) Derivation, the workshop performed the preliminary work of the Success Case Analysis. The Success Case Analysis considered the services when working as intended, and identified the requirements that need to be placed for the services to deliver their safety benefits (as defined by the SAC).

The Success Case Analysis workshop has been done in two steps, i.e. reviewing and updating the work done during V1 (Task 8) based on which the safety requirements have been developed during the V2 (Task 20) activities. This is further explained in the following sections.

Note the SACs were reviewed following the VP-501 (V2 – as part of P04.07.02) and VP-798 (V2 as part of P04.03) exercises. No changes were necessary.

Task 8 (V1)

The overall objective of the Success Case workshop was to provide the Task 8 (V1) team with a foundation upon which to perform the Success Case Analysis.

This objective was broken down into the following:

- Reviewing and developing the Functional Model (which includes the functional blocks). The functional blocks described the services from a functional perspective, enabled the completeness of the Operational Requirements (ORs) to be assessed, and provided a reference for the safety requirements to be described against. Note the Functional Model is not present in this document since the concept is sufficiently mature to use the SPR-level Model directly.

- Reviewing and discussing different scenarios (presented in A.1) for each of the services. The various possible scenarios in which the services could operate were explored and the

boundary between the Success and Failure cases was established. The scenarios also helped to confirm the completeness of the ORs.

Following the workshop the ORs were reviewed, and:

- Any missing requirements were specified to ensure the services were completely described.
- By using the foundation provided by the workshop the SCSOs were defined and then reviewed by the project contributors and WP16.6.1 safety experts.

Task 20 (V2)

The results from the Task 8 (V1) analysis were reviewed as the first step of Task 20 (V2). In addition the following work was undertaken:

- Development and assessment of the 'SPR level' model. The 'SPR level' model provides a model of the system at a high level, but unlike the functional model it also includes architectural details (who or what performs the functions). The 'SPR level' model can be found in section 3.2.
- Development and assessment of the threads (scenarios). The threads show the interactions between the various elements of the SPR level model through specific scenarios which represent the way the concepts will be used in operational situations. The full list of the threads can be found in Appendix A.

2.6.1.1 Introduction

The Success Case Safety Objectives (SCSOs) define the safety related functions that the concept will perform, in terms of the services to aircraft. These define the *complete* range of functions which the services provide, and correspond to the E-OCVM lifecycle phase 2 in terms of their level of detail. They can be considered as the safety related operational objectives for the services.

The SCSOs were defined based on assessment of the Operational Requirements, the SAfety Criteria derivation, and the Success Case analysis. These were then reviewed by safety experts and concept experts (at the operational level). They summarise the functionality described by the Operational Requirements (ORs), which were defined at varying levels of detail (for example some were physical, others were assumptions, others logical... etc.) into a complete and consistent set of requirements. These could then be properly safety assessed, which was simply not possible with the existing ORs.

Note that the SCSOs presented here represent the final version of the SCSOs, including minor refinements made during the failure case analysis. In addition, these are the SCSOs following Task 20 (V2) whereby they were re-assessed and refined in light of concept changes.

The SCSOs were then further reviewed following the VP-501 (V2 – as part of P04.07.02) and VP-798 (V2 as part of P04.03) exercises. As in the case of SACs, no changes were necessary.

2.6.1.2 Safety Objectives for Normal Operations related to TRACT

Ref	Phase of Flight / Operational Service	Related AIM Barrier	Achieved by / Safety Objective
1	En Route / TRACT	MB10.1.1.2.1.1 Failure to identify Conflict	SCSO 31
2	En Route / TRACT	MB10.1.1.2.1.1 Failure to identify Conflict	SCSO 32
3	En Route / TRACT	MB4.1.1.1.1.1 No independent ATCO Monitoring	SCSO 33
4	En Route / TRACT	MB10.1.1.2.1.1 Failure to identify Conflict	SCSO 34
5	En Route / TRACT	MBX.1.3.3 ATCO lost awareness of	SCSO 35

		previously identified conflict	
6	En Route / TRACT	MF7.1.1 Conflict resolution leads to knock-on conflict	SCSO 36

Table 3 Operational Services & Safety Objectives (success approach) – TRACT

Table 5 summarizes the safety objectives for normal operations for TRACT and it also provides the traceability towards the OSED requirements and the SACs corresponding to each SCSO.

ID [OSED Req. ref.]	Text	Rationale	Ref. SAC
SCSO 31 [REQ-04.07.02-OSED-0003.2017; REQ-04.07.02-OSED-0003.3061; REQ-04.07.02-OSED-0003.4042; REQ-04.07.02-OSED-0003.4053]	TRACT shall attempt to resolve potential conflicts between aircraft without the necessity of controller intervention.	This safety objective relates to the AIM Barrier Pre-Cursor MB10.1.1.2.1.1 'Failure to identify Conflict'. The prime objective of TRACT is to ensure that aircraft trajectories are adjusted and de-conflicted so that they do not require planner or tactical resolution - this therefore reduces the risk of a planner failing to identify a conflict	SAC 31
SCSO 32 [REQ-04.07.02-OSED-0003.2018]	TRACT shall not create additional conflicts or degrade existing conflicts as a result of solving potential conflicts.	This safety objective relates to the AIM Barrier Pre-Cursor MB10.1.1.2.1.1 'Failure to identify Conflict'. TRACT should not increase the number of ATC induced Tactical conflicts, however there is a risk that in some situations TRACT causes induced conflicts because TRACT introduces additional uncertainty to the aircraft trajectory, and there is a period where the instruction has been issued (from TRACT), but not accepted and displayed to the controllers.	SAC 32
SCSO 33 [REQ-04.07.02-OSED-0003.3085; REQ-04.07.02-OSED-0003.3088; REQ-04.07.02-OSED-0003.2031; REQ-04.07.02-OSED-0003.2020]	TRACT shall monitor conformance with aircraft under TRACT resolution.	This safety objective relates to the AIM Barrier Pre-Cursor MB4.1.1.1.1.1 No independent ATCO Monitoring. TRACT shall monitor conformance of aircraft under a TRACT resolution therefore reduces the risk of an imminent collision if the ATCO is not monitoring the interaction	SAC 33
SCSO 34 [REQ-04.07.02-OSED-0003.3080; REQ-04.07.02-OSED-0003.6001; REQ-04.07.02-OSED-0003.5009]	TRACT shall only attempt to resolve conflicts where speed adjustment is a suitable means of conflict resolution.	This safety objective relates to the AIM Barrier Pre-Cursor MB10.1.1.2.1.1 Failure to identify Conflict. If TRACT tried to resolve other types of conflicts (e.g. head on) it would fail to resolve the conflict, but for a period of time	SAC 33

		would be indicating that it was resolving the conflict. If the controller trusted this, there would be an imminent infringement by the time the TRACT relinquished the aircraft. It is noted that this would be mitigated by the planner and tactical tools (assuming they are operating and independent of TRACT).	
SCSO 35 [REQ-04.07.02-OSED-0003.2019; REQ-04.07.02-OSED-0003.3065; REQ-04.07.02-OSED-0003.3107; REQ-04.07.02-OSED-0003.3066; REQ-04.07.02-OSED-0003.3067; REQ-04.07.02-OSED-0003.2037; REQ-04.07.02-OSED-0003.3115; REQ-04.07.02-OSED-0003.2039; REQ-04.07.02-OSED-0003.3108; REQ-04.07.02-OSED-0003.3078; REQ-04.07.02-OSED-0003.4026; REQ-04.07.02-OSED-0003.4027; REQ-04.07.02-OSED-0003.4029; REQ-04.07.02-OSED-0003.4050; REQ-04.07.02-OSED-0003.3116]	TRACT shall inform the controller (and other relevant parties) of any aircraft that is under TRACT resolution and the relevant status/details of the resolution.	The controller can identify flights that are under TRACT resolution (and check the details of the resolution to satisfy himself that it will work) and does not attempt to solve conflicts that are already being dealt with by TRACT. Also the controller is kept updated as to the status of the resolution	SAC 34
SCSO 36 [REQ-04.07.02-OSED-0003.3117; REQ-04.07.02-OSED-0003.2040; REQ-04.07.02-OSED-0003.3113; REQ-04.07.02-OSED-0003.3114; REQ-04.07.02-OSED-0003.4028]	The TRACT resolution shall be overridden if deemed unsuitable by the ATCO, or informed by the pilot.	The responsibility of separation is ultimately the responsibility of the controller, therefore they must have the ability to discard the TRACT solution if deemed necessary, in particular if the TRACT resolution is interfering with a conflict management activity that the ATCO is attempting (i.e. he/she is not satisfied with the TRACT resolution or the aircraft if involved in another potential encounter(s) which the controller wants to resolve).	SAC 32
SCSO 37 [REQ-04.07.02-OSED-0003.6001; REQ-04.07.02-OSED-0003.5001]	TRACT shall only attempt to solve conflictions for those aircraft which are eligible	TRACT shall only attempt to provide resolutions for those flights that are eligible e.g. it will not attempt to provide a resolution for any aircraft that may be performing abnormal/unusual manoeuvres	SAC 31
SCSO 38 [REQ-04.07.02-OSED-0003.2040; REQ-04.07.02-OSED-0003.3108; REQ-04.07.02-OSED-0003.3078; REQ-04.07.02-OSED-0003.2039]	TRACT will discard a resolution for any change in aircraft trajectory that is currently under TRACT resolution	Any new clearances that are issued to an aircraft will automatically deem the TRACT resolution no longer valid	SAC 34

900 **Table 4 List of Safety Objectives (success approach) for Normal Operations - TRACT**

901 ### 2.6.1.3 Safety Objectives for Normal Operations related to CD/R aid to PC

Ref	Phase of Fight /	Related AIM Barrier	Achieved by / Safety

	Operational Service		Objective
1	En Route / CD/R to PC	MF7.1.1 Conflict resolution leads to knock-on conflict MB10.1.1.2.1.2 Misjudge Conflict Resolution	SCSO 21
2	En Route / CD/R to PC	MB10.1.1.2.1.2 Misjudge Conflict Resolution MF9.1.2 Conflict resolution leads to knock-on pre-tactical conflict	SCSO 22
3	En Route / CD/R to PC	MF9.1.2 Conflict resolution leads to knock-on pre-tactical conflict	SCSO 23
4	En Route / CD/R to PC	MB10.2.2 Inadequate planner-upstream coordination	SCSO 24
5	En Route / CD/R to PC	MB10.1.1.2 Inadequate planning task MB10.1.1.1.2.2 Incorrect planning data - negative impact!	SCSO 25
6	En Route / CD/R to PC	MB10.1.1.1.2.1 No planning information	SCSO 26
7	En Route / CD/R to PC	MB10.1.2.1 Inadequate planner-exec coordination MB10.1.1.1.2.2 Incorrect planning data MB6.1.2.1 Conflict due to level bust	SCSO 27
8	En Route / CD/R to PC	MB10.1.1.1.2.2 Incorrect planning data	SCSO 28
9	En Route / CD/R to PC	MB7.1.2.3.A Potential conflict due to bad instructions given to pilot	SCSO 29
10	En Route / CD/R to PC	MB10.2.2 Inadequate planner-upstream coordination MB10.1.2.1 Inadequate planner-exec coordination	SCSO 210
11	En Route / CD/R to PC	Enables all the above mentioned barriers	SCSO 211
12	En Route / CD/R to PC	ATC Induced Pre-Tactical Conflict	SCSO 212

Table 5 Operational Services & Safety Objectives (success approach) – CD/R aid to PC

Table 7 summarizes the safety objectives for normal operations for the CD/R aid to PC tool and it also provides the traceability towards the OSED requirements and the SACs corresponding to each of the SCSOs.

ID [OSED Req. ref.]	Text	Rationale	Ref. SAC
SCSO 21 [REQ-04.07.02-OSED-0002.2012; REQ-04.07.02-OSED-0002.3047; REQ-04.07.02-OSED-0002.3058; REQ-04.07.02-OSED-0002.3087; REQ-04.07.02-OSED-0002.3051; REQ-04.07.02-OSED-0002.3059; REQ-04.07.02-OSED-0002.3119; REQ-04.07.02-OSED-0002.2013]	The PC aid shall indicate pairs of aircraft which have planning encounters at the entry or exit sector boundary.	This safety objective relates to the AIM Barrier Pre-Cursor MB10.1.1.2.1.1 Failure to identify Conflict due to the fact that PC aid identifies conflicts which the controller may otherwise have missed. It also relates to MB10.1.1.2.1.2	SAC 21

		Misjudge Conflict Resolution due to the fact that PC aid would automatically identify conflicts which still exist after an inadequate resolution is applied.	
SCSO 22 [REQ-04.07.02-OSED-0002.2012; REQ-04.07.02-OSED-0002.3087; REQ-04.07.02-OSED-0002.3058; REQ-04.07.02-OSED-0002.3056; REQ-04.07.02-OSED-0002.3055; REQ-04.07.02-OSED-0002.3076; REQ-04.07.02-OSED-0002.2013]	The PC aid shall identify planning encounters in proposed resolutions.	This safety objective relates to the AIM Barrier Pre-Cursor MB10.1.1.2.1.2 Misjudge Conflict Resolution due to the fact that The PC aid, via the what if probing would identify an inadequate resolution proposed by the controller. It also relates to MF7.1.1 Conflict resolution leads to knock-on conflict due to the fact The PC aid, via the what if probing would identify a new conflict created by the proposed resolution.	SAC 21
SCSO 23 [REQ-04.07.02-OSED-0002.3077; REQ-04.07.02-OSED-0002.3056; REQ-04.07.02-OSED-0002.3055; REQ-04.07.02-OSED-0002.3049; REQ-04.07.02-OSED-0002.2012]	The PC Aid shall detect planning encounters which would involve the subject flight for all sector coordination entry and exit levels.	This safety objective relates to the AIM Barrier Pre-Cursor MF7.1.1 Conflict resolution leads to knock-on conflict. The PC Aid will support the controller by showing encounter free options before the controller decides upon a resolution thereby reducing the chance that they pick a resolution which leads to a knock-on conflict	SAC 21
SCSO 24 [REQ-04.07.02-OSED-0002.2014]	The PC aid shall monitor aircraft's achievability to meet entry and exit coordination.	This safety objective relates to the AIM Barrier Pre-Cursor MB10.2.2 Inadequate planner-upstream coordination. The tool helps to identify situations where the aircrew are deviating vertically and therefore may create a new conflict/workload issue in the next sector. Therefore the controller is more likely to provide adequate upstream coordination.	SAC 21 SAC 22 SAC 23
SCSO 25 [REQ-04.07.02-OSED-0002.2016; REQ-04.07.02-OSED-0002.3060]	The PC aid shall coordinate entry and exit conditions without the necessity of controller intervention.	This safety objective relates to the AIM Barrier Pre-Cursor MB10.1.1.2 Inadequate planning task due to the fact that automating some coordination reduces workload for controller,	SAC 21 SAC 22 SAC 23

		in very high workload situations this gives the controller more time to perform their task, and they are therefore less likely to make errors in judgement. It also relates to MB10.1.1.1.2.2 Incorrect planning data. This could actually have a negative impact due to the fact that some coordinations are not handled by the controller, therefore they may not be as aware of the situation and therefore may have reduced situational awareness.	
SCSO 26 [REQ-04.07.02-OSED-0002.4016]	The PC Aid shall enable the application of constraints to the coordination trajectory.	This safety objective relates to the AIM Barrier Pre-Cursor MB10.1.1.1.2.1 No planning information. The controller can input constraints to the system, therefore this improves the information available and displayed by other existing tools, which means they are less likely to mislead the controller. It also enables the new tools to perform more accurate trajectory prediction, which may help the controller to identify encounters.	SAC 21 SAC 22 SAC 23
SCSO 27 [REQ-04.07.02-OSED-0002.2053]	The PC Aid shall detect deviations from each flights entry and exit conditions.	This safety objective relates to the AIM Barrier Pre-Cursor MB10.1.2.1 Inadequate planner-exec coordination due to the fact that The tool identifies a situation where the planner has instructed the tactical to implement a resolution and the tactical has failed to do so. It also relates to MB10.1.1.1.2.2 Incorrect planning data due to the fact that the tool allows the resolution to be entered into the system so that it can be used by other tools, thus improving the data available to other tools.	SAC 21 SAC 22 SAC 23
SCSO 28 [REQ-04.07.02-OSED-0002.3052; REQ-04.07.02-OSED-0002.3055; REQ-04.07.02-OSED-0002.2011]	The PC Aid shall indicate the predicted trajectories of a subject aircraft and any aircraft which may be interacting with it.	This safety objective relates to the AIM Barrier Pre-Cursor MB10.1.1.1.2.2 Incorrect planning data. The tool is providing details of the trajectory of relevant aircraft to the controller, which means they are less likely to have an inaccurate	SAC 21 SAC 22

		picture of the situation.	
SCSO 29 [REQ-04.07.02-OSED-0002.3109; REQ-04.07.02-OSED-0002.3055; REQ-04.07.02-OSED-0002.3110; REQ-04.07.02-OSED-0002.2038]	The PC Aid shall identify aircraft which are between the subject aircraft's current flight level and proposed exit flight level when a controller is assessing an exit flight level.	This safety objective relates to the AIM Barrier Pre-Cursor MB7.1.2.3.A Potential conflict due to bad instructions given to pilot. The tool will help reduce the chance of the PC coordinating an exit level which requires the tactical to make many clearances to achieve. Since this is likely to reduce the number of clearances the tactical makes, it must reduce the chance of the tactical giving a bad clearance	SAC 21 SAC 22
SCSO 210 [REQ-04.07.02-OSED-0002.3044; REQ-04.07.02-OSED-0002.3043]	The PC Aid shall improve communication between controllers.	This safety objective relates to the AIM Barrier Pre-Cursor MB10.2.2 Inadequate planner-upstream coordination. The tools allow precise communication between sectors therefore reduces the risk of inadequate upstream coordination. It also relates to MB10.1.2.1 Inadequate planner-exec coordination due to the fact the tool will allow more precise communication and sharing of information between controllers.	SAC 21 SAC 22
SCSO 211 [REQ-04.07.02-OSED-0002.2010; REQ-04.07.02-OSED-0002.1002]	The PC aid tool shall be active at all CWPs at all times.	Correct assumption, but needs to be validated.	SAC 21 SAC 22
SCSO 212 [REQ-04.07.02-OSED-0002.3047]	The PC Aid shall identify planning encounters against a flight for every MTCD probe where the flight is blocking a level/s and/or likely to perform unusual manoeuvres.	Correct assumption, but needs to be validated.	SAC 21

907 **Table 6 List of Safety Objectives (success approach) for Normal Operations - CD/R aid to PC**

908 ### 2.6.1.4 Safety Objectives for Normal Operations related to CD/R aid to TC

Ref	Phase of Fight / Operational Service	Related AIM Barrier	Achieved by / Safety Objective
1	En Route / CD/R to TC	MBX1.3.1 ATCO misjudgement of separation MBX.1.2.3 Failed to Detect Conflict MBX1.1.1 Inadequate traffic picture MB4.2.1 ATCO misjudgement of separation MB4.2.2 ATCO failure to act	SCSO 11

2	En Route / CD/R to TC	MF6.1.2 Conflict due to Crew/ac Deviation MBX1.1.1 Inadequate traffic picture MB4.3 Inadequate Pilot Response to ATC	SCSO 12
3	En Route / CD/R to TC	MBX.1.3.1 ATCO misjudgement of separation MBX1.1.1 Inadequate traffic picture MB4.1.2 ATCO failure to identify conflict in time MF7.1.1 Conflict resolution leads to knock on conflict	SCSO 13
4	En Route / CD/R to TC	MBX.1.3.2 ATCO failure to act	SCSO 14
5	En Route / CD/R to TC	MBX1.3.1 ATCO misjudgement of separation MF7.1.1 Conflict resolution leads to knock on conflict MB4.1.2.2 Inadequate information for conflict management MBX1.1.1 Inadequate traffic picture	SCSO 15
6	En Route / CD/R to TC	Enables all the above mentioned barriers	SCSO 16

Table 7 Operational Services & Safety Objectives (success approach) – CD/R aid to TC

Table 9 summarizes the safety objectives for normal operations for the CD/R aid to TC tool and it also provides the traceability towards the OSED requirements and the SACs corresponding to the CD/R aid to TC.

ID [OSED Req. ref.]	Text	Rationale	Ref. SAC
SCSO 11 [REQ-04.07.02-OSED-0001.2002; REQ-04.07.02-OSED-0001.3027; REQ-04.07.02-OSED-0001.3028; REQ-04.07.02-OSED-0001.3032; REQ-04.07.02-OSED-0001.3037; REQ-04.07.02-OSED-0001.3097; REQ-04.07.02-OSED-0001.3095; REQ-04.07.02-OSED-0001.2034; REQ-04.07.02-OSED-0001.3099; REQ-04.07.02-OSED-0001.3101; REQ-04.07.02-OSED-0001.3112; REQ-04.07.02-OSED-0001.3008; REQ-04.07.02-OSED-0001.3093; REQ-04.07.02-OSED-0001.3007; REQ-04.07.02-OSED-0001.2007; REQ-04.07.02-OSED-0001.2035; REQ-04.07.02-OSED-0001.3089; REQ-04.07.02-OSED-0001.3091; REQ-04.07.02-OSED-0001.3094]	The TC Aid shall indicate all relevant pairs of aircraft whose predicted (tactical or deviated) trajectories result in an infringement upon the horizontal and vertical minimum separation.	Success Case Analysis (preliminary) performed during workshop (Task 8) involving safety and ATC experts identified the requirements that need to be placed for the services to deliver their safety benefits when working as intended. Related AIM Barriers MB5 and MF4 [3]. This safety objective relates to the AIM Barrier Pre-Cursor MBX1.3.1 ATCO misjudgement of separation as the TC aid would automatically identify conflicts which still exist after an inadequate resolution is applied. It relates to MBX.1.2.3 Failed to Detect Conflict as the TC aid detects all relevant interactions within the sector therefore reducing the risk of the Tactical failing to detect conflictions. It also relates to MBX1.1.1 Inadequate traffic picture as the TC aid detects all relevant interactions within the sector therefore reducing the risk of the Tactical being unaware of any conflicts due to not having an adequate traffic awareness	SAC 11 SAC 12

SCSO 12; [REQ-04.07.02-OSED-0001.2004; REQ-04.07.02-OSED-0001.2005; REQ-04.07.02-OSED-0001.3090; REQ-04.07.02-OSED-0001.3006; REQ-04.07.02-OSED-0001.3118; REQ-04.07.02-OSED-0001.3019; REQ-04.07.02-OSED-0001.3020; REQ-04.07.02-OSED-0001.3021; REQ-04.07.02-OSED-0001.3022; REQ-04.07.02-OSED-0001.3023; REQ-04.07.02-OSED-0001.3024; REQ-04.07.02-OSED-0001.3026; REQ-04.07.02-OSED-0001.3010]	The TC Aid shall indicate the following deviations between an aircraft's known position and predicted trajectory: 1) Route Deviation (ROUTE) 2) Vertical Deviation Rate (RATE) 3) Cleared flight level deviation (CFL) 4) Speed Deviations (SPD) 5) No valid flight plan data available (NoTT)	Success Case Analysis (preliminary) performed during workshop (Task 8) involving safety and ATC experts identified the requirements that need to be placed for the services to deliver their safety benefits when working as intended. Related AIM Barriers MF6.1 and MF4 [3]. This safety objective relates to the AIM Barrier Pre-Cursor MF6.1.2 Conflict due to Crew/ac Deviation due the fact the TC aid shall detect deviations from any instructions issues to the aircraft that affects the trajectory. Therefore there is a reduced risk of a conflict being created due to these deviations	SAC 11 SAC 12 SAC 14
SCSO 13 [REQ-04.07.02-OSED-0001.3038]	For the subject aircraft the TC aid shall identify conflicts for any probed clearances.	Success Case Analysis (preliminary) performed during workshop involving safety and ATC experts identified the requirements that need to be placed for the services to deliver their safety benefits when working as intended. Related AIM Barrier MF7.1 [3]. This safety objective relates to the AIM Barrier MBX.1.3.1 ATCO misjudgement of separation due to the fact that the TC aid would automatically identify conflicts which still exist after an inadequate resolution is applied. It also relates to MBX1.1.1 Inadequate traffic picture due to the fact that the TC aid what if functionality will identify any conflictions for any probed clearances they are about to issue that they may not have been aware of due to an inadequate traffic picture. It also relates to MF7.1.1 Conflict resolution leads to knock on conflict due to the fact that the TC aid, via the what if probing would identify a new conflict created by the proposed resolution	SAC 11 SAC 12 SAC 13
SCSO 14 [REQ-04.07.02-OSED-0001.3105; REQ-04.07.02-OSED-0001.3104; REQ-04.07.02-OSED-0001.2008]	TC Aid shall support the TC to correctly prioritise and resolve conflicts indicated to the ATCO by TC	Success Case Analysis (preliminary) performed during workshop involving safety and ATC experts identified the requirements that need to be placed for the services to deliver their safety benefits when working as intended. Related AIM Barriers MB5, MF7.1, and	SAC 11 SAC 12

	aid in a timely way.	MF4 [3]. This safety objective relates to the AIM Barrier MBX.1.3.2 ATCO failure to act. The TC aid shall display to the controller all conflictions and will indicate the severity/geometry of those interactions, therefore indicating the highest priority of tasks	
SCSO 15 [REQ-04.07.02-OSED-0001.2036; REQ-04.07.02-OSED-0001.3106; REQ-04.07.02-OSED-0001.3039; REQ-04.07.02-OSED-0001.3038]	The TC Aid shall detect Tactical encounters which would involve the subject flight for all flight levels within the sector.	This safety objective relates to the AIM Barrier MBX1.3.1 ATCO misjudgement of separation due to the fact that the TC aid shall display to the Tactical Controller the occupancy of all other levels in the sector and any potential conflictions if they were to use these levels for the subject flight, therefore reducing the risk of the tactical misjudging separation. It also relates to MF7.1.1 Conflict resolution leads to knock on conflict due to the fact that the TC Aid will help the controller by showing encounter free options before the controller decides upon a resolution thereby reducing the chance that they pick a resolution which leads to a knock-on conflict. It also relates to MBX1.1.1 Inadequate traffic picture due to the fact that the TC aid what-else functionality will reduce the risk of the Tactical having an inadequate traffic picture as they have a constant view of flight level occupancy in the sector with regards to the subject flight	SAC 11 SAC 12 SAC 13
SCSO 16 [REQ-04.07.02-OSED-0001.1001]	The TC aid tool shall be active at all CWPs at all times.	This is a correct assumption, but will need to be validated during the simulation	SAC 11 SAC 12 SAC 13 SAC 14 SAC 15

Table 8 List of Safety Objectives (success approach) for Normal Operations - CD/R aid to TC

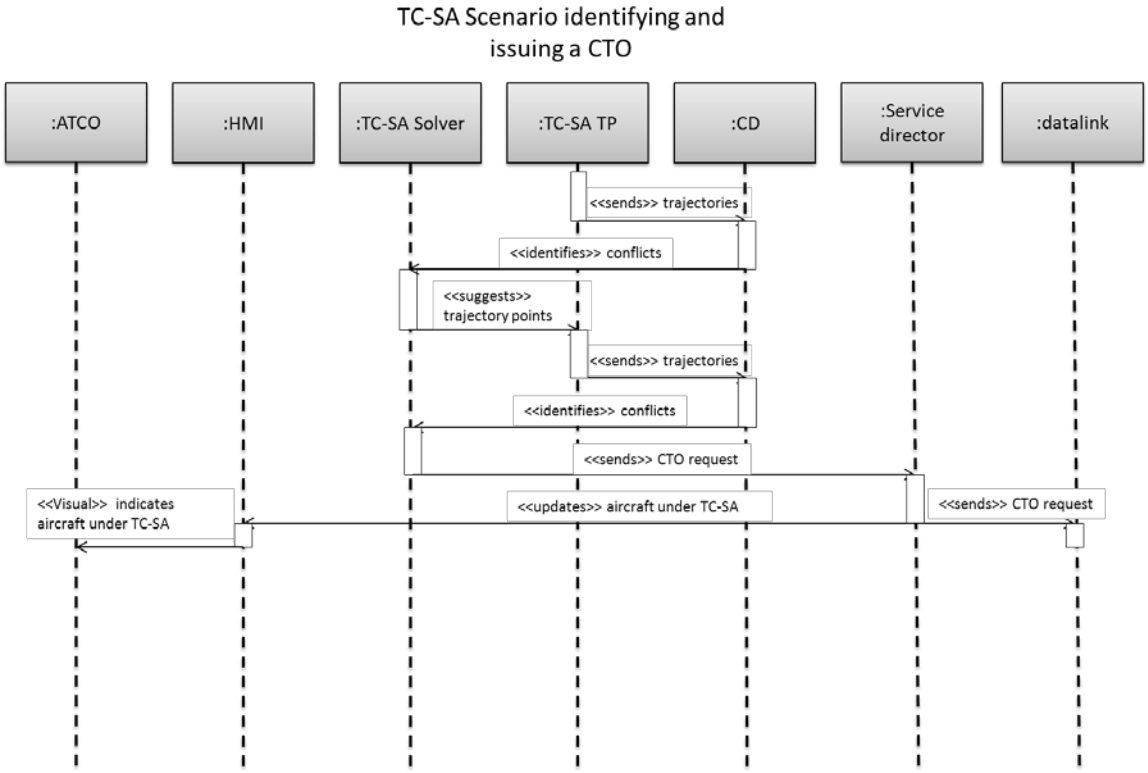
2.6.2 Analysis of the Concept for a Typical Flight

This section records the description of the services that were discussed during the Success Case Analysis. They provided the basis for the understanding of the services' successful operation, i.e. they provide the description (at a high level) of the success case. These descriptions helped to shape the functional blocks, and the Success Case Safety Objectives (SCSOs).

2.6.2.1 Sequence Diagram

The diagrams below show examples of sequence diagrams that were used to help derive the SCSOs in Task 8 (V1). These were found to be a useful tool to ensure that the SCSOs covered all aspects of the services. They were also useful in the failure case analysis to ensure hazards were not missed.

925 Finally, they help during discussions to ensure all workshop participants have the same view of the
926 concept and are thinking about them in the same way. It was not feasible to discuss all scenarios in
927 the concept during the workshop, therefore only a selection of example sequence diagrams were
928 produced.



929

930 **Figure 7 TRACT Sequence Diagram**

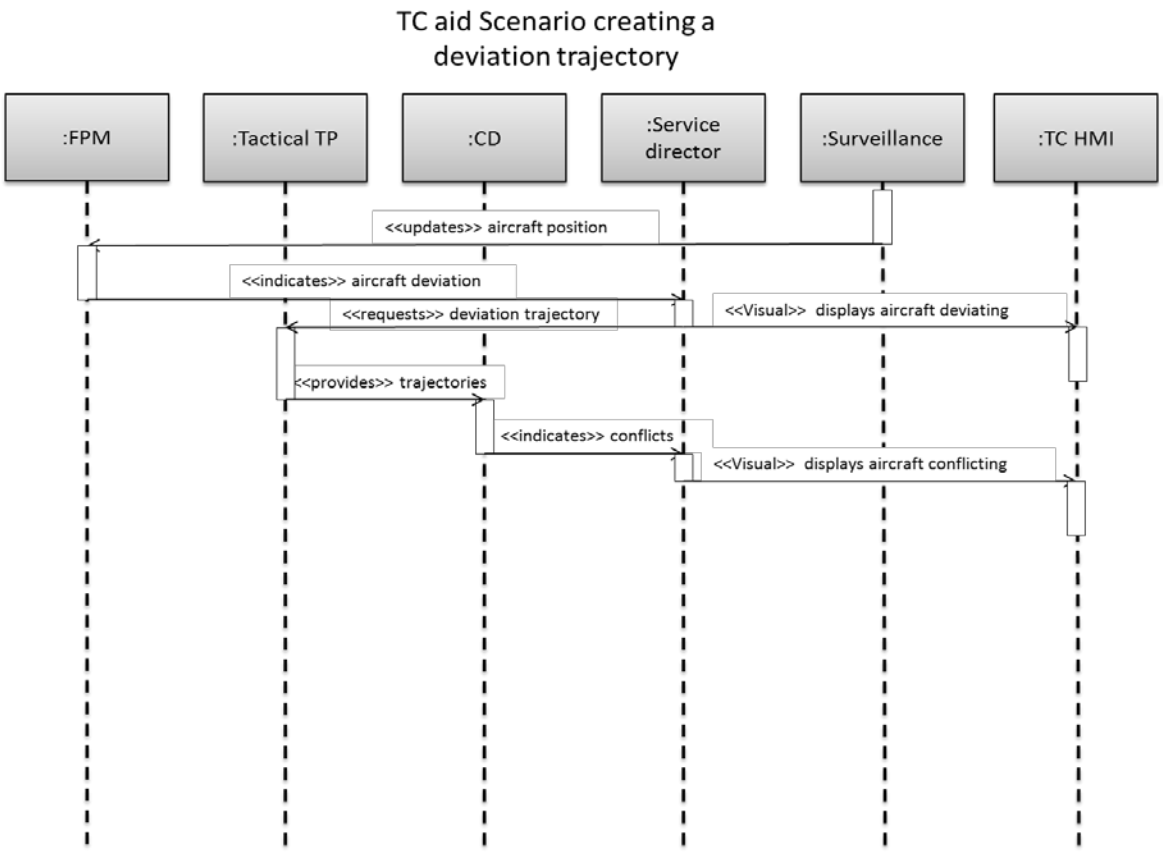


Figure 8 CD/R aid to TC Sequence Diagram

2.6.2.1.1 TRACT

1) TRACT retrieves the current traffic situation from the FDPS.
2) TRACT performs trajectory prediction, and identifies clusters of aircraft that may have potential conflicts.
3) TRACT identifies a potential conflict between two aircraft.
4) TRACT attempts to solve the conflict:
   a. TRACT calculates a speed adjustment that can be applied.
   b. TRACT cannot calculate a speed adjustment. In this case the conflict is passed on so that the PC aid will deal with it and the use case ends here.
5) TRACT issues an instruction to an aircraft to adjust its speed by issuing a Controlled Time Over (CTO) via the datalink.
6) TRACT indicates to the PC that the conflict is under TRACT instruction.
7) The aircraft displays the instruction to the aircrew.
8) Aircrew response:
   a. The aircrew accepts the instruction.
   b. The aircrew does not respond (in this instance we return to step 6).
   c. The aircrew rejects the instruction.
9) The aircrew's response is relayed to the ground through datalink. Additionally the FMS calculates a new trajectory (if the aircrew accepted the instruction) and reports this to the ground.

10) TRACT receives the response:

a. The aircrew accepted the instruction. TRACT monitors the aircraft (1), and updates the PC aid to show that the aircraft is conforming to TRACT.

b. The aircrew did not respond. TRACT labels the aircraft as 'standby' while awaiting and updating for a *TBD* period (return to step 6).

c. The aircrew have not responded for a *TBD* period. TRACT discards the aircraft from further considerations. Unclear what happens in this instance, the high level OSED talks about 'an indicator helps the ATCO in identifying long "standby" in order to address the air crew directly by voice".

d. The aircrew rejects the instruction. TRACT discards the aircraft from calculations for TBD period.[5] (Return to step 1).

11) TRACT is monitoring an aircraft under TRACT and detects a deviation. TRACT resolutions for that aircraft are cancelled and all related TRACT resolutions are discarded (CTOs removed).

2.6.2.1.2 CD/R aid to PC

1) The PC receives an offer.

2) The system assesses the potential conflicts relating from this:

a. The system considers that there are no conflicts and accepts the offer. This is recorded by the system. The 'PC aid' tool then uses a trajectory based on the offered level for conflict detection purposes. Step 6.

b. The system determines that there are planning interactions at the offered level and indicates the flight to the PC.

3) The PC interrogates the system regarding the offered flight:

a. The PC identifies an alternative offered level or coordination conditions and suggests them.

b. The PC decides to accept the offered level and deal with any planning interactions. Step 6.

4) The other sector PC receives an alternative suggestion:

a. The offered level is automatically accepted. Step 6.

b. The offered level is not accepted by the PC. The PCs then need to discuss and agree a resolution (15).

5) The other sector TC then instructs the aircrew based on the agreed level in the system.

6) The PC aid performs Flight Path Monitoring (FPM) on the flight:

a. The flight does not deviate. No further action is taken.

b. The flight deviates from the offered level or coordination conditions. The PC is alerted. The PCs then has to resolve the issue based on current operating procedures.

2.6.2.1.3 CD/R aid to TC

1) The 'TC aid' tool gets data from the FPDS.

[5] Note that the ETA min/max is downlinked just before the CTO is calculated so there is a low (but non-zero) probability that the calculated CTO may be outside the ETA min/max which would cause a rejection. Other operational reasons for rejection may exist. The process here states that the aircraft would no longer be considered suitable for a TC-SA resolution. However, it may make more sense to just re-compute a new CTO. For further analysis.

2) The 'TC aid' tool performs trajectory prediction and detects a conflict.

3) The 'TC aid' tool alerts the TC.

4) The TC uses the 'TC aid' tool to perform a 'what if' assessment and identify a resolution.

5) The TC issues an instruction via R/T to the aircrew, and enters it into the system.

6) The aircrew accept the instruction and it is implemented on the aircraft through, for example its entry into the FMS.

7) The aircraft updates the trajectory and the 'TC aid' tool, the TC and the PC monitor the situation:

   a. The aircraft conforms to the clearance. No further action.

   b. The aircraft deviates from the clearance. The monitoring aids alert the TC. The controller contacts the aircrew via R/T:

      i. The pilot can correct the deviation and inputs the correction to the FMS. Step 6.

      ii. The pilot cannot return to the cleared trajectory. The TC clears the aircraft's route of other traffic.

      iii. The TC concludes that the Monitoring Aids (MONA) warning is not relevant and suppresses it.

2.7 Conflict Detection, Resolution and Monitoring Operations under Abnormal Conditions

The purpose of this section is to assess the ability of the "Conflict Detection, Resolution and Monitoring" tools to work through (robustness), or at least recover from (resilience) any abnormal conditions, external to the "Conflict Detection, Resolution and Monitoring" System, that might be encountered relatively infrequently.

2.7.1 Identification of Abnormal Conditions

The list below shows the abnormal conditions under which the concepts are judged to operate. These were explicitly considered in the safety analysis throughout this document. This list includes those abnormal conditions identified during the safety workshop in Task 8 (V1). The following abnormal conditions scenarios have been identified for each of the three operational services:

- Severe weather – e.g. rapid wind changes that cannot be predicted and therefore modelled;
- Traffic Overload in Sector;
- Use of emergency vertical separation;
- Unusual traffic – e.g. formation flights, supersonic flights;
- Aircraft equipment malfunction e.g. transponder failure;
- Non-responsive aircraft (e.g. serious aircraft malfunction which means aircraft cannot comply with ATC instruction - e.g. engine failure);
- Non-responsive aircraft - radio failure;
- Non-responsive aircraft - datalink fail;
- Border with less sophisticated/incompatible ANSP;
- Significant deviation from filed flight plans (for a non-trivial number of aircraft) e.g. unexpected airport closure. Clarification: this is not a situation whereby pilots are deviating unexpectedly, but rather a situation where ATC are forced to issue many instructions which mean that a significant number of aircraft are no longer able to maintain to their flight plan;

- Serious Tactical Deviation (e.g. Aircraft takes instruction but does something else, or aircraft takes another aircraft's instruction). Controller's attention is drawn only to the aircraft in question, causing immediate/unpredictable overload;
- TMA Holds are full, aircraft are holding En Route;
- Complete loss of communication - voice and datalink.

2.7.2 Potential Mitigations of Abnormal Conditions

In order to identify the relevant safety requirements and safety integrity requirements (success and failure case respectively) it is necessary to identify both the normal and abnormal conditions under which the concepts will operate. Table 10 Abnormal Conditions and Potential Mitigations shows the results of the analysis for abnormal conditions and the derived safety objectives for the three operational services. Note the resultant safety objectives are recorded in Section 2.6.1.

Ref	Abnormal Condition	Operational Effect[6]			Mitigation		
		PC Aid	TC Aid	TRACT	PC Aid	TC Aid	TRACT
1	Severe weather – not as expected	Coordination trajectory inaccurate	The aircraft is following the cleared instructions so not deviating, but the TP is not accurate, therefore may not be predicting interactions correctly.	Aircraft do not achieve predicted trajectories	Deviation trajectories (SCSO27)	Deviation trajectories (SCSO11, SCSO12)	CTOs are monitored for conformance (OR 0003.3088). Pilot shall report to the ATCO if FMS alerts that the CTO cannot be met within the uncertainty that TRACT requires (safety requirement to be validated). Then the ATCO takes action to resolve the conflict. (SCSO36)
2	Traffic overload in	None	Controller is	None	All SCSOs for	Deviation	TRACT can

[6] Within the context of En Route separation.

Ref	Abnormal Condition	Operational Effect[b]			Mitigation		
		PC Aid	TC Aid	TRACT	PC Aid	TC Aid	TRACT
	Sector		overloaded therefore he is too busy to enter all clearances into the system and/or he is not updating them.		PC aid	trajectories (SCSO11, SCSO12)	monitor success rate in terms of generating resolutions and use it to alert supervisor so they can take appropriate action (SCSO36)
3	Use of emergency vertical separation (500 ft)	Trajectories are based upon flight levels of *1000ft separation,* therefore would interactions be picked up for aircraft at the same x500ft? If not could this cause nuisance alerts?	Trajectories are based upon flight *levels of 1000ft separation,* therefore would interactions be picked up for aircraft at the same x500ft? If not could this cause nuisance alerts?	None	TC aid would show relevant conflicts until 1000ft separation can be re-established (SCSO21, SCSO22, SCSO23)	TC Aid would show relevant conflicts until 1000ft separation can be re-established SM parameters can be adjusted. Controller will endeavour to apply lateral where possible due to TCAS going off (SCSO11)	SCSO36
4	Unusual traffic – e.g. formation flights, supersonic flights	What kind of coordination trajectory would the unusual traffic	As PC aid, how does TC aid manage this situation	None	E.g. the PC Aid would use a level/s block for the unusual	E.g. the TC Aid would use a level/s block for the unusual	There could be a number of a/c characteristics

Ref	Abnormal Condition	Operational Effect[b]			Mitigation		
		PC Aid	TC Aid	TRACT	PC Aid	TC Aid	TRACT
		produce? E.g. for a formation flight would you need to block the whole level			flight, then the planner would use radar for resolving any climb through etc. Or unusual flight is highlighted for any what-if probe regardless of level match (SCSO22)	flight, then the tactical would use radar for resolving any climb through etc.	that mean that an a/c is not eligible for TRACT management ATCO to be aware of how TRACT works and that may affect TRACT resolutions. There may be special procedures in place for unusual flights (SCSO36, SCSO34)
5	Aircraft equipment malfunction e.g. transponder failure	PC Aid will produce a non-radar trajectory based on times and estimates	TC Aid will produce a non-radar trajectory based on times and estimates	Worst case scenario TRACT is unable to apply CTO to aircraft			Pilot can inform ATCO of any known failures, then ATCO can remove CTO (SCSO36)
6	Non-responsive aircraft (e.g. serious aircraft malfunction e.g. engine failure – and cannot comply with ATC instruction)	Aircraft not following cleared instructions	Aircraft not following cleared instructions	Aircraft not following cleared instructions	Planner can enter a coordinated descent (e.g. if a/c is in emergency descent) which will cover all of	Deviation Trajectories Flight can be recognised manually to adjacent sectors Possibly can	CTOs are monitored for conformance (OR 0003.3088). (SCSO36)

Ref	Abnormal Condition	Operational Effect[b]			Mitigation		
		PC Aid	TC Aid	TRACT	PC Aid	TC Aid	TRACT
					those levels for coordinating other aircraft. Can you include emergency flight for every single MTCD probe even if not level matching? (SCSO26, SCSO27, SCSO29)	enter 'pseudo-clearances' to try and follow what a/c is doing to keep deviation trajectories more accurate (SCSO11, SCSO12)	
6b	Non-responsive - Radio Fail	Assume Aircraft will follow radio fail procedures, cannot issue any new clearances that differ from flight planned route		No effect on TRACT	Use PC Aid to re-coordinate aircraft if necessary – requirements necessary to alert PC Aid of this? (All SCSOs for PC aid)	Can enter 'pseudo-clearances' as you can predict what aircraft will do (SCSO11, SCSO12)	
6c	Non-responsive datalink fail			TRACT does not receive EPP data and does not receive confirmation that the CTO has been applied	Revert to voice comms	Revert to voice comms	TRACT warns the ATCO of this (SCSO35)
7	Failure of navigational aids – ground and/or air	None	None	None	Deviation trajectories	Deviation trajectories	Pilot reports that he cannot achieve CTO (or reports problem with aircraft) and

Ref	Abnormal Condition	Operational Effect[b]			Mitigation		
		PC Aid	TC Aid	TRACT	PC Aid	TC Aid	TRACT
							ATCO can remove CTO.
8	Border with less sophisticated / incompatible ANSP	PC Aid: The coordination trajectory from the incompatible ANSP may not be modelling exactly what the aircraft is doing e.g. may be route following as the system does not realise the aircraft is on a heading		None	SCSO26		None
9	Significant deviation from filed flight plans (for a non-trivial number of aircraft) e.g. unexpected airport closure. Clarification: this is not a situation whereby pilots are deviating unexpectedly, but rather a situation where ATC are forced to issue many instructions which mean that a significant number of aircraft are no		Not expected to be a significant problem as the trajectory prediction is utilising clearances rather than flight plans.	Rate of TRACT successfully resolving potential conflicts is reduced Note: new TRACT resolutions will not be created immediately but after a defined period	Deviation Trajectories (All SCSOs for PC aid)	Deviation trajectories (SCSO11, SCSO12)	

Ref	Abnormal Condition	Operational Effect[b]			Mitigation		
		PC Aid	TC Aid	TRACT	PC Aid	TC Aid	TRACT
	longer able to maintain to their flight plan.						
10	Serious Tactical Deviation (e.g. Aircraft takes instruction but does something else, or aircraft takes another aircrafts' instruction). Controller's attention is drawn only to the aircraft in question, causing immediate/unpredictable overload		Aircraft not following their clearances		PC Aid assists Planner in monitoring wider traffic set (All SCSOs for PC aid)	TC aid should mitigate by displaying information to the Planner (e.g. info from the TC Aid made available to the PC Aid/Planner) – to be defined (SCSO11, SCSO12)	TRACT assists Planner in monitoring wider traffic set
11	TMA Holding full, aircraft are holding En Route				Holding a/c will be highlighted for any probe		When any clearance is given to an aircraft (other than route following) the CTO is discarded
12	Loss of comms for all	No effect on toolset	No effect on toolset	No effect on toolset	Same as today apart from use of datalink	Same as today apart from use of datalink	Same as today apart from use of datalink
13	(New scenario from 16/06				PC Aid may pick up on conflict if flight has not	TC Aid alerts controller to potential	New mitigation- TRACT

Ref	Abnormal Condition	Operational Effect[b]			Mitigation		
		PC Aid	TC Aid	TRACT	PC Aid	TC Aid	TRACT
	workshop). Phase one: TRACT identifies an encounter 25 mins ahead and applies 1 CTO to a/c #1, but not to a/c #2. Phase two: 20 mins ahead – Wind changes and slows a/c #2, or TP wasn't good, and now both a/c are in conflict even with the CTO. There will be no update to the TRACT resolution. TRACT applies a CTO to one aircraft, the wind then changes which slows down the other aircraft (beyond the boundaries of uncertainty that TRACT places on a/c #2) with which				been coordinated yet – to apply only if ATCO has been alerted or does not believe TRACT resolution will work	encounter (what are the procedures here – should the Tactical always intervene on TC Aid alert?) - to apply only if ATCO has been alerted or does not believe TRACT resolution will work	monitors the TRACT resolution and warns the ATCO that it cannot assure the resolution

Ref	Abnormal Condition	Operational Effect[b]			Mitigation		
		PC Aid	TC Aid	TRACT	PC Aid	TC Aid	TRACT
	the aircraft is conflicting with. This then makes the CTO unsuitable. TRACT is not monitoring the flight.						

1044 **Table 9 Abnormal Conditions and Potential Mitigations**

2.8 Mitigation of System-generated Risks (failure approach)

This section concerns the Conflict Detection, Resolution and Monitoring system under internal failure conditions. Before any conclusion can be reached concerning the adequacy of the safety specification of the Conflict Detection, Resolution and Monitoring system, at the OSED level, it is necessary to assess the possible adverse effects that failures internal to the end-to-end Conflict Detection, Resolution and Monitoring System might have upon the provision of the ATM services and to derive integrity safety objectives to mitigate against these effects.

2.8.1 Identification and Analysis of System-generated Hazards

The functional hazards presented below in sections 2.8.1.1, 2.8.1.2 and 2.8.1.3 have been identified during the Task 20 (V2) workshop based on the SCSOs presented in Table 5, Table 7 and Table 9.

The *Maximum Tolerable Frequency of Occurrence* figures in Table 11, Table 12 and Table 13 have been developed during the workshop using the following principle (from the Guidance to Apply the SESAR Safety Reference Material, edition 00.01.00):

- The MAC model barrier upon which the hazard impact is referenced to identify the base safety level (maximum tolerable frequency of occurrence per flight hour).
- This number is then divided by the estimated number of hazards on that barrier.
- Finally the number is divided by an impact modifier (IM). This requires a judgement of the impact of the hazard on the barrier, and is a reflection of the number of aircraft that will be effected, the timeframe of the impact (e.g. complete vs. partial), and the controller's ability to deal with the hazard (e.g. credible vs. not credible).

The following is an example only for the purposes of demonstrating the method, and is not an actual hazard *Maximum Tolerable Frequency of Occurrence*:

- TC aid tool could affect the Tactical Management Barrier (MAC-SC3). This has a maximum tolerable frequency of occurrence (per flight hour) of $1E^{-4}$.
- The estimated number of hazards on this barrier is 25 therefore the figure is reduced to $4E^{-6}$.
- If the example hazard caused a single credible nuisance alarm, then all the controller has to do is identify that the aircraft are separated, therefore an IM (or MF) of 0.1 is used (based on expert judgement). This gives $4E^{-5}$ as the final figure.
- Alternatively, *if* the example hazard caused missed alarm, that was not credible, it might be considered worse than a nuisance alarm (as the controller has to detect the possible loss of separation himself). Therefore an IM of 1 is used. This gives a final figure of $4E^{-6}$.

The calculations of the maximum tolerable frequency of occurrence presented in the *Maximum Tolerable Frequency of Occurrence* column in Table 11, Table 12 and Table 13 for each identified hazard are shown in section B.2 in Appendix B.

2.8.1.1 TRACT

ID	Description	Related SO *(success approach)*	Operational Effects	Mitigations of Effects	Maximum Tolerable Frequency of Occurrence
Hz 001	TRACT – the separating actor – executive	SCSO 31 SCSO 32 SCSO 35	Executive controller delaying separation assurance as	The ATCO has access to the CTO information, and may identify non-credible resolutions.	2.00E-04

	controller delayed		he/she believes TRACT to be the separating actor	The ATCO has the TC aid to assist in solving conflicts. Unusual flights should be highlighted to the ATCO. Procedures that the controller must follow in the instance of unusual flights.	
Hz 002	TRACT – the separating actor - planner controller delayed	SCSO 31 SCSO 32 SCSO 35	Planner controller delaying or failing to assuring separation as he/she believes TRACT to be the separating actor	The ATCO has access to the CTO information. The ATCO has the PC aid to assist in solving conflicts. Unusual flights should be highlighted to the ATCO. Procedures that the controller must follow in the instance of unusual flights.	2.00E-04
Hz 003	TRACT – managing the aircraft	SCSO 31 SCSO 32 SCSO 34 SCSO 37	TRACT managing aircraft unnecessarily, resulting in increased workload for the controller	The ATCO has access to the CTO information, and may identify non-credible resolutions. The ATCO has the PC/TC aid to assist in solving conflicts. Pilot may refuse the CTO if it is the aircraft which has just been issued a clearance[7].	2.00E-04
Hz 004	TRACT – doesn't provide resolution	SCSO 31 SCSO 34 SCSO 35 SCSO 37	TRACT being unable to provide resolutions leading to workload increase for controller.	The ATCO has the PC/TC aid to assist in solving conflicts.	2.00E-04
Hz 005	TRACT – the separating actor – tactical controller fails separation	SCSO 31 SCSO 32 SCSO 35	Tactical fails to assure separation as he/she believes TRACT to be the separating actor.	ATCO applies relevant procedures.	4.00E-06

1082 **Table 10: System-Generated Hazards and Analysis for TRACT**

[7] Note pilots should be aware that a clearance may be valid only for a certain amount of time and should expect

1083 ### 2.8.1.2 CD/R aid to PC

ID	Description	Related SO *(success approach)*	Operational Effects	Mitigations of Effects	Maximum Tolerable Frequency of Occurrence
Hz 001	CD/R aid to PC misleads the controller which fails to take action	SCSO 21 SCSO 22 SCSO 23 SCSO 25 SCSO 28 SCSO 29 SCSO 210	The tool misleads the controller such that he fails to take appropriate action for a pre-tactical encounter.	TC Aid will eventually pick up encounter. Situational awareness of Planner and Tactical on both sides monitoring. Some kind of deviation monitoring may pick up error.	2.00E-04
Hz 002	CD/R aid to PC misleads the controller and increases workload	SCSO 21 SCSO 22 SCSO 23 SCSO 25 SCSO 28 SCSO 29 SCSO 210	The tool misleads the controller such that he takes unnecessary action for a pre-tactical encounter.	TC Aid will eventually pick up encounter. Situational awareness of Planner and Tactical – controllers will be able to detect the possible error. Some kind of deviation monitoring may pick up the possible error.	4.00E-03
Hz 003	CD/R aid to PC – flight automatically coordinated inappropriately	SCSO 25	Flights automatically coordinated inappropriately, resulting in an induced tactical or pre-tactical encounter.	TC Aid will eventually pick up encounter. Situational awareness of Planner and Tactical – controllers will be able to detect the possible error by different means (e.g. radar). Some kind of deviation monitoring may pick up the possible error.	2.00E-04
Hz 004	CD/R aid to PC suffers a detected failure	All apply	The tool suffers a detected failure resulting in increased workload for the controller, potentially leading to a missed encounter, or unnecessary action.	Other aspects of the PC Aid may still be working e.g. TP and MTCD. Situational awareness of Planner and Tactical – controllers will be able to detect the possible error by different means (e.g. radar). Some kind of deviation monitoring may pick up the possible error. TC Aid will eventually pick	2.00E-03

				up encounter.	
Hz 005	CD/R aid to PC misunderstood by the controller	SCSO 21 SCSO 22 SCSO 23 SCSO 25 SCSO 28 SCSO 29 SCSO 210	The tools are working correctly, however the controller may misunderstand/ misinterpret the data shown and make a bad planning decision. This therefore increases work load to an unacceptable level, and may increase the risk of causing a safety related incident.	Training. Tactical may question planner's decision and solve the possible safety related incident. Situational awareness of Planner – controller will be able to detect and assess the possible error by different means (e.g. radar). Some kind of deviation monitoring may pick up the possible error. TC Aid will eventually pick up encounter.	2.00E-03

1084 **Table 11: System-Generated Hazards and Analysis for CD/R aid to PC**

1085 ### 2.8.1.3 CD/R aid to TC

ID	Description	Related SO *(success approach)*	Operational Effects	Mitigations of Effects	Maximum Tolerable Frequency of Occurrence
Hz 001	CD/R aid to TC misleads the controller	SCSO 11 SCSO 12 SCSO 14	The tool misleads the controller into missing a tactical conflict.	Executive controller picks up encounter from radar scan. Other tools (STCA etc.) can help.	4.00E-06
Hz 002	CD/R aid to TC presents nuisance alerts	SCSO 11 SCSO 12 SCSO 14	The tool presents nuisance alerts to the controller which increase workload, potentially leading to a missed tactical conflict.	The controller can delete/supress nuisance alerts. In order to avoid nuisance alerts parameters for situations when the TC aid should trigger alerts have to be defined.	8.00E-05
Hz 003	CD/R aid to TC presents nuisance resolution	SCSO 11 SCSO 12 SCSO 14	The tool presents nuisance resolution proposals leading to a missed tactical conflict.	The controller can use other tools to double check the proposal (e.g. radar). If an unsafe clearance was made by the ATCO then the conflict detection would alert controller to the confliction. Ground based and airborne	4.00E-04

				safety nets e.g. STCA.	
Hz 004	CD/R aid to TC suffers a detected failure	All apply	The tool suffers a detected failure resulting in increased workload for the controller, potentially leading to a missed encounter, or unnecessary action.	Work without the TC aid and reduce flow rates through sectors. Ground based and airborne safety nets e.g. STCA.	8.00E-05
Hz 005	CD/R aid to TC misunderstood by the controller	SCSO 11 SCSO 12 SCSO 14	The tools are working correctly, however the controller may misunderstand/ misinterpret the data shown and make a bad tactical decision. This therefore increases work load to an unacceptable level, and may increase the risk of causing a safety related incident.	Training. Planner may question executives' decision and make the executive aware of the possible safety related incident. Some kind of deviation monitoring may pick up the possible error. TC Aid will eventually pick up encounter.	4.00E-05

1086 **Table 12: System-Generated Hazards and Analysis for CD/R aid to TC**

1087 2.8.2 Derivation of Safety Objectives (integrity/reliability)

1088 Based on the system generated hazards presented in Table 11, Table 12 and Table 13 the
1089 integrity/reliability safety objectives have been developed. These failure case safety objectives
1090 specify the functions required of the service to be safe when it fails. The FCSOs and the
1091 corresponding Hazard Id from which they were derived are presented in sections 2.8.2.1, 2.8.2.2 and
1092 2.8.2.3 for all three operational services.

1093 2.8.2.1 TRACT

ID	SO ID	Safety Objectives (integrity/reliability)
Hz 001	FCSO 31	The frequency of the Executive controller delaying separation assurance for a TRACT cluster as he/she believes TRACT to be the separating actor shall be no greater than 2E-4 per flight hour
Hz 002	FCSO 32	The frequency of Planner controller delaying or failing to assure separation for a TRACT cluster as he/she believes TRACT to be the separating actor

		shall be no greater than 2E-4 per flight hour
Hz 003	FCSO 33	The frequency of TRACT managing aircraft unnecessarily, resulting in increased workload for the controller shall be no greater than 2E-4 per flight hour
Hz 004	FCSO 34	The frequency of TRACT being unable to provide resolutions which it should be able to leading to workload increase[8] for the controller shall be no greater than 2E-4 per flight hour
Hz 005	FCSO 35	The frequency of the Executive controller failing to assure separation for a TRACT cluster as he/she believes TRACT to be the separating actor shall be no greater than 4E-6 per flight hour

1094 **Table 13: Safety Objectives (integrity/reliability) - TRACT**

1095 ### 2.8.2.2 CD/R aid to PC

ID	SO ID	Safety Objectives (integrity/reliability)
Hz 001	FCSO 21	The frequency of the tool misleading the controller such that he fails to take appropriate action for a pre-tactical encounter shall be no more than 2E-4 per flight hour
Hz 002	FCSO 22	The frequency of the tool misleading the controller such that he takes unnecessary action for a pre-tactical encounter shall be no more than 4E-3 per flight hour
Hz 003	FCSO 23	The frequency of the tool automatically coordinating flights inappropriately, resulting in an induced tactical or pre-tactical encounter shall be no more 2E-4 per flight hour
Hz 004	FCSO 24	The frequency of the tool suffers a detected failure resulting in increased workload for the controller, potentially leading to a missed encounter, or unnecessary action shall be no more 2E-3 per flight hour
Hz 005	FCSO 25	The frequency of the controller misunderstanding/misinterpreting the tool potentially leading to making a bad planning decision shall be no more 2E-3 per flight hour

1096 **Table 14 Safety Objectives (integrity/reliability) - PC aid**

1097 ### 2.8.2.3 CD/R aid to TC

ID	SO ID	Safety Objectives (integrity/reliability)
Hz 001	FCSO 11	The frequency of the tool misleading the controller into missing a tactical conflict shall be no greater than 4E-6 per flight hour
Hz 002	FCSO 12	The frequency of the tool presenting nuisance alerts to the controller which increase workload, potentially leading to a missed tactical conflict shall be no greater than 8E-5 per flight hour

[8] Note that the 'increase' of workload is explicitly in the context of ATCOs operating within an environment of increased traffic enabled by the tools, i.e. a traffic load that can only be managed with the aid of the tools.

Hz 003	FCSO 13	The frequency of the tool presenting nuisance resolution proposals leading to a missed tactical conflict shall be no greater than 4E-4 per flight hour
Hz 004	FCSO 14	The frequency of the tool suffering a detected failure resulting in increased workload for the controller, potentially leading to a missed encounter, or unnecessary action shall be no greater than 8E-5 per flight hour
Hz 005	FCSO 15	The frequency of the controller misunderstanding/misinterpreting the tool potentially leading to making a bad tactical decision shall be no greater than 4E-5 per flight hour

Table 15 Safety Objectives (integrity/reliability) - TC aid

2.9 Impacts of Conflict Detecting, Resolution and Monitoring operations on adjacent airspace or on neighbouring ATM Systems

Any potential interaction with adjacent airspace and impact on neighbouring ATM system are already addressed in previous sections.

No additional safety objectives have been identified on that subject apart from the ones already derived from the assessment of the operations in normal/abnormal conditions.

2.10 Achievability of the SAfety Criteria

The general approach to showing that the SACs' potential has been satisfied has been done through the specification of Safety Objectives (success and failure) in sections 2.6.1 and 2.8.

The SACs were also quantified by assessing the AIM precursors which the concepts would affect, and judging the extent to which the concepts could have a positive (or negative) impact upon them. The precursor impacts were then aggregated to produce the final results for each SAC. Sections 2.10.1, 2.10.2, and 2.10.3 below show these calculations.

The result from the *Barrier Benefit* column was calculated in the following way:

- The SCSOs which could contribute towards a given SAC were identified and their benefit (in the *Benefit* column) was estimated by the safety experts;
- The estimated benefit was then multiplied with the precursor number from the AIM model (*Precursor effected* column) and as a result the *Barrier Benefit* was obtained;
- The barrier benefits were then added for each corresponding SAC and the total barrier benefit was then obtained per SAC.

Note that the quantifications are only performed for SACs which are expressed as a quantifiable benefit. For example those specifying "no increase in…" are not quantified.

2.10.1 TRACT

SCSO ID	SAC ID	Precursor effected	Precursor rationale	Benefit	Benefit rationale	Barrier Benefit
SCSO 31	SAC 31	MB10.1.1.2.1.1 Failure to identify Conflict (33%)	The prime objective of TRACT is to ensure that aircraft trajectories are adjusted and de-conflicted so that they do not require planner or tactical resolution -	10%	Just because TRACT detects a conflict further out than the Planner is looking does not reduce the chances of the Planner not	3.3%

SCSO ID	SAC ID	Precursor effected	Precursor rationale	Benefit	Benefit rationale	Barrier Benefit
			this therefore reduces the risk of a planner failing to identify a conflict		detecting it themselves	
TOTAL	**SAC 31**					**3.3%**

Table 16 SAC Quantification - TRACT

2.10.2 CD/R aid to PC

SCSO ID	SAC ID	Precursor effected	Precursor rationale	Benefit	Benefit rationale	Barrier Benefit
SCSO 21	SAC 22	MB10.1.1.2.1.1 Failure to identify Conflict (33%)	PC aid identifies conflicts which the controller may otherwise have missed.	40%	Primary focus of the conflict detection, it should alert the controller where they would previously have missed, but sometimes they will miss the alert.	13.200 %
		MB10.1.1.2.1.2 Misjudge Conflict Resolution (7%)	PC aid would automatically identify conflicts which still exist after an inadequate resolution is applied.	5%	This is so low because it is likely they would use the 'what if' function to catch this problem, but in the rare cases where they did specify a conflicting resolution, the tool would identify the new/continued conflict to them. Assumes that the concept shows planning encounters at all times.	0.350%
SCSO 22	SAC 22	MB10.1.1.2.1.2 Misjudge Conflict Resolution (7%)	The PC aid, via the what if probing would identify an inadequate resolution proposed by the controller	50%	Rather than the controller having to rely on judgement and experience in deciding a course of action e.g. which heading to use, the 'what-if' tool will display an accurate trajectory (and any associated conflicts) as a result of their decision.	3.500%
	SAC 21	MF9.1.2 Conflict resolution leads to knock-on pre-tactical conflict (15%)	The PC aid, via the what if probing would identify a new conflict created by the proposed resolution	40%		6.000%
SCSO 23	SAC 21	MF9.1.2 Conflict resolution leads to	The PC Aid will help the controller by showing encounter free options before the controller	40%	Rather than having to 'try out' different coordination levels via the 'what-if' tool the	6.000%

SCSO ID	SAC ID	Precursor effected	Precursor rationale	Benefit	Benefit rationale	Barrier Benefit
		knock-on pre-tactical conflict (15%)	decides upon a resolution thereby reducing the chance that they pick a resolution which leads to a knock-on conflict		'what-else' planner tools will at a glance show free levels for coordination	
SCSO 24	SAC 22	MB10.2.2 Inadequate planner-upstream coordination (15%)	The tool helps to identify situations where the aircrew are deviating vertically and therefore may create a new conflict/workload issue in the next sector. Therefore the controller is more likely to provide adequate upstream coordination.	15%	A large part of the Planner Controller task is to monitor if coordinations will be met and are constantly scanning for this and do not necessarily need an alert to inform them of this. (However, as traffic levels increase it may become more important....)	2.250%
SCSO 25	SAC 22	MB10.1.1.2 Inadequate planning task (45%)	Automating some coordination reduces workload for controller, in very high workload situations this gives the controller more time to perform their task, and they are therefore less likely to make errors in judgement.	15%	Not particularly high percentage as Integrated Coordination could potentially reduce a controller situational awareness which could lead to inadequate coordination decisions	6.750%
		MB10.1.1.1.2.2 Incorrect planning data - negative impact! (-5%)	As some coordinations are not handled by the controller, they will not be as aware of the situation and therefore have reduced situational awareness.	5%	see rationale for precursor	-0.250%
SCSO 26	SAC 22	MB10.1.1.1.2.1 No planning information (5%)	The controller can input constraints to the system. This improves the information available and therefore displayed by other existing tools, which means they are less likely to mislead the controller. It also enables the new tools to perform more accurate trajectory prediction, which may help the controller identify encounters.	50%	With the ability to enter coordination constraints and conditions to coordinations, there should be a large % of coordinations that have all of the adequate information attached to them	2.500%
SCSO 27	SAC 22	MB10.1.2.1 Inadequate planner-exec coordination (5%)	The tool identifies a situation where the planner has instructed the tactical to implement a resolution and the	40%	The Flight Path monitoring functionality will be particularly useful for the scenario as	2.000%

SCSO ID	SAC ID	Precursor effected	Precursor rationale	Benefit	Benefit rationale	Barrier Benefit
			tactical has failed to do so.		described in 'rationale for precursor'	
		MB10.1.1.1.2.2 Incorrect planning data (5%)	The tool allows the resolution to be entered into the system so that it can be used by other tools, thus improving the data available to other tools.	40%	All parties should have the correct planning information when using the PC Aid	2.000%
	SAC 23	MB6.1.2.1 Conflict due to level bust (65%)	The tool will help to detect aircraft which are deviating from their planned coordinations and therefore help the controller to alert the pilot and allow them to correct the problem.	10%	This would only apply when the deviation is at a sector boundary	6.500%
SCSO 28	SAC 22	MB10.1.1.1.2.2 Incorrect planning data (5%)	The tool is providing details of the trajectory of relevant aircraft to the controller, which means they are less likely to have an inaccurate picture of the situation.	35%	The associated HMI from the Planner MTCD provides a clear traffic picture for the Planner Controller, therefore reducing the risk if there being inadequate planning information for the Planner controller to use when making their decisions	1.750%
SCSO 29	SAC 22	MB7.1.2.3.A Potential conflict due to bad instructions given to pilot (20%)	The tool will help reduce the chance of the PC coordinating an exit level which requires the tactical to make many clearances to achieve. Since this is likely to reduce the number of clearances the tactical makes, it must reduce the chance of the tactical giving a bad clearance	5%	The Tactical controller with their experience should still not make 'bad' clearances even if the coordination level is unachievable- they would just ask the planner to change the coordination level	1.000%
SCSO 210	SAC 22	MB10.2.2 Inadequate planner-upstream coordination (15%)	Allows precise communication between sectors therefore reduces the risk of inadequate upstream coordination	5%	An important part of the Planner Role is to ensure all pertinent information is passed on to the upstream sector, so therefore a low percentage improvement.	0.750%

SCSO ID	SAC ID	Precursor effected	Precursor rationale	Benefit	Benefit rationale	Barrier Benefit
		MB10.1.2.1 Inadequate planner-exec coordination (5%)	The tool will allow more precise communication and sharing of information between controllers…	5%	An important part of the Planner Role is to ensure all pertinent information is passed on to the Tactical controller, so therefore a low percentage improvement.	0.250%
TOTAL	**SAC 21**					**12%**
	SAC 22					**36%**
	SAC 23					**7%**

1125 **Table 17 SAC Quantification - CD/R aid to PC**

1126 ## 2.10.3 CD/R aid to TC

SCSO ID	SAC ID	Precursor effected	Precursor rationale	Benefit	Benefit rationale	Barrier Benefit
SCSO 11	SAC 12	MBX1.3.1 ATCO misjudgement of separation (7%)	TC aid would automatically identify conflicts which still exist after an inadequate resolution is applied.	40%	The TC aid provides accurate resolution prediction for interactions therefore there a high % improvement against a tactical misjudging the separation	2.8%
		MBX.1.2.3 Failed to Detect Conflict (32%)	TC aid detects all relevant interactions within the sector therefore reducing the risk of the Tactical failing to detect conflictions	50%	High % improvement as the TC aid should detect all interactions	16.0%
		MBX1.1.1 Inadequate traffic picture (5%)	TC aid detects all relevant interactions within the sector therefore reducing the risk of the Tactical being unaware of any conflicts due to not having an adequate traffic awareness	40%	High % improvement of the tactical having an inadequate traffic picture as the TC Aid provides constant display and monitoring of all interactions	2.0%

					within the sector	
	SAC 11	MB4.2.1 ATCO misjudgement of separation (12%)	The TC aid alerts controllers within the bounds of its parameters, and therefore never makes a 'misjudgement', noting that it can be incorrect if it's inputs are incorrect	30%	Sometimes the inputs will be wrong, but most of the time it will help	3.6%
		MB4.2.2 ATCO failure to act (20%)	This is the primary purpose of the tool: to ensure that conflicts which the controller might not detected are indicated to them	50%	The tool will help reduce the number of times the controller fails to act by prompting them, but sometimes the failure to act cannot be avoided and a prompt does not resolve the conflict.	10.0%
SCSO 12	SAC 14	MF6.1.2 Conflict due to Crew/ac Deviation (71%)	The TC aid shall detect deviations from any instructions issues to the aircraft that affects the trajectory. Therefore there is a reduce risk of a conflict being created due to these deviations	40%	High % improvement to the precursors due to the controller being alerted to any deviations therefore can correct before any conflicts occur	28.4%
	SAC 12	MBX1.1.1 Inadequate traffic picture (5%)	The scenario is: Controller issues an instruction to the aircraft, but does not enter it into the system, therefore the aircraft is considered to be deviating. Because the tool indicates the 'deviation' the controller will know to enter it into the system, which means that if there is a later conflict he has full information.	5%	Considered to be a rare situation: firstly the controller needs to issue an instruction and then fail to enter it, and secondly this aircraft needs to subsequently be involved in a potential conflict.	0.25%

	SAC 11	MB4.3 Inadequate Pilot Response to ATC (2%)	The conformance monitor will detect when the pilot deviates from the clearance and therefore allow the controller time to contact the pilot and correct the problem, particularly if the deviation results in a potential conflict	10%	There will only be a limited number of times when there is a conflict resultant and the controller has time to resolve the conflict with the pilot.	0.2%
SCSO 13	SAC 12	MBX.1.3.1 ATCO misjudgement of separation (7%)	TC aid would automatically identify conflicts which still exist after an inadequate resolution is applied.	50%	Rather than the controller having to rely on judgement and experience in deciding a course of action e.g. which heading to use, the 'what-if' tool will display an accurate trajectory (and any associated conflicts) as a result of their decision.	3.5%
	SAC 12	MBX1.1.1 Inadequate traffic picture (5%)	The TC aid what if functionality will identify any conflictions for any probed clearances they are about to issue that they may not have been aware of due to an inadequate traffic picture	30%	By using the 'what-if' tool to probe clearances and also having a constant monitor of all interactions in the sector should have a high % impact on the chance of the Tactical having an inadequate traffic picture. Sometimes there may be an inadequate traffic picture because the system and the controller are missing information (otherwise it would be a higher	1.5%

					improvement)	
	SAC11	MB4.1.2 ATCO failure to identify conflict in time (55%)	The TC aid, via the what if probing would identify a new conflict created by the proposed resolution	10%	This will reduce a small proportion of the number of times when an ATCO would have failed to identify an imminent infringement	5.5%
	SAC 13	MF7.1.1 Conflict resolution leads to knock on conflict (5%)	The TC aid, via the what if probing would identify a new conflict created by the proposed resolution	50%	By using the 'what-if' probe for all resolutions there should be a very low risk of a conflict resolution leading to a knock on conflict, therefore high % improvement	2.5%
SCSO 14	SAC 12	MBX.1.3.2 ATCO failure to act (4%)	The TC aid shall display to the controller all conflictions and will indicate the severity/geometry of those interactions, therefore indicating the highest priority of tasks	30%	The constant display of interactions and the severity is continually displayed to the controller so there *should* be a high % improvements in the ATCO failing to act. This needs to be checked against the context of *how controllers work.*	1.05%
SCSO 15	SAC 12	MBX1.3.1 ATCO misjudgement of separation (7%)	The TC aid shall display to the Tactical Controller the occupancy of all other levels in the sector and any potential conflictions if they	15%	Normally the 'what-if' tool reduces the risk of mis-judgment of separation, but sometimes this 'what-else' tool	1.05%

			were to use these levels for the subject flight, therefore reducing the risk of the tactical misjudging separation		will help the controller identify a suitable resolution	
	SAC 13	MF7.1.1 Conflict resolution leads to knock on conflict (5%)	The TC aid will help the controller by showing encounter free options before the controller decides upon a resolution thereby reducing the chance that they pick a resolution which leads to a knock-on conflict	50%	Rather than having to 'try out' different levels via the 'what-if' tool the 'what-else' planner tools will at a glance show free levels for coordination	2.5%
	SAC 11	MB4.1.2.2 Inadequate information for conflict managemen t (5%)	The TC aid will give the controller better information about conflicts	50%	The tool will be providing a significant increase the information available to the controller in relation to conflict management	2.0%
	SAC 12	MBX1.1.1 Inadequate traffic picture (5%)	The TC aid what-else functionality will reduce the risk of the Tactical having an inadequate traffic picture as they have a constant view of flight level occupancy in the sector with regards to the subject flight	30%	The 'what-else' functionality will have a fairly high % of reducing the risk of the Tactical having an inadequate traffic picture as at a glance they can assess which levels are occupied with relevance to a particular aircraft	1.5%
TOTAL	**SAC 11**					**21%**
	SAC 12					**30%**
	SAC 13					**5%**
	SAC 14					**28%**

1127 **Table 18 SAC Quantification - CD/R aid to TC**

2.11 Validation & Verification of the Safety Specification

3 Safe Design at SPR Level

3.1 Scope

This section addresses the following activities:

- derivation of the Safety Requirements for the Conflict Detection, Resolution and Monitoring system previously described – section 3.2
- analysis of the operation of the Conflict Detection, Resolution and Monitoring system described above under normal operational conditions – section 3.3
- design analysis – case of internal failures of operations and the PSSA of the Conflict Detection, Resolution and Monitoring as described above – section 3.4

3.2 The Conflict Detection, Resolution and Monitoring Systems SPR-level Model

The diagrams below show the SPR level models as developed, in accordance with the SRM [1] guidance material, through discussion in the workshops and beyond. These diagrams were a key part of the Task 20 V2-V3 SPR analysis. They formed the reference against which Safety Requirements were specified, and in developing them the completeness of the concept's description was explored. The diagrams were the result of the Success Case Analysis workshop and post workshop discussions.

Note the SPR-Functional Model is not present in this document since the concept is sufficiently mature to use the SPR-level Model directly.

3.2.1 Description of SPR-level Model

The following figure shows the several elements composing the Conflict Detection, Resolution and Monitoring system, located in a Controller Working Position (CWP) providing ATS services. For completeness reasons, external elements interacting with the Conflict Detection, Resolution and Monitoring system elements are also showed in this model in order to derive relevant requirements and/or assumptions for the specification of the Conflict Detection, Resolution and Monitoring system.

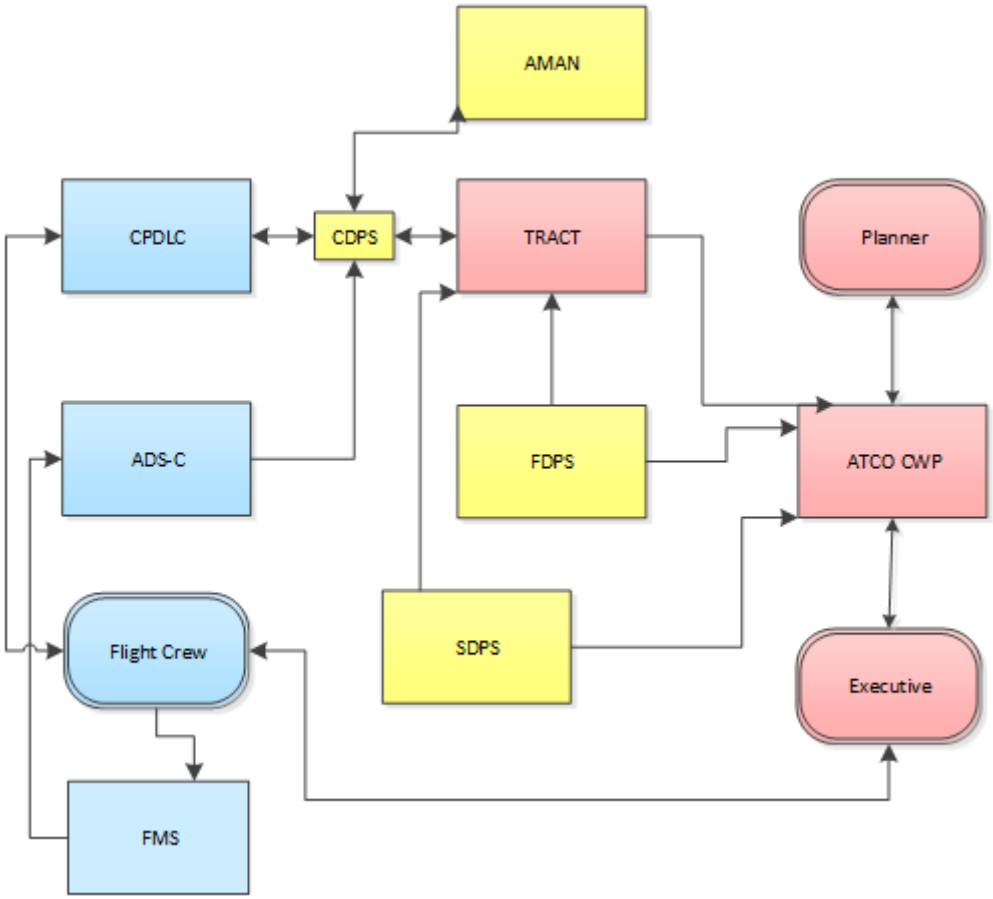


Figure 9: TRACT SPR level model

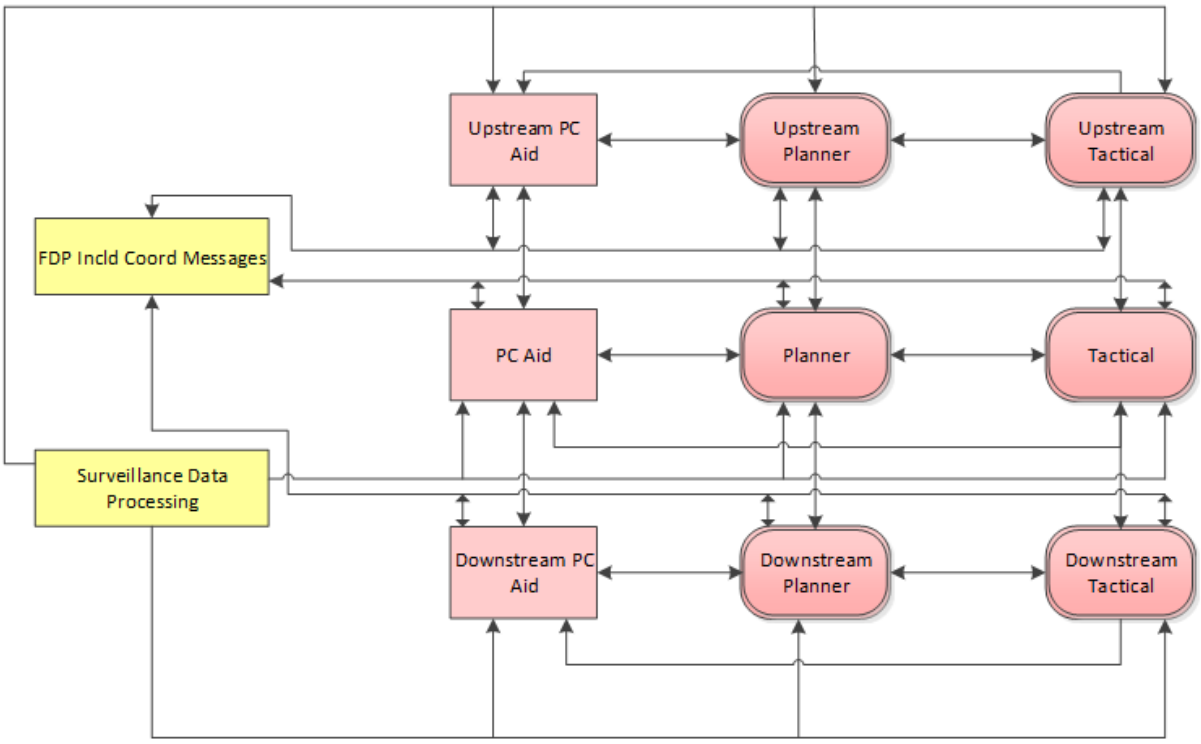


Figure 10: PC Aid SPR level model

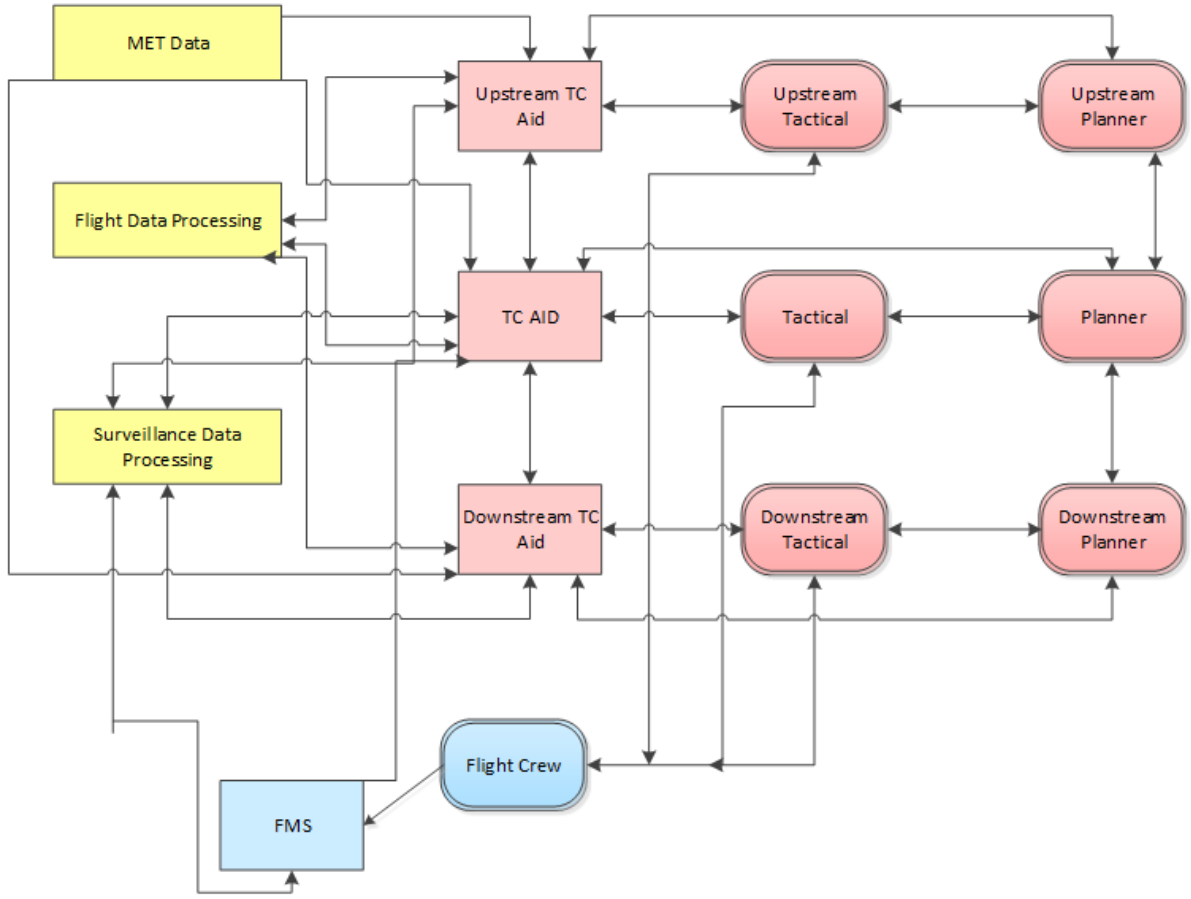


Figure 11: TC aid SPR level model

3.2.1.1 Aircraft Elements

The aircraft elements, presented in section 3.2.1 for all three operational services, are coloured in blue.

3.2.1.2 Ground Elements

The aircraft elements, presented in section 3.2.1 for all three operational services, are coloured in pink.

3.2.1.3 External Entities

The aircraft elements, presented in section 3.2.1 for all three operational services, are coloured in yellow.

3.2.2 Task Analysis

No Human Performance (HP) Assessment has been performed at this stage of the project.

3.2.3 Derivation of Safety Requirements (Functionality and Performance – success approach)

This section provides the safety requirements satisfying the safety objectives (functionality and performance) presented and derived in section 2. These safety requirements are defined at the level of the relevant elements of the SPR-level models shown in Figure 9, Figure 10 and Figure 11.

Table 20, Table 23, Table 26 show, for each of the three operational services, how the Safety Objectives map on to the related elements of the SPR-level Models.

Table 21, Table 24 and Table 27 shows the full list of requirements (and how they map on to the related elements of the SPR-level Models and on the SCSOs) identified in Table 20, Table 23 and Table 26.

Note it has been decided that the results from P04.03 EXE-VP798 will be included in this Safety Assessment. The exercise was designed to test the impact of the different Route Networks (DRA & FRA) and Separation Tools (MTCD, MONA & EAP) on KPAs/TAs. However, only the fixed route part of the concept is common between P04.07.02 and P04.03. As a consequence, only the results concerning the fixed route environment will be taken into consideration for this safety assessment. The key results are presented in the form of additional Success Case Safety Requirements in the section 3.2.3.4.

3.2.3.1 CD/R aid to TC

Safety Objectives *(success approach)*	**Requirement** *(forward reference)*	**Maps on to**
SCSO 11	It shall be possible for flights other than those in the sector to be recognised/made relevant in order that they are included in TC aid calculations.	FDPS > SDPS > TC Aid
	Where no CFL is available the tactical trajectory shall use the Entry flight level of the first controlled sector.	FDPS > SDPS > TC Aid
	The Tactical trajectory shall be updated by any clearances input into the TC Aid.	Executive > TC Aid > SDPS
	The TC Aid shall compare tactical trajectories between flights within the sector to predict the horizontal and vertical separation that will be achieved between them.	FDPS > SDPS > TC Aid
	The TC Aid shall detect any conflicting tactical trajectories within the minimum horizontal separation thresholds.	TC Aid
	The TC Aid shall display an alert to the controllers when any conflicting tactical trajectories are detected.	TC Aid > Executive > Planner
	For the identification of Tactical encounters a ground speed uncertainty shall be taken into account.	SDPS > TC Aid
	The controller shall be provided with all of the relevant	

	information needed for each encounter.	TC Aid > Executive
	The reaction time of the controller and flight crew shall be considered for the calculation of a tactical trajectory following a clearance.	Executive > Flight Crew > TC Aid
	The TC Aid shall display the conflicting trajectories on the situation display within x number of seconds (after the detection of the conflict) to the controller.	TC Aid > SDPS > Executive
SCSO 12	The TC Aid shall create a deviation trajectory if Flight Path Monitoring detects a Route deviation.	TC Aid > SDPS
	The TC Aid shall create a deviation trajectory if Flight Path Monitoring detects a Lateral deviation.	TC Aid > SDPS
	The TC Aid shall create a deviation trajectory if Flight Path Monitoring detects a Vertical Rate Deviation.	TC Aid > SDPS
	The TC Aid shall create a deviation trajectory if Flight Path Monitoring detects a CFL deviation.	TC Aid > SDPS
	The TC Aid shall create a deviation trajectory if Flight Path Monitoring detects a Speed Deviation.	TC Aid > SDPS
	The TC Aid shall create a deviation trajectory if Flight Path Monitoring detects that there is no valid flight plan data available.	TC Aid > SDPS
	The TC Aid shall alert the controller to any detected deviations via HMI on the radar display.	TC Aid > SDPS > ATCO CWP
	The TC Aid shall continuously monitor actual track data and controller clearance data.	TC Aid > SDPS
	The TC Aid shall detect deviations between controller clearance data and Mode S downlinked airborne parameters.	FMS > SDPS > TC Aid
SCSO 13	On request for a what-if probe for a heading or direct route the TC Aid shall display if that heading or direct route is conflict free.	TC Aid
SCSO 14	ATCOs shall be able to delete/supress/hide alerts.	Executive > TC Aid
SCSO 15	The TC Aid shall provide what-else probing.	TC Aid
	The TC Aid shall compare the proposed tactical trajectory of a subject flight against the actual traffic situation when the controller requests a what-if or what-else probe.	TC Aid
	On request for a what-else probe the TC Aid shall display if the flight levels are conflict free or not, and if a vertical rate is necessary to achieve the level.	Executive > SDPS
	On request for a what-else probe for headings or direct routes the TC Aid shall display if that headings or direct routes are conflict free.	Executive > SDPS

SCSO 16	The TC Aid shall be available at all controller workstations. It shall be possible to enable and disable the TC Aid.	TC Aid > ATCO CWP TC Aid > ATCO CWP

Table 19: Mapping of Safety Objectives to the SPR-level Model Elements – TC aid

The following table lists the safety requirements derived from Table 20: Mapping of Safety Objectives to the SPR-level Model Elements – TC aid for TC aid. They are presented per SPR-model elements. A reference to the corresponding Safety objective(s) is also provided. In case same[9] or similar[10] requirements are already present in the OSED [4] the corresponding reference has also been provided.

SR# [same or similar OSED req]	Requirement Text *[SPR Equivalent]*	Derived from
FDPS > SDPS > TC Aid		
SR-111	It shall be possible for flights other than those in the sector to be recognised/made relevant in order that they are included in TC aid calculations. *[REQ-04.07.02-SPR-CDR1.1010]*	SCSO 11
SR-113 [REQ-04.07.02-OSED-0001.3089]	Where no CFL is available the tactical trajectory shall use the Entry flight level of the first controlled sector. *[REQ-04.07.02-SPR-CDR1.1030]*	SCSO 11
SR-114	The TC Aid shall compare tactical trajectories between flights within the sector to predict the horizontal and vertical separation that will be achieved between them. *[REQ-04.07.02-SPR-CDR1.1050]*	SCSO 11
Executive > TC Aid > SDPS		
SR-115	The Tactical trajectory shall be updated by any clearances input into the TC Aid. *[REQ-04.07.02-SPR-CDR1.1040]*	SCSO 11
TC Aid		
SR-116	The TC Aid shall detect any conflicting tactical trajectories within the minimum horizontal separation thresholds. *[REQ-04.07.02-SPR-CDR1.1060]*	SCSO 11
SR-1110	On request for a what-if probe for a heading or direct route the TC Aid shall display if that heading or direct route is conflict free. *[REQ-04.07.02-SPR-CDR1.1260]*	SCSO 13
SR-1113	The TC Aid shall provide what-else probing. *[REQ-04.07.02-SPR-CDR1.1290]*	SCSO 15
SR-1114	The TC Aid shall compare the proposed tactical trajectory of a subject flight against the actual traffic situation when	SCSO 15

[9] *"Same"* in this case means that both the meaning and the text of the requirement are the same with the OSED Requirement.
[10] *"Similar"* in this case means that the meaning of the requirement is the same but the text is slightly different compared to the OSED Requirement.

	the controller requests a what-if or what-else probe. *[REQ-04.07.02-SPR-CDR1.1300]*	
TC Aid > Executive > Planner		
SR-1115	The TC Aid shall display an alert to the controllers when any conflicting tactical trajectories are detected. *[REQ-04.07.02-SPR-CDR1.1070]*	SCSO 11
SDPS > TC Aid		
SR-1116	For the identification of Tactical encounters a ground speed uncertainty shall be taken into account. *[REQ-04.07.02-SPR-CDR1.1080]*	SCSO 11
TC Aid > Executive		
SR-1117	The controller shall be provided with all of the relevant information needed for each encounter. *[REQ-04.07.02-SPR-CDR1.1090]*	SCSO 11
Executive > Flight Crew > TC Aid		
SR-1119	The TC Aid shall display the conflicting trajectories on the situation display within x number of seconds (after the detection of the conflict) to the controller. *[REQ-04.07.02-SPR-CDR1.1110]*	SCSO 11
TC Aid > SDPS		
SR-1120 [REQ-04.07.02-OSED-0001.2005]	The TC Aid shall create a deviation trajectory if Flight Path Monitoring detects a Route deviation. *[REQ-04.07.02-SPR-CDR1.1120]*	SCSO 12
SR-1122 [REQ-04.07.02-OSED-0001.3026]	The TC Aid shall create a deviation trajectory if Flight Path Monitoring detects a Vertical Rate Deviation. *[REQ-04.07.02-SPR-CDR1.1140]*	SCSO 12
SR-1124	The TC Aid shall create a deviation trajectory if Flight Path Monitoring detects a Speed Deviation. *[REQ-04.07.02-SPR-CDR1.1160]*	SCSO 12
FMS > SDPS > TC Aid		
SR-1130	The TC Aid shall detect deviations between controller clearance data and Mode S downlinked airborne parameters. *[REQ-04.07.02-SPR-CDR1.1220]*	SCSO 12
Executive > SDPS		
SR-1132	On request for a what-else probe the TC Aid shall display if the flight levels are conflict free or not, and if a vertical rate is necessary to achieve the level. *[REQ-04.07.02-SPR-CDR1.1320]*	SCSO 15
SR-1133 [REQ-04.07.02-	On request for a what-else probe for headings or direct routes the TC Aid shall display if that headings or direct	SCSO 15

OSED-0001.1001]	routes are conflict free. *[REQ-04.07.02-SPR-CDR1.1330]*	
TC Aid > ATCO CWP		
SR-1134 [REQ-04.07.02-OSED-0001.2001]	The TC Aid shall be available at all controller workstations. *[REQ-04.07.02-SPR-CDR1.1340]*	SCSO 16
SR-1135	It shall be possible to enable and disable the TC Aid. *[REQ-04.07.02-SPR-CDR1.1350]*	SCSO 16
Executive > TC Aid		
SR-1136	ATCOs shall be able to delete/supress/hide alerts. *[REQ-04.07.02-SPR-CDR1.1360]*	SCSO 14

Table 20: Derivation of Safety Requirements (success case) from Safety Objectives – TC aid

In order to provide a basis upon which the safety assessment was performed, the ATM Operational Concept & Environmental factors were discussed by the group. These are described below and captured as assumptions. Assumptions which are considered fundamental to the service will require subsequent validation in the project lifecycle. The selection of those assumptions which require validation will be down to the technical and operational experts.

In determining the assumptions a number of difficulties arose mainly due to the fact that there is expected to be a wide variation in the usage of these tools. The particular environment and sector traffic complexity will strongly influence how these tools will be employed. As the maturity of the service evolves these assumptions should be refined.

Assumptions for CD/R aid to TC are presented in Table 22.

ID	**Implementation Assumptions**
A 001	CD/R for TC is based on tactical trajectories that are clearance / surveillance based.
A 002	CD/R for TC (What-Else) will provide the controller with a view of possible clearances and will help the controller validate possible solutions.
A 003	CD/R for TC will detect conflicts 4 – 6 minutes in advance of a potential loss of separation.
A 004	CD/R for TC remains permanently "on".
A 005	CD/R for TC utilises data that is derived from Tactical or Deviation Trajectories.
A 006	Both the planner and tactical have access to the CD/R for TC toolset.
ID	**Actual Assumptions**
A 001	The detection of potential conflicts through (What-If) functionality will be provided through TDB alerts and associated strip highlights which will support the main tactical controlling task.
A 002	There is no facility for the controller to uplink planning amendments to the pilot.
A 003	TRACT and STCA shall be independent[11] (however, presentation to the controller may be harmonised)

[11] There is the possibility of interaction between STCA and CD/R for TC due to the fact that they occur in similar timeframes (STCA 0 – 2 minutes, CD/R for TC 0-6 minutes). To guard against

1208 **Table 21: Assumptions made in deriving the above Safety Requirements – TC aid**

1209 ### 3.2.3.2 CD/R aid to PC

Safety Objectives *(Functionality and Performance from success approach)*	**Requirement** *(forward reference)*	**Maps on to**
SCSO 21	The PC Aid shall make the controller aware to any planning encounters that are being monitored if they increase in severity.	PC Aid > FDPS > SDPS > PC Aid > Planner
	If a flight is involved in a planning encounter with more than one environmental flights these encounters will be displayed as individual pairs.	PC Aid > FDPS > SDPS > PC Aid
	The planner shall be able to distinguish which of the displayed encounters are pertinent through selective filtering functionality.	Planner > PC Aid
	ATCOs shall be able to delete/supress/hide alerts.	Planner > PC Aid
SCSO 22	The PC Aid shall continuously monitor any planning encounters within the sector.	PC Aid > FDPS > SDPS > PC Aid
	The PC Aid shall continuously display any planning encounters that are being monitored within the sector.	
	The PC Aid shall indicate any what-if encounters on the situation display and PC Aid tool displays when the Planner probes an alternative coordinated level, heading or direct route (i.e. a 'what-if' probe).	PC Aid > FDPS > SDPS > PC Aid
	The what-if encounters display will be removed from the situation display and tools on cessation of the 'what-if' probe, and the clearance will not be committed to the system.	Planner > PC Aid > SDPS
	The planner shall be able to commit the alternative coordination to the system by a specific action.	Planner > PC Aid > SDPS
	The revised coordination shall be indicated to the upstream planner and upstream Executive.	Planner > PC Aid > FDPS
		PC Aid > FDPS > Upstream

this it is assumed that they are independent. The Hazard Analysis later considers the possibility of overlap and proposes mitigations that STCA will overrule TC-Aid.

	The PC aid shall display the severity and geometry of each encounter that is displayed to the planner.	Planner > Upstream Executive FDPS > SDPS > PC Aid > Planner
SCSO 23	When a subject flight is selected, the PC Aid shall display to the planner any potential speculative encounters at all sector coordination entry and exit levels. All potential what-else encounters at every sector entry and exit flight level shall be displayed in elevation view to the Planner controller.	FDPS > PC Aid PC Aid > Planner
SCSO 24	The PC Aid shall alert the Planner controller if the system predicts the flight will not achieve coordinated exit flight level.	SDPS > PC Aid > Planner
SCSO 25	The PC Aid shall automatically coordinate flights into the sector without reference to the planner controller when the coordination passes the MTCD check. Where the coordination fails the MTCD check, the PC Aid shall refer the coordination offer to the Planner controller for manual assessment. The PC Aid shall automatically set the exit flight level for a flight without reference to the planner controller when the corresponding flight level passes the MTCD check. The PC Aid shall alert the planner to coordinate an exit flight level in the instances that the system does not do this automatically, or cannot find a suitable XFL. It shall be possible for the Planner to override any “integrated coordination” automatic coordination decision by the system. It shall be possible for the Planner to withdraw a coordination offer that has been made to the Downstream sector if this coordination is no longer relevant to that Downstream Sector. The PC Aid shall alert the planner to any coordination that have been rejected or revised by the downstream sector. Any rejected coordination shall be removed from the PC Aid consideration.	FDPS > PC Aid FDPS > PC Aid > Planner PC Aid > FDPS FDPS > PC Aid > Planner Planner > FDPS Planner > FDPS > Downstream Executive > Downstream Planner Downstream Planner > FDPS > PC Aid > Planner

		FDPS > PC Aid
SCSO 26	The planner shall be able to apply coordination constraints to the coordination trajectory to a flight as either a heading, speed or direct route instruction. The coordination trajectory and any TP and MTCD outputs shall be updated by the committal of coordination constraints.	PC Aid > SDPS PC Aid > SDPS
SCSO 27	The PC Aid shall alert the controller if the flight is deviating from the applied coordination constraints. The deviation alerts associated with coordination constraints shall be triggered at times/events appropriate to the controller role.	PC Aid > SDPS > PC Aid > Planner PC Aid > SDPS > PC Aid > Planner
SCSO 28	The PC Aid shall produce a coordination trajectory for every flight of interest to the sector as soon as the flight is recognised to the sector. The FDPS shall alert the ATCO that there is a new coordination offer for the sector via the PC Aid. The FDPS alert about the new coordination offer shall remain displayed until the Planner has taken some action to interrogate the new coordination offer. On interrogation of a coordination offer via what-if or what-else probe, the coordination trajectories of the subject flight and any environmental flights that form an encounter with the subject flight shall be displayed within x number of seconds. On cessation of the interrogation probe of the subject flight the coordination trajectories of that flight and any interacting environmental flights shall disappear. The Planner shall be able to reject a flight from the upstream sector if he decides that the coordination offer is unsuitable and/or unsafe for the traffic situation at that time. The Planner shall be able to revise the flight level of any coordination offer.	FDPS/SDPS > PC Aid FDPS > PC Aid > Planner PC Aid > Planner PC Aid > SDPS PC Aid > SDPS Planner > FDPS > Upstream Planner > Upstream Executive Planner > FDPS > Upstream Planner > Upstream Executive
SCSO 29	When the Planner probes a potential Exit flight level via the What-if or What-else, the PC Aid shall display to the Planner all other flights (context flights) that are between the entry level	

	and proposed exit flight level along the subject flight's trajectory. Context encounters shall be distinguishable from planning encounters.	PC Aid > SDPS PC Aid
SCSO 210	The planner shall be able to accept a flight via the PC aid which shall inform all relevant parties i.e. upstream planner and upstream executive. The time between which the planner points out encounters of tactical interest to the tactical workstation display shall be x number of seconds. The Executive and Planner shall be able to independently remove the coordination point out from their respective work positions.	Planner > FDPS > Upstream Executive > Upstream Planner PC Aid > SDPS Executive > Planner > PC Aid > SDPS
SCSO 211	The PC Aid shall be available continuously at all controller work positions, regardless of role assigned at that workstation. The controller shall have the ability to select or de-select the PC aid display.	PC Aid PC Aid
SCSO 212	The PC Aid shall highlight those flights that are Holding within the sector against every MTCD probe. The PC Aid shall highlight any unusual/unexpected flights operating within the sector against every MTCD probe.	PC Aid > Planner PC Aid > Planner

Table 22 Mapping of Safety Objectives to the SPR-level Model Elements – PC aid

The following table lists the safety requirements derived from Table 23 for PC aid. They are presented per SPR-model elements. A reference to the corresponding Safety objective(s) is also provided. In case same[12] or similar[13] requirements are already present in the OSED [4] the corresponding reference has also been provided.

SR# [same or similar OSED req]	**Requirement Text *[SPR Equivalent]***	**Derived from**
PC Aid > FDPS > SDPS > PC Aid		
SR-211	The PC Aid shall continuously monitor any planning encounters within the sector. *[REQ-04.07.02-SPR-CDR2.1010]*	SCSO 22

[12] *"Same"* in this case means that both the meaning and the text of the requirement are the same with the OSED Requirement.
[13] *"Similar"* in this case means that the meaning of the requirement is the same but the text is slightly different compared to the OSED Requirement.

SR-212	The PC Aid shall continuously display any planning encounters that are being monitored within the sector. *[REQ-04.07.02-SPR-CDR2.1020]*	SCSO 22
SR-214	If a flight is involved in a planning encounter with more than one environmental flights these encounters will be displayed as individual pairs. *[REQ-04.07.02-SPR-CDR2.1050]*	SCSO 21
PC Aid > FDPS > SDPS > PC Aid > Planner		
SR-215	The PC Aid shall make the controller aware to any planning encounters that are being monitored if they increase in severity. *[REQ-04.07.02-SPR-CDR2.1030]*	SCSO 21
Planner > PC Aid > SDPS		
SR-216	The PC Aid shall indicate any what-if encounters on the situation display and PC Aid tool displays when the Planner probes an alternative coordinated level, heading or direct route (i.e. a 'what-if' probe). *[REQ-04.07.02-SPR-CDR2.1060]*	SCSO 22
SR-217	The what-if encounters display will be removed from the situation display and tools on cessation of the 'what-if' probe, and the clearance will not be committed to the system. *[REQ-04.07.02-SPR-CDR2.1070]*	SCSO 22
Planner > PC Aid > FDPS		
SR-218	The planner shall be able to commit the alternative coordination to the system by a specific action. *[REQ-04.07.02-SPR-CDR2.1080]*	SCSO 22
PC Aid > FDPS > Upstream Planner > Upstream Executive		
SR-219	The revised coordination shall be indicated to the upstream planner and upstream Executive. *[REQ-04.07.02-SPR-CDR2.1090]*	SCSO 22
FDPS > SDPS > PC Aid > Planner		
SR-2110	The PC aid shall display the severity and geometry of each encounter that is displayed to the planner. *[REQ-04.07.02-SPR-CDR2.1100]*	SCSO 22
FDPS > PC Aid		
SR-2111	When a subject flight is selected, the PC Aid shall display to the planner any potential speculative encounters at all sector coordination entry and exit levels. *[REQ-04.07.02-SPR-CDR2.1110]*	SCSO 23
SR-2112 [REQ-04.07.02-OSED-0002.3056]	The PC Aid shall automatically coordinate flights into the sector without reference to the planner controller when the coordination passes the MTCD check. *[REQ-04.07.02-SPR-CDR2.1140]*	SCSO 25

SR-2113	Any rejected coordination shall be removed from the PC Aid consideration. *[REQ-04.07.02-SPR-CDR2.1210]*	SCSO 25
PC Aid > Planner		
SR-2114 [REQ-04.07.02-OSED-0002.2016]	All potential what-else encounters at every sector entry and exit flight level shall be displayed in elevation view to the Planner controller. *[REQ-04.07.02-SPR-CDR2.1120]*	SCSO 23
SR-2115	The FDPS alert about the new coordination offer shall remain displayed until the Planner has taken some action to interrogate the new coordination offer. *[REQ-04.07.02-SPR-CDR2.1280]*	SCSO 28
SR-2116	The PC Aid shall highlight those flights that are Holding within the sector against every MTCD probe. *[REQ-04.07.02-SPR-CDR2.1420]*	SCSO 212
SR-2117	The PC Aid shall highlight any unusual/unexpected flights operating within the sector against every MTCD probe. *[REQ-04.07.02-SPR-CDR2.1430]*	SCSO 212
SDPS > PC Aid > Planner		
SR-2118	The PC Aid shall alert the Planner controller if the system predicts the flight will not achieve coordinated exit flight level. *[REQ-04.07.02-SPR-CDR2.1130]*	SCSO 24
FDPS > PC Aid > Planner		
SR-2119	Where the coordination fails the MTCD check, the PC Aid shall refer the coordination offer to the Planner controller for manual assessment. *[REQ-04.07.02-SPR-CDR2.1150]*	SCSO 25
SR-2120	The PC Aid shall alert the planner to coordinate an exit flight level in the instances that the system does not do this automatically, or cannot find a suitable XFL. *[REQ-04.07.02-SPR-CDR2.1170]*	SCSO 25
SR-2121	The FDPS shall alert the ATCO that there is a new coordination offer for the sector via the PC Aid. *[REQ-04.07.02-SPR-CDR2.1270]*	SCSO 28
PC Aid > FDPS		
SR-2122 [REQ-04.07.02-OSED-0002.4016]	The PC Aid shall automatically set the exit flight level for a flight without reference to the planner controller when the corresponding flight level passes the MTCD check. *[REQ-04.07.02-SPR-CDR2.1160]*	SCSO 25
Planner > FDPS		
SR-2123	It shall be possible for the Planner to override any “integrated coordination” automatic coordination decision by the system. *[REQ-04.07.02-SPR-CDR2.1180]*	SCSO 25

Planner > FDPS > Downstream Executive > Downstream Planner		
SR-2124	It shall be possible for the Planner to withdraw a coordination offer that has been made to the Downstream sector if this coordination is no longer relevant to that Downstream Sector. *[REQ-04.07.02-SPR-CDR2.1190]*	SCSO 25
Downstream Planner > FDPS > PC Aid > Planner		
SR-2125	The PC Aid shall alert the planner to any coordination that have been rejected or revised by the downstream sector. *[REQ-04.07.02-SPR-CDR2.1200]*	SCSO 25
PC Aid > SDPS		
SR-2126	The planner shall be able to apply coordination constraints to the coordination trajectory to a flight as either a heading, speed or direct route instruction. *[REQ-04.07.02-SPR-CDR2.1220]*	SCSO 26
SR-2127	The coordination trajectory and any TP and MTCD outputs shall be updated by the committal of coordination constraints. *[REQ-04.07.02-SPR-CDR2.1230]*	SCSO 26
SR-2129	On interrogation of a coordination offer via what-if or what-else probe, the coordination trajectories of the subject flight and any environmental flights that form an encounter with the subject flight shall be displayed within x number of seconds. *[REQ-04.07.02-SPR-CDR2.1300]*	SCSO 28
SR-2130	On cessation of the interrogation probe of the subject flight the coordination trajectories of that flight and any interacting environmental flights shall disappear. *[REQ-04.07.02-SPR-CDR2.1310]*	SCSO 28
SR-2131	When the Planner probes a potential Exit flight level via the What-if or What-else, the PC Aid shall display to the Planner all other flights (context flights) that are between the entry level and proposed exit flight level along the subject flight's trajectory. *[REQ-04.07.02-SPR-CDR2.1340]*	SCSO 29
SR-2132	The time between which the planner points out encounters of tactical interest to the tactical workstation display shall be x number of seconds. *[REQ-04.07.02-SPR-CDR2.1380]*	SCSO 210
PC Aid > SDPS > PC Aid > Planner		
SR-2133	The PC Aid shall alert the controller if the flight is deviating from the applied coordination constraints. *[REQ-04.07.02-SPR-CDR2.1240]*	SCSO 27
SR-2134	The deviation alerts associated with coordination constraints shall be triggered at times/events appropriate to the controller role. *[REQ-04.07.02-SPR-CDR2.1250]*	SCSO 27

FDPS/SDPS > PC Aid		
SR-2135	The PC Aid shall produce a coordination trajectory for every flight of interest to the sector as soon as the flight is recognised to the sector. *[REQ-04.07.02-SPR-CDR2.1260]*	SCSO 28
Planner > FDPS > Upstream Planner > Upstream Executive		
SR-2136	The Planner shall be able to reject a flight from the upstream sector if he decides that the coordination offer is unsuitable and/or unsafe for the traffic situation at that time. *[REQ-04.07.02-SPR-CDR2.1320]*	SCSO 28
SR-2137	The Planner shall be able to revise the flight level of any coordination offer. *[REQ-04.07.02-SPR-CDR2.1330]*	SCSO 28
Planner > FDPS > Upstream Executive > Upstream Planner		
SR-2138	The planner shall be able to accept a flight via the PC aid which shall inform all relevant parties i.e. upstream planner and upstream executive. *[REQ-04.07.02-SPR-CDR2.1360]*	SCSO 210
Executive > Planner > PC Aid > SDPS		
SR-2140	The Executive and Planner shall be able to independently remove the coordination point out from their respective work positions. *[REQ-04.07.02-SPR-CDR2.1390]*	SCSO 210
PC Aid		
SR-2141	The PC Aid shall be available continuously at all controller work positions, regardless of role assigned at that workstation. *[REQ-04.07.02-SPR-CDR2.1400]*	SCSO 211
SR-2142	The controller shall have the ability to select or de-select the PC aid display. [REQ-04.07.02-SPR-CDR2.1410]	SCSO 211
SR-2143	Context encounters shall be distinguishable from planning encounters. *[REQ-04.07.02-SPR-CDR2.1350]*	SCSO 29
Planner > PC Aid		
SR-2144	The planner shall be able to distinguish which of the displayed encounters are pertinent through selective filtering functionality. *[REQ-04.07.02-SPR-CDR2.1440]*	SCSO 21
SR-2145	ATCOs shall be able to delete/supress/hide alerts. *[REQ-04.07.02-SPR-CDR2.1450]*	SCSO 21

Table 23 Derivation of Safety Requirements (success case) from Safety Objectives – PC aid

In order to provide a basis upon which safety was to be assessed, the ATM Operational Concept & Environmental factors were discussed by the group. These are described below and captured as assumptions. Assumptions which are considered fundamental to the service will require subsequent validation in the project lifecycle. The selection of those assumptions which require validation will be down to the technical and operational experts.

There are a number of alternative implementations of CD/R aid to PC, Table 25 describes which assumptions are believed to be common across those solutions.

In determining the assumptions, a number of difficulties arose mainly due to the fact that there is expected to be a wide variation in usage of these tools. The specifics of the environment and sector traffic complexity will strongly influence how these tools will be employed. As the maturity of the service evolves these assumptions should be refined.

ID	Implementation Assumptions
A 001	CD/R for PC is based on planned flight data behaviour between sectors.
A 002	CD/R for PC utilises data that is derived from planning trajectories (when transitioning levels), which is constrained to the agreed lateral, sector exit and entry levels co-ordinations.
A 003	CD/R for PC utilises data that is derived from co-ordination trajectories (when considering entry and exit conditions).
A 004	CD/R for PC remains permanently "on".
A 005	Modifications made by the planner will update the tactical toolset appropriately (data is synchronised).
A 006	The receiving planner flight level is the same as the offering planner flight level (and other coordination constraints).
A 007	Trajectories do not model CTOs (TRACT constraint).
ID	**Actual Assumptions**
A 001	Both the planner and tactical have access to the CD/R for PC toolset.
A 002	There is no facility for the controller to uplink planning amendments to the pilot.
A 003	It is expected that planner and tactical controller sector pairs will continue to have defined separation controlling tasks despite the potential implementation of MSP.
A 004	The TC aid tools are independent of the PC Aid (and TRACT).

Table 24 Assumptions made in deriving the above Safety Requirements – PC aid

3.2.3.3 TRACT

Safety Objectives *(Functionality and Performance from success approach)*	**Requirement** *(forward reference)*	**Maps on to**
SCSO 31	TRACT shall assess the eligibility of all flights of the whole traffic set.	FDPS
	TRACT shall consider the traffic set made of all flight plan data from the FDPS Area of Interest.	FDPS
	TRACT shall compute a global resolution by the application of a CTO to those flights that are eligible.	TRACT/ADS-C
	The TRACT service shall compute a solution that	TRACT/PLANNER/E

	maintains or improves the controller's situational awareness. TRACT shall send a CTO to the aircraft via datalink.	XECUTIVE TRACT/CPDLC
SCSO 32	TRACT shall assess the whole of the traffic set (both eligible and non-eligible aircraft) to detect encounters between pairs of aircraft. TRACT shall solve encounters periodically without creating any new unsolved ones.	TRACT TRACT
SCSO 33	TRACT shall warn the controllers when a CTO is not implemented as expected or when any aircraft involved in a TRACT solution deviates from its trajectory.	TRACT/ATCO CWP
SCSO 34	TRACT shall not attempt to solve a confliction where convergences or divergences between a pair of aircraft are of a small angle. TRACT shall apply CTOs on trajectory points that are aligned on the aircraft's FMS trajectory. TRACT shall only issue CTOs that are achievable by small speed adjustments.	TRACT FMS TRACT/ADS-C
SCSO 35	The controller shall be informed via HMI to the fact that an aircraft is under a TRACT resolution. The status of the TRACT resolution shall be displayed to the controller. The TRACT resolution indicator shall not be able to be directly removed by the controllers unless they are discarding the TRACT solution. It shall be clear to the controller which aircraft pairs are involved in conflict resolution. If there is no answer from the flight crew, TRACT shall consider the answer to be 'STAND BY'.	TRACT/ATCO CWP TRACT/ATCO CWP PLANNER/EXECUTIVE/ATCO CWP PLANNER/EXECUTIVE/ATCO CWP FLIGHT CREW/CPDLC
SCSO 36	The flight crew shall assess the eligibility of the CTO before committing to the CTO. The ATCO shall have access to the position and time of any CTO. The flight crew shall have the ability to accept or reject the CTO. The flight crew shall have the ability to reply 'STAND BY' if they need more time to consider the acceptability of the CTO. If the flight crew respond with an 'UNABLE' reply to the CTO, TRACT shall uplink a cancellation message to all	FLIGHT CREW/CPDLC/FMS ADS-C/TRACT/PLANNER/EXECUTIVE FLIGHT CREW/CPDLC/FMS FLIGHT CREW/CPDLC/FMS FLIGHT CREW/FMS/ADS-C

	other aircraft with a CTO in the cluster. If the flight crew respond with an 'UNABLE' reply to the CTO, TRACT shall not attempt to send another CTO to the aircraft for at least X (e.g. 15) minutes depending on the ANSP's off-line configuration.	FLIGHT CREW/FMS/ADS-C
SCSO 37	TRACT shall consider any flight that is already subject to an AMAN Time constraint as ineligible for a CTO. TRACT shall cross check with the FMS to see if the flight is already subject to an AMAN time constraint. TRACT shall only consider those flights to be eligible that are i4D equipped.	TRACT/AMAN TRACT/AMAN/FMS TRACT/FMS
SCSO 38	TRACT shall discard/delete a resolution whenever the ATCO issues a clearance to change the behaviour of an aircraft under a TRACT resolution. TRACT shall alert the flight crew when the TRACT resolution has been discarded. Any HMI indication related to a TRACT solution shall be removed whenever TRACT discards that solution. TRACT shall alert the ATCO when the TRACT resolution has been discarded.	TRACT/EXECUTIVE TRACT/FLIGHT CREW TRACT/ATCO CWP TRACT/EXECUTIVE /PLANNER

Table 25 Mapping of Safety Objectives to the SPR-level Model Elements – TRACT

The following table lists the safety requirements derived from Table 26 for TRACT. They are presented per SPR-model elements. A reference to the corresponding Safety objective(s) is also provided. In case same[14] or similar[15] requirements are already present in the OSED [4] the corresponding reference has also been provided.

SR# [same or similar OSED req]	**Requirement Text *[SPR Equivalent]***	**Derived from**
FDPS		
SR-311	TRACT shall assess the eligibility of all flights of the whole traffic set. *[REQ-04.07.02-SPR-TRA3.1010]*	SCSO 31
SR-312	TRACT shall consider the traffic set made of all flight plan data from the FDPS Area of Interest. *[REQ-04.07.02-SPR-TRA3.1020]*	SCSO 31
TRACT/ADS-C		
SR-313	TRACT shall compute a global resolution by the application of a CTO to those flights that are eligible. *[REQ-04.07.02-SPR-TRA3.1030]*	SCSO 31

[14] *"Same"* in this case means that both the meaning and the text of the requirement are the same with the OSED Requirement.
[15] *"Similar"* in this case means that the meaning of the requirement is the same but the text is slightly different compared to the OSED Requirement.

SR-314	TRACT shall only issue CTOs that are achievable by small speed adjustments. *[REQ-04.07.02-SPR-TRA3.1120]*	SCSO 34
TRACT/PLANNER/EXECUTIVE		
SR-315 [REQ-04.07.02-OSED-0003.3062]	The TRACT service shall compute a solution that maintains or improves the controller's situational awareness. *[REQ-04.07.02-SPR-TRA3.1040]*	SCSO 31
TRACT/CPDLC		
SR-316	TRACT shall send a CTO to the aircraft via datalink. *[REQ-04.07.02-SPR-TRA3.1050]*	SCSO 31
TRACT		
SR-317 [REQ-04.07.02-OSED-0003.2018]	TRACT shall assess the whole of the traffic set (both eligible and non-eligible aircraft) to detect encounters between pairs of aircraft. *[REQ-04.07.02-SPR-TRA3.1060]*	SCSO 32
SR-318 [REQ-04.07.02-OSED-0003.2031]	TRACT shall solve encounters periodically without creating any new unsolved ones. *[REQ-04.07.02-SPR-TRA3.1070]*	SCSO 32
SR-3110 [REQ-04.07.02-OSED-0003.3080]	TRACT shall not attempt to solve a confliction where convergences or divergences between a pair of aircraft are of a small angle. *[REQ-04.07.02-SPR-TRA3.1100]*	SCSO 34
TRACT/ATCO CWP		
SR-3111 [REQ-04.07.02-OSED-0003.5005]	TRACT shall warn the controllers when a CTO is not implemented as expected or when any aircraft involved in a TRACT solution deviates from its trajectory. *[REQ-04.07.02-SPR-TRA3.1080]*	SCSO 33
SR-3112	The controller shall be informed via HMI to the fact that an aircraft is under a TRACT resolution. *[REQ-04.07.02-SPR-TRA3.1130]*	SCSO 35
SR-3113	The status of the TRACT resolution shall be displayed to the controller. *[REQ-04.07.02-SPR-TRA3.1140]*	SCSO 35
SR-3114	Any HMI indication related to a TRACT solution shall be removed whenever TRACT discards that solution. *[REQ-04.07.02-SPR-TRA3.1310]*	SCSO 38
FMS		
SR-3115	TRACT shall apply CTOs on trajectory points that are aligned on the aircraft's FMS trajectory. *[REQ-04.07.02-SPR-TRA3.1110]*	SCSO 34
PLANNER/EXECUTIVE/ATCO CWP		
SR-3116	The TRACT resolution indicator shall not be able to be directly removed by the controllers unless they are	SCSO 35

	discarding the TRACT solution. *[REQ-04.07.02-SPR-TRA3.1150]*	
SR-3117	It shall be clear to the controller which aircraft pairs are involved in conflict resolution. *[REQ-04.07.02-SPR-TRA3.1160]*	SCSO 35
FLIGHT CREW/CPDLC		
SR-3118 [REQ-04.07.02-OSED-0003.4026]	If there is no answer from the flight crew, TRACT shall consider the answer to be 'STAND BY'. *[REQ-04.07.02-SPR-TRA3.1170]*	SCSO 35
FLIGHT CREW/CPDLC/FMS		
SR-3119	The flight crew shall assess the eligibility of the CTO before committing to the CTO. *[REQ-04.07.02-SPR-TRA3.1180]*	SCSO 36
SR-3120	The flight crew shall have the ability to accept or reject the CTO. *[REQ-04.07.02-SPR-TRA3.1200]*	SCSO 36
SR-3122	The flight crew shall have the ability to reply 'STAND BY' if they need more time to consider the acceptability of the CTO. *[REQ-04.07.02-SPR-TRA3.1220]*	SCSO 36
ADS-C/TRACT/PLANNER/EXECUTIVE		
SR-3123	The ATCO shall have access to the position and time of any CTO. *[REQ-04.07.02-SPR-TRA3.1190]*	SCSO 36
FLIGHT CREW/FMS/ADS-C		
SR-3124	If the flight crew respond with an 'UNABLE' reply to the CTO, TRACT shall uplink a cancellation message to all other aircraft with a CTO in the cluster. *[REQ-04.07.02-SPR-TRA3.1230]*	SCSO 36
SR-3125 [REQ-04.07.02-OSED-0003.4028]	If the flight crew respond with an 'UNABLE' reply to the CTO, TRACT shall not attempt to send another CTO to the aircraft for at least X (e.g. 15) minutes depending on the ANSP's off-line configuration. *[REQ-04.07.02-SPR-TRA3.1240]*	SCSO 36
TRACT/AMAN		
SR-3126	TRACT shall consider any flight that is already subject to an AMAN Time constraint as ineligible for a CTO. *[REQ-04.07.02-SPR-TRA3.1250]*	SCSO 37
TRACT/AMAN/FMS		
SR-3127	TRACT shall cross check with the FMS to see if the flight is already subject to an AMAN time constraint. *[REQ-04.07.02-SPR-TRA3.1260]*	SCSO 37
TRACT/FMS		

SR-3128 [REQ-04.07.02-OSED-0003.5001]	TRACT shall only consider those flights to be eligible that are i4D equipped. *[REQ-04.07.02-SPR-TRA3.1270]*	SCSO 37
TRACT/EXECUTIVE		
SR-3130	TRACT shall discard/delete a resolution whenever the ATCO issues a clearance to change the behaviour of an aircraft under a TRACT resolution. *[REQ-04.07.02-SPR-TRA3.1290]*	SCSO 38
TRACT/FLIGHT CREW		
SR-3131	TRACT shall alert the flight crew when the TRACT resolution has been discarded. *[REQ-04.07.02-SPR-TRA3.1300]*	SCSO 38
TRACT/EXECUTIVE/PLANNER		
SR-3132	TRACT shall alert the ATCO when the TRACT resolution has been discarded. *[REQ-04.07.02-SPR-TRA3.1320]*	SCSO 38

Table 26 Derivation of Safety Requirements (success case) from Safety Objectives - TRACT

In order to provide a basis upon which the safety assessment was to be performed, the ATM Operational Concept & Environmental factors were discussed by the group. These are described below and captured as assumptions. Assumptions which are considered fundamental to the service will require subsequent validation in the project lifecycle. The selection of those assumptions which require validation will be down to the technical and operational experts.

In determining the assumptions a number of difficulties arose mainly due to the fact that there is expected to be a wide variation of usage of these tools. The particular environment and sector traffic complexity will strongly influence how these tools will be employed. As the maturity of the service evolves these assumptions should be refined.

Assumptions for TRACT are presented in Table 28 below.

ID	Assumptions
A 001	Apparent separation will be achieved at the TRACT horizon which could be inside or outside of the sector of interest. This shall be achieved between 25 and 6 minutes prior to potential loss of separation.
A 002	TRACT will operate on conflicts with a time horizon of between 25 minutes to 15 minutes, to avoid overlap with the planner tasks.
A 003	TRACT will require no ATCO interaction.
A 004	Speed variation will be between ±5%.
A 005	Speed adjustments may be applied to either one or more aircraft within a cluster.
A 006	All aircraft that are the subject of a TRACT resolution will be highlighted to the tactical and planner controllers irrespective of whether the aircraft is subject to a speed adjustment.
A 007	When conflicts are being solved the TRACT solution takes into account all aircraft that are predicted to be within the wider region.

A 008	There is no limit to the number of aircraft that could be under TRACT control within a sector.
A 009	Failure to receive a CTO authorise / reject response from the pilot within 3 minutes will result in the request assumed to be STAND BY.
A 010	All requests will be accepted / rejected via datalink.
A 011	Controllers will be able to determine which aircraft pairs are subject to TRACT.
A 012	Pilots of aircraft not subject to a CTO (but nonetheless part of a TRACT conflict resolution) will maintain the aircraft's existing speed schedule and route.
A 013	MTCD shall take into account the resolutions provided by TRACT to ensure that TRACT and MTCD use consistent information.
A 014	~~The speed adjustments made by the FMS are made gradually and there are no step changes in aircraft speed necessary to achieve the CTO.~~[16]
A 015	Controllers can obtain information on the nature of the speed change and location of the CTO.
A 016	TRACT adjustments are limited to amendments in aircraft speed made through the issuing of CTOs to the target aircraft.
A 017	TRACT resolutions are to be considered as advisory.
A 018	Once a TRACT resolution has been initiated for a pair of aircraft it will be implemented unless overridden by the ATCO.
A 019	The FMS adjustments are implemented in such a way that they do not impede the predictability of aircraft trajectories which will aid controller situation awareness.
A 020	TRACT remains permanently "on".
A 021	ATCOs will not be negatively influenced by aircraft indicated to be under TRACT resolution (this is an operational assumption)

Table 27 Assumptions made in deriving the above Safety Requirements - TRACT

Note: It was noted that to address the hazard of the aircraft not under a CTO (but part of a TRACT resolution) deviating from their assumed speed it might be necessary to derive a safety requirement that increases the separation buffer to the extent that this hazard is mitigated. However this level of detail is beyond the scope of the task at this stage of the project's lifecycle, and it is therefore recorded here for future work to reference.

3.2.3.4 Conflict Detection in Fixed Route

Note this section refers to the results gathered from VP-798 which took place under P04.03. Note also there was no VALR for VP-798 at the time this SAR was produced. All the requirements were extracted from the key results presented in a Webex (attendees are presented below) on the 2nd June 2016 – a rationale for the specific requirement was also provided in order to make the provenience of the requirements clearer.

Webex attendees:

[16] Superseded by A 018.

- Adrien Jarry – DSNA;
- David Bole Richard – DSNA;
- Pascal Deketelaere – DSNA;
- Fabrice Cauchard – DSNA;
- Paul Repper – NATS;
- Mihai Ogica – Think Research on behalf of NATS.

SR# [same or similar OSED req]	Requirement Text *[SPR Equivalent]*	Derived from	Rationale
SR-411	The conflict detection function shall compute at its defined look ahead time, whatever the CWP display setting or configuration.	SCSO 21 SCSO 23	The aim is to ensure a permanent computation / automatic detection whatever the HMI configuration of the CWP (especially regarding the display settings). Thus, the system is still able to trigger an (critical) alert. For example, if the ATCO reduces the time horizon of the MTCD to 10min (from the HMI, i.e. reducing the timeline of the agenda), the MTCD capability of detection will not be impacted as it will still be able to detect conflicts at a 15 min (for example) time horizon and it will still be able to integrate the conflict information in a different part of the CWP HMI such as in label or flight leg.
SR-412	The conflict detection's Trajectory Prediction function shall take into account accurate flight data (such as aircraft speed).	SCSO 28	False and missed detections due to TP inaccuracy (e.g. inaccurate SPD data) need to be avoided, especially when the time horizon is close to the current time.
SR-413	The conflict detection's upper bounds of the look ahead time shall be at least 15 minutes.	SCSO 21 SCSO 23	In the reference scenario (i.e. without MTCD) the PC is

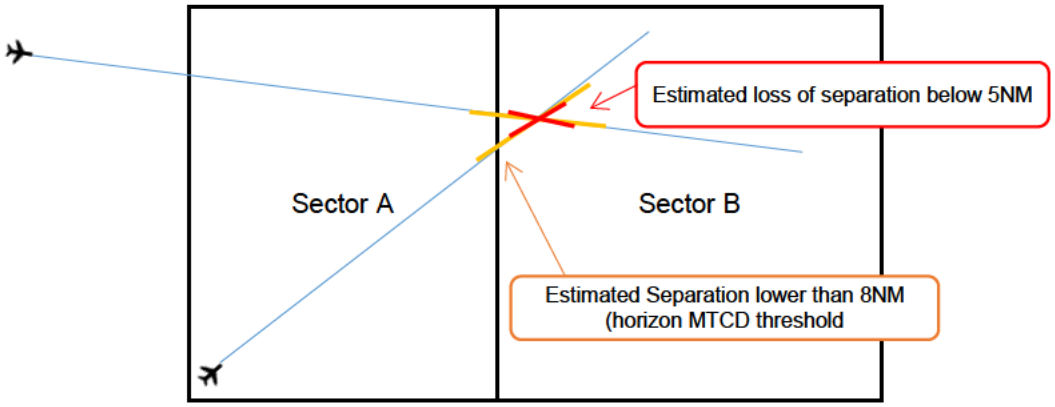
			working at a look ahead time at or above 15 minutes. Thus, the MTCD shall do the same; otherwise its added-value will be very limited. A look ahead time lower than 10 minutes is starting to be too close to the "tactical" horizon of the conflict detection (i.e. the TCT based on aircraft attitude is starting to be more relevant than the MTCD based on planned trajectory).
SR-414	The conflict detection's lower bounds of the look ahead time shall be consistent with the upper bounds of the TCT look ahead time.	SCSO 21 SCSO 23	Clutter due to displaying the same conflicts by two separate tools needs to be avoided. Otherwise this can create loss of situational awareness. Also, the MTCD's operational performance of detecting conflicts might start to be less relevant or accurate compared to the one proposed by a Tactical Controller Tool (i.e. the TCT based on aircraft attitude is starting to be more relevant instead of the MTCD based on planned trajectory).
SR-415	The conflict notification filters shall reflect individual sector adaptations.	SCSO 21 SCSO 22 SCSO 23	Conflicts under / over filtering will be avoided in order to prevent missing conflicts or a loss of situational awareness.
SR-416	The conflict detection function shall inform the controller about each potential loss of separation within the AOR & AOI, involving at least one distributed flight.	SCSO 21 SCSO 22 SCSO 23	Specific conflict cases where the conflict's location is too close to a sector boundary and where a coordination may be required to

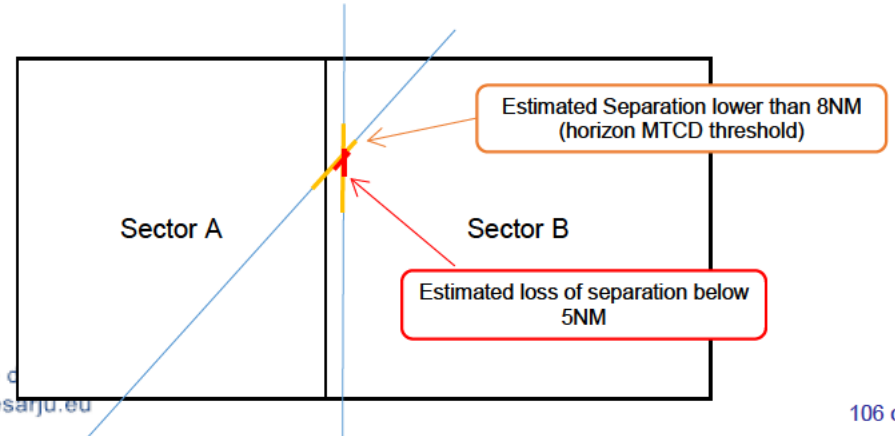
			manage these conflicts are included by this requirement. Refer to the illustrations in section 3.2.3.4.1.
SR-417	The HMI shall classify data blocks by priority and/or severity order.	SCSO 21 SCSO 22 SCSO 23	The conflict detection tool will enhance the controller's situational awareness and will help the controller in assessing the severity of each encounter.
SR-418	The system (MTCD and its HMI) shall support the ATCO to mentally represent the geometry of a conflict.	SCSO 22	The controller's situational awareness and decision making will be enhanced by the tool through helping the controller to mentally represent the conflict geometry.

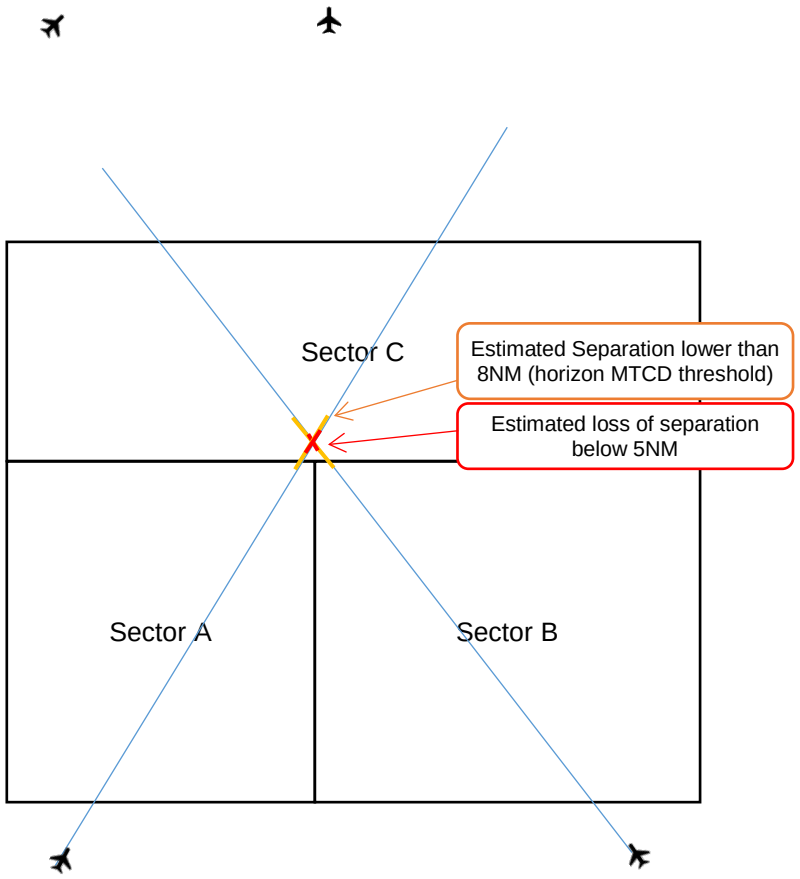
Table 28 Additional Success Case Safety Requirements following VP-798

3.2.3.4.1 Explanation for SR-416

Illustrations for SAR-416: In these cases, below sector A shall be aware of sector B's issues to anticipate the need of coordination (better situational awareness for PC of sector A).







3.3 Analysis of the SPR-level Model – Normal Operational Conditions

This section aims to ensure that the SPR-level design is complete, correct and internally coherent with respect to the safety requirements derived for the normal operating conditions that were used to develop the corresponding safety objectives in section 2.6.1.

The analysis necessarily depends on proving the Safety Requirements from three perspectives:

- a static view of the system behaviour using a Thread Analysis technique presented in A.1;
- check that the system design operates in a way that does not have a negative effect on the operation of related ground-based and airborne safety nets;
- a dynamic view of the system behaviour using validation exercises.

3.3.1 Scenarios for Normal Operations

Table 30, Table 31 and Table 32 are presenting the scenarios (developed in accordance with the SRM [1]) used to assess the completeness of the safety requirements for normal operations.

Note since it has been considered that the OSED use cases did not cover all the aspects from a safety perspective, it has been decided that these scenarios will be used instead of the OSED use cases.

The scenarios for normal operations obtained for TRACT are the following ones:

ID	Scenario	Rationale for the Choice
1	*TRACT Resolves a conflict*	Complete list of scenarios to help identify safety requirements and possible hazard causes.
	a) Alternative flow 1: Flight already has a CTO	
	b) Alternative flow 2: Aircrew cannot accept CTO	
	c) Alternative flow 3: Aircrew reply standby to the CTO	
2	*TRACT discards a TRACT Flight*	
	a) Alternative Flow 1: The primary TRACT flight to discard has no CTO	
	b) Alternative Flow 2: The secondary TRACT flight to discard has no CTO	
	c) Alternative Flow 3: The secondary TRACT flight is involved in another TRACT resolution	
	d) Failure Flow 1: The EPP data still contains the CTO	

1321 **Table 29: Operational Scenarios – Normal Conditions TRACT**

1322 The scenarios for normal operations obtained for the PC aid are the following ones:

ID	Scenario	Rationale for the Choice
1	*Entry Coordination*	Complete list of scenarios to help identify safety requirements and possible hazard causes.
	a) Alternative Flow 1: Revised Coordination	
	b) Alternative Flow 2: Discussion with Executive	
2	*Exit Coordination – Nominal scenario*	
	a) Alternative Flow 1 – Revision from downstream planner	
	b) Alternative Flow 2 – Rejection from downstream planner	
	c) Alternative Flow 3 – After level has been accepted you have to withdraw offer to downstream planner	
	d) Alternative Flow 4: After exit flight level has been accepted, planner wants to revise exit level	
3	*Encounter arises with already accepted coordination*	
4	*Integrated Coordination – Entry Boundary*	
5	*Integrated Coordination – Exit Boundary*	

Table 30 Operational Scenarios – Normal Conditions PC aid

The scenarios for normal operations obtained for the TC aid are the following ones:

ID	Scenario	Rationale for the Choice
1	*TC Aid detects conflicts between 2 aircraft*	Complete list of scenarios to help identify safety requirements and possible hazard causes.
	a) Alternative Flow 1: Conflict is not relevant	
	b) Failure Flow 1: Warning is not valid	
	c) Failure Flow 2: TC ignores warning	
2	*Conflict resolution with what-else probing*	
3	*Detection of Deviations with MONA*	
	a) Alternative Flow 1: MONA is not valid	

Table 31 Operational Scenarios – Normal Conditions TC aid

For a complete understanding of the flow of the scenarios for each operational service please see Appendix A.

3.3.2 Thread Analysis of the SPR-level Model – Normal Operations

Thread Analysis uses a particular graphical presentation in which the actions of the individual elements of the SPR-level Model, and the interactions between those elements, are represented as a continuous 'thread', from initiation to completion. These threads were used to identify the safety requirements presented in section 3.2.3.

The thread analysis of the several scenarios for normal operations listed in previous section is presented in Appendix A.

3.3.3 Effects on Safety Nets – Normal and Abnormal Operational Conditions

The potential ground-based/airborne safety nets that are used to provide services in the En Route environment will remain the same regardless of the implementation of the "Conflict Detection, Resolution and Monitoring" concept.

TRACT and the PC aid tool are not designed to interfere with the functional parameters of the current existing safety nets hence the new concept will have no operational impact on the safety nets. There is the possibility of interaction between STCA and CD/R for TC due to the fact that they occur in similar timeframes (STCA 0 – 2 minutes, CD/R for TC 0-6 minutes). To guard against this it is assumed that they are independent. This possibility of overlap between the two tools has been considered in the Hazard Analysis and it has been proposed as mitigation that STCA will overrule TC-Aid. This should be further discussed.

3.3.4 Dynamic Analysis of the SPR-level Model – Normal and Abnormal Operational Conditions

The validation exercises that already took place in the frame of P04.07.02 are:

- For TC Aid:
  - VP-171 (V2) [12];
  - VP-594 (V2) [13];
  - VP-175 (V3) [15].

- For PC Aid:
  - VP-172 (V2) [12];
  - VP-500 (V2) [15];
  - VP-501 (V2) [16];
- For TRACT:
  - VP-170 (V2) [12];
  - VP-592 (V2) [13].

The results from these trials have been used to assess the validity of a sub-set of the safety requirements; focusing predominantly on those relating to the success case. As expected, because of the maturity of the system or due to various validation constraints, not all of them were verified; e.g. those requiring longer term quantitative analysis of event frequencies. This is expected to improve in the next steps of the project.

3.3.4.1 TC Aid

3.3.4.1.1 Success Case Safety Requirements

Evidence for the verification of the following success case safety requirements for TC Aid shown in Table 33 can be found within the following two VALRs:

- P04.07.02 Iteration 1 VALR [12], section 6.2 – VP-171 Report
- P04.07.02 Iteration 2 VALR [13], section 6.2 – VP-594 Report
- P04.07.02 Iteration 3 VALR [15], section 6.2 – VP-175 Report

Requirement ID (SPR; SAR) / Text	Verified	Evidence taken/observed from/during the validation exercises
REQ-04.07.02-SPR-CDR1.1010; SR-111 It shall be possible for flights other than those in the sector to be recognised/made relevant in order that they are included in TC aid calculations.	Yes	Other flights than those in the sector were recognised and included in the TC aid calculations.
REQ-04.07.02-SPR-CDR1.1030; SR-113 Where no CFL is available the tactical trajectory shall use the Entry flight level of the first controlled sector.	Yes	A tactical trajectory was produced using the entry flight level of the first controlled sector when no CFL was available.
REQ-04.07.02-SPR-CDR1.1040; SR-115 The Tactical trajectory shall be updated by any clearances input into the TC Aid.	Partially	The tactical trajectory was updated by controller's clearances. However due to some software issues, the trajectory was not updating in real time.
REQ-04.07.02-SPR-CDR1.1050; SR-114 The TC Aid shall compare tactical trajectories between flights within the sector to predict the horizontal and vertical separation that will be achieved between them.	Yes	The Conflict Detection & Resolution (CD&R) service supported the Tactical Controller in assuring separation between (pairs of) aircraft. This included comparing the tactical trajectories between flights within the sector in order to predict the horizontal/vertical separation that will be achieved.

REQ-04.07.02-SPR-CDR1.1060; SR-116 The TC Aid shall detect any conflicting tactical trajectories within the minimum horizontal separation thresholds.	Yes	The Conflict Detection & Resolution (CD&R) service supported the Tactical Controller in assuring separation between (pairs of) aircraft. This included detecting any conflicting tactical trajectories within the minimum horizontal separation thresholds.
REQ-04.07.02-SPR-CDR1.1070; SR-1115 The TC Aid shall display an alert to the controllers when any conflicting tactical trajectories are detected.	Yes	The controllers were able to detect any conflicting tactical trajectories using the alerts provided by the TC Aid.
REQ-04.07.02-SPR-CDR1.1080; SR-1116 For the identification of Tactical encounters a ground speed uncertainty shall be taken into account.	Partially	The ground speed uncertainty was taken into account for the conflict detection only.
REQ-04.07.02-SPR-CDR1.1090; SR-1117 The controller shall be provided with all of the relevant information needed for each encounter.	Yes	The controller was provided with all the relevant information (e.g. a/c pair involved in the conflict, the sector in which the conflict took place, the beginning/end of infringement, closest point of approach, etc.).
REQ-04.07.02-SPR-CDR1.1100; SR-1118 The reaction time of the controller and flight crew shall be considered for the calculation of a tactical trajectory following a clearance.	Yes	Latency times, which proved to be adequate, to account for the reaction of the controller and the flight crew were fixed during the exercise. It has been found that the latency times vary with each simulated airspace.
REQ-04.07.02-SPR-CDR1.1110; SR-1119 The TC Aid shall display the conflicting trajectories on the situation display within x number of seconds (after the detection of the conflict) to the controller.	Partially	The system was always looking for conflicts. The arising conflicting trajectories were displayed in a timely manner to the controller such that the controller's reaction time was not delayed by the display latency. However how fast the conflicting trajectories were displayed was not measured during the validation exercises.
REQ-04.07.02-SPR-CDR1.1120; SR-1120 The TC Aid shall create a deviation trajectory if Flight Path Monitoring detects a Route deviation.	Yes	Deviation Trajectories were displayed for: -Route deviations (Rate - vertical, lateral); -Cleared flight level deviations; -No Valid Flight Plan Data Available.
REQ-04.07.02-SPR-CDR1.1130; SR-1121	Yes	Deviation Trajectories were displayed for:

The TC Aid shall create a deviation trajectory if Flight Path Monitoring detects a Lateral deviation.		-Route deviations (Rate - vertical, lateral); -Cleared flight level deviations; -No Valid Flight Plan Data Available.
REQ-04.07.02-SPR-CDR1.1140; SR-1122 The TC Aid shall create a deviation trajectory if Flight Path Monitoring detects a Vertical Rate Deviation.	Yes	Deviation Trajectories were displayed for: -Route deviations (Rate - vertical, lateral); -Cleared flight level deviations; -No Valid Flight Plan Data Available.
REQ-04.07.02-SPR-CDR1.1150; SR-1123 The TC Aid shall create a deviation trajectory if Flight Path Monitoring detects a CFL deviation.	Yes	Deviation Trajectories were displayed for: -Route deviations (Rate - vertical, lateral); -Cleared flight level deviations; -No Valid Flight Plan Data Available.
REQ-04.07.02-SPR-CDR1.1160; SR-1124 The TC Aid shall create a deviation trajectory if Flight Path Monitoring detects a Speed Deviation.	No	This was not applicable for the En Route airspace. However mode S data was used to recognise wrongly indicated speeds. The deviation trajectory due to a speed deviation will be taken into account when the system will be tested for APP.
REQ-04.07.02-SPR-CDR1.1170; SR-1125 The TC Aid shall create a deviation trajectory if Flight Path Monitoring detects that there is no valid flight plan data available.	Yes	Deviation Trajectories were displayed for: -Route deviations (Rate - vertical, lateral); -Cleared flight level deviations; -No Valid Flight Plan Data Available.
REQ-04.07.02-SPR-CDR1.1190; SR-1128 The TC Aid shall alert the controller to any detected deviations via HMI on the radar display.	Yes	As soon as a deviation was detected a warning was displayed to the controllers and the tactical trajectory was replaced by the deviation trajectory for further conflict detection and resolution.
REQ-04.07.02-SPR-CDR1.1200; SR-1127 The TC Aid shall continuously monitor actual track data and controller clearance data.	Yes	Monitoring Aids (MONA) were implemented which continuously monitor the adherence of all aircraft to their cleared trajectories.
REQ-04.07.02-SPR-CDR1.1220; SR-1130	Yes	The TC Aid detected deviations between controller clearance

The TC Aid shall detect deviations between controller clearance data and Mode S downlinked airborne parameters.		data and Mode S downlinked airborne parameters.
REQ-04.07.02-SPR-CDR1.1260; SR-1110 On request for a what-if probe for a heading or direct route the TC Aid shall display if that heading or direct route is conflict free.	Yes	This was done through the What-if and What-else functions.
REQ-04.07.02-SPR-CDR1.1290; SR-1113 The TC Aid shall provide what-else probing.	Yes	Both What-if and What-else functions were used by the controller.
REQ-04.07.02-SPR-CDR1.1300; SR-1114 The TC Aid shall compare the proposed tactical trajectory of a subject flight against the actual traffic situation when the controller requests a what-if or what-else probe.	Yes	The Conflict Detection & Resolution (CD&R) service supported the Tactical Controller in assuring separation between (pairs of) aircraft. This included the comparison of the proposed tactical trajectory of a subject flight against the actual traffic situation at the time of the what-if or what-else probe.
REQ-04.07.02-SPR-CDR1.1320; SR-1132 On request for a what-else probe the TC Aid shall display if the flight levels are conflict free or not, and if a vertical rate is necessary to achieve the level.	Yes	Tested, with a safety buffer taken into account for solving conflicts: *"If a flight level can only be reached with a given vertical rate an adequate rate buffer needs to be taken into account (e.g. if 2000 feet/minute or more are possible, restrict the solution space to 2500 feet/minute or more)" [12] (hence a safety buffer of 500 feet)*
REQ-04.07.02-SPR-CDR1.1330; SR-1133 On request for a what-else probe for headings or direct routes the TC Aid shall display if that headings or direct routes are conflict free.	Yes	The Resolution Advisory was implemented as "What-else" probing which does not require a controller input: - CFL-what-else probing; - DIRECT-what-else probing; - Heading what-else probing.
REQ-04.07.02-SPR-CDR1.1340; SR-1134 The TC Aid shall be available at all controller workstations.	Yes	It has been confirmed by DFS concept experts that the TC Aid was available at all controllers' workstations during the simulations.
REQ-04.07.02-SPR-CDR1.1350; SR-1135 It shall be possible to enable and disable the TC Aid.	Yes	It was possible to enable/disable the TC aid (e.g. the TC aid was switched off for the reference scenario).
REQ-04.07.02-SPR-CDR1.1360; SR-1136 ATCOs shall be able to delete/supress/hide alerts.	Yes	New requirement. However the functionality was already existent and tested during the validation exercises.

Table 32 TC Aid Success Case Safety Requirements Verification

3.3.4.1.2 Failure Case Safety Requirements

Due to their numerical nature the failure case safety requirements could not be verified/validated in the simulations.

3.3.4.2 PC Aid

3.3.4.2.1 Success Case Safety Requirements

Three validation exercises took place in the frame of P04.07.02 – PC Aid, i.e.:

- P04.07.02 Iteration 1 VALR [12], section 6.3 – VP-172 Report
- P04.07.02 Iteration 3 VALR [15], section 6.2 - VP-500
- P04.07.02 Iteration 4 VALR [16], section 4 – VP-501

However, only results from VP-500 and VP-501 were taken into account as evidence for the validation/verification of the success case safety requirements for PC Aid. This is because VP-172 used a different platform (to the one used in VP-500 and VP-501) to test the PC Aid tool and it has been decided that the further PC Aid validation activities will be a development of the platform used for VP-500 and VP-501, not the platform used under VP-172.

In addition to taking into account the results from the aforementioned VALRs, two safety questionnaires containing the success case safety requirements were produced for VP-501. One of the questionnaires (the one containing purely functional requirements) was verified against existent project documentation[17] by the safety team, whereas the other questionnaire (containing requirements which needed validation rather than verification) was intended for the controllers. Results are shown in sections 3.3.4.2.1.1 and 3.3.4.2.1.2. Note some of the wording of the requirements (NOT the meaning) was slightly changed to make them sound appropriate for a questionnaire. A reference to the original requirement in the SPR is provided. Note evidence from the VP-501 VALR [16] was used for both safety questionnaires.

3.3.4.2.1.1 Success Case Safety Requirements – VP-501 ATCO Validation

The results provided in Table 34 show the requirements' validation outcome extracted from the controller's answers provided during VP-501 and from the VP-501 VALR [16].

The VP-501 solution scenario consisted of an interoperability Through European Collaboration (iTEC) based IBP with integrated TC Aid [18](interim Future Area Control Tools <iFACTS>) and PC Aid (Risk Module). The Risk Module featured six types of risks presented in the following form:

- a warning in the data track label;
- by demand in the displayed flight trajectory;
- in a specific tabular called a "Conflict Risk Display (CRD)".

A What If probe was available to the Planner Controllers showing these six types of conflicts which occurred if certain level changes were applied.

For more information about the VP-501 tools please see the corresponding VALR [16] or the OSED [4].

Requirements	Validated	Comments / Evidence
	Yes/No/Partially	
The PC Aid continuously	Partially	Even though it continuously monitored the

[17] Documentation from the system developer which shows if a certain requirement has been met or not for the VP-501 simulation.
[18] Note the TC Aid was not the subject of the validation.

monitored any planning encounters within the AOR *[REQ-04.07.02-SPR-CDR2.1010]*		planning encounters, the PC Aid did miss some conflicts. However, the missed conflicts were shown in iFACTS. The PC Aid also monitored tactical encounters but planner controllers did not find this relevant to their role. They rather thought this is an unnecessary increase in workload. Comments included: • *"Often too much. Lots of repeated interactions".*
The PC Aid continuously displayed any planning encounters that were being monitored within the AOR *[REQ-04.07.02-SPR-CDR2.1020]*	Partially	In addition to the comments for *[REQ-04.07.02-SPR-CDR2.1010]*, ATCOs mentioned the risks could be displayed in a better way. This was because at a quick glance it was difficult to identify the reason for the conflict - causing low situational awareness. One of the planners mentioned: *"Again often too many [interactions displayed]".* This is related to the evidence found for [REQ-04.07.02-SPR-CDR2.1450] in section 3.3.4.2.1.2.
I [planner controller] was able to distinguish which of the displayed encounters were pertinent through the selective filtering functionality *[REQ-04.07.02-SPR-CDR2.1440]*	Partially	The planner controllers had the possibility to sort the risk table and to filter the risks shown (by removing types of risks) but *"with difficulty and found I perform this function slower than in today's kit*". They also felt this as *"heavy on workload"*. Overall the impression was that the ATCOs found it difficult to know which risks were relevant and which were irrelevant and they expressed a need for automated filtering support. ATCOs believed this would reduce workload considerably. According to section 4.1.1.1.2 in the VALR [16]: *"ATCOs commented that they found the risks hard to interpret and monitor when they were presented in a tabular form and preferred the graphical view iFACTS provided with the SM and LAD."*
The PC Aid made me [planner controller] aware to any planning encounters that were being monitored if they increased in severity	Yes	If a risk worsens by 2NM it reappears even if it had been previously acknowledged. However, ATCOs thought that this function needed to be refined as the risks reappeared far too many times.

[REQ-04.07.02-SPR-CDR2.1030]		Comments included: • *"This massively increased workload. These cannot be repeated multiple times"* • *"It did repeat interactions which worsened but also repeated interactions which did not get any worse"*
All potential what-else encounters at every sector entry and exit flight level were displayed to me [planner controller] in elevation view *[REQ-04.07.02-SPR-CDR2.1120]*	No	There was no what-else functionality tested in the VP-501 simulation.
The PC Aid alerted me [planner controller] whenever the system thought that a flight would not achieve its coordinated exit flight level *[REQ-04.07.02-SPR-CDR2.1130]*	No	It was hard for PCs to assess the XFL alerts as due to technical issues, multiple non-conformance alerts were presented to ATCOs. Specific non-conformance events relating to the PC were therefore hard to distinguish and the PCs tended to ignore them. This made it hard for the ATCOs to distinguish which alerts were "real" and which were just false alarms.
Whenever a coordination passed the MTCD check the PC Aid automatically coordinated that flight into the sector without referencing it to me [planner controller] *[REQ-04.07.02-SPR-CDR2.1140]*	Yes	Any issues/risks would have been displayed by the PC Aid. One of the ATCO commented: *"Although this is not always safe as displayed in testing."*
Whenever a coordination failed the MTCD check the PC Aid referred the coordination offer to me [planner controller] for manual assessment *[REQ-04.07.02-SPR-CDR2.1150]*	Yes	The PC Aid accepts everything into the sector. Problems would be highlighted in the Conflict Risk Display.

Whenever a potential exit flight level passed the MTCD check the PC Aid automatically set that specific exit flight level without referencing it to me [planner controller] *[REQ-04.07.02-SPR-CDR2.1160]*	Yes	
The PC Aid alerted me [planner controller] to coordinate an exit flight level if the system did not do this automatically or could not find a suitable XFL *[REQ-04.07.02-SPR-CDR2.1170]*	Partially	Even though pop-up boxes of coordination in and out were present in order for the coordination to go through, one of the controllers disagreed with this requirement. This might be connected with the terminology in the requirement, "alerting" might not be the right word. Further investigation needed.
I [planner controller] was able to withdraw a coordination offer made to the downstream sector if that coordination was no longer relevant to the downstream sector *[REQ-04.07.02-SPR-CDR2.1190]*	No	The system did not let the ATCOs withdraw a coordination offer.
The PC Aid alerted me [planner controller] to any coordination that had been rejected or revised by the downstream sector *[REQ-04.07.02-SPR-CDR2.1200]*	Yes	Even though the controllers only experienced revised coordinations during the simulation, the system has both functionalities. Note according to section 4.1.2.4.1.5 in the VALR [16]: *"Note that due to the fact that some standing agreements were not correctly input into iTEC, the PC had to manually amend the XFLs more than he would in current operations. This lead to an increase in workload."*
Any rejected coordination was removed from the PC Aid consideration *[REQ-04.07.02-SPR-CDR2.1210]*	Partially	The functionality exists however, one of the controllers did not provide any answer for this requirement. This may have been because he might have not experienced any rejected coordinations. Further investigation required.
Whenever I [planner controller] used any coordination constraints the coordination trajectory and any TP and MTCD outputs were	No	There were no coordination constraints in the simulation. One of the controllers specified: *"Didn't get any"*. However, one of the VALR's [16]

updated *[REQ-04.07.02-SPR-CDR2.1230]*		recommendations, in section 5.2.1, to further develop the system suggests the inclusion of Coordination Constraints in future validation exercises.
The PC Aid alerted me [PC/TC] whenever a flight was deviating from the applied coordination constraint(s) *[REQ-04.07.02-SPR-CDR2.1240]*	No	See comment for *[REQ-04.07.02-SPR-CDR2.1230]*.
Deviation alerts associated with coordination constraints were triggered at times/events appropriate to the controller role *[REQ-04.07.02-SPR-CDR2.1250]*	No	See comment for *[REQ-04.07.02-SPR-CDR2.1230]*.
The FDPS alerted me [planner controller] via the PC Aid whenever there was a new coordination offer *[REQ-04.07.02-SPR-CDR2.1270]*	Yes	
The FDPS (via the PC Aid) alert about the new coordination offer remained displayed until I [planner controller] took action to interrogate the new coordination offer *[REQ-04.07.02-SPR-CDR2.1280]*	Yes	This was possible through the coordination windows.
On cessation of the interrogation probe of the subject flight the coordination trajectories of that flight and any interacting environmental flights disappeared *[REQ-04.07.02-SPR-CDR2.1310]*	Partially	If the ATCO stopped the what if probe, the trajectories of the flights that would have interacted with that what-if probe would disappear if they were not relevant anymore. According to section 4.1.1.1.3 in the VALR [16]: *"The What-If probes allowed ATCOs to assess the consequences of executing a clearance without affecting the corresponding data for the actual flight. They were invoked in the same way an ATCO would enter a clearance but instead of "executing" the command, ATCOs selected the "probe" option instead."* One controller disagreed and one did not

		provide any answer, even though the functionality was present. This may be because controllers had to manually clear the probe which was cumbersome. Improvements in HMI to make this functionality more user friendly are needed.
I [planner controller] was able to reject a flight from the upstream sector if I [planner controller] thought the coordination offer was unsuitable and/or unsafe for the traffic situation at the time *[REQ-04.07.02-SPR-CDR2.1320]*	Partially	The functionality was existent but it may not have been used athere was no need to reject an offer during the measured runs. One of the controllers commented: *"Not tested".*
Whenever I [planner controller] probed a potential exit flight level via the what-if or what-else probes, the PC Aid displayed all other flights (context flights) that were between the entry level and proposed exit flight level along the subject flight's trajectory *[REQ-04.07.02-SPR-CDR2.1340]*	Partially	This was only valid for the what-if probe and, according to one controller: *"Only within the VOI (Volume of Interest). Needs to show outside in some sectors".*
I [planner controller] was able to distinguish context encounters from planning encounters *[REQ-04.07.02-SPR-CDR2.1350]*	Partially/No?	There is a specific risk (Coordination Context Risks) that is meant to show context encounters, however the ATCOs provided mixed responses for this requirement. This may be due to the controllers being unfamiliar with the terminology "context encounters". Also, coordination context risks were manually invoked. The process of manually requesting them was cumbersome and therefore ATCOs rarely used this feature Moreover, according to section 4.1.1.1.2 in the VALR [16]: *"Coordination Context Risks (CCRs) and Interest Coordination Risks (ICR) were manually invoked, however, ATCOs said they did not provide useful information as a PC. This information was also not easy to access to due the fact they had to manually request these by hooking the flight, clicking on the callsign and then*

		selecting the "CCR request" or "ICR request" buttons."
The PC Aid was available continuously at all controller working stations regardless of role assigned at that workstation *[REQ-04.07.02-SPR-CDR2.1400]*	Yes	
The PC Aid highlighted those flights that were holding within the sector against every MTCD probe *[REQ-04.07.02-SPR-CDR2.1420]*	No	Holding flights were not tested during the simulation.
The PC Aid highlighted any unusual/unexpected flights operating within the sector against every MTCD probe *[REQ-04.07.02-SPR-CDR2.1430]*	No	Even though it is planned to implement this in the real system, this functionality was not present/tested during the simulation. One controller stated: *"This [system] does not do this and is essential and works in today's NERC iFACTS system".*

Table 33 PC Aid Success Case Safety Requirements Validation

3.3.4.2.1.2 Success Case Safety Requirements Verification

Table 36 shows the outcome of the verification of the functional success case safety requirements. As mentioned in section 3.3.4.2.1, this verification was undertaken by checking with P10.04.01, who are responsible for building the system for VP-501, which requirements were included within the PC Aid. Evidence was also gathered from the VP-501 VALR [16].

Questions / Requirements	Delivered / Not delivered / Partially delivered	Comments / Evidence
ATCOs were able to delete/supress/hide alerts *[REQ-04.07.02-SPR-CDR2.1450]*	Not delivered	Needs checking. According to section 4.1.2.2.3 in the VALR [16]: *"Feedback from ATCOs implied that the number of risks within the CRD was a real problem with the PC spending the majority of the time within each run trying to make sense of the risks presented and removing the risks that were not salient. In one run on the BCN sector, the PC said that out of about 200 risks, only 12 risks were "real" risks. PCs said*

		that filtering is vital to reduce the number of risks presented which would also reduce workload considerably." Note in the text above the word "risk/s" = "alert/s".
Flights involved in a planning encounter with more than one environmental flights were displayed as individual pairs *[REQ-04.07.02-SPR-CDR2.1050]*	Delivered	
Whenever the planner probed an alternative coordinated level, heading or direct route (i.e. a 'what-if' probe) the PC Aid indicated the what-if encounters on the situation display and on the PC Aid tool displays *[REQ-04.07.02-SPR-CDR2.1060]*	Partially delivered	What-if not available for Heading, Speed and CFL.
When any what-if probe was ceased, the what-if encounters display was removed from the situation display and tools and the clearance was not committed to the system *[REQ-04.07.02-SPR-CDR2.1070]*	Delivered	As stated in the evidence for *[REQ-04.07.02-SPR-CDR2.1310]* in section 3.3.4.2.1, according to section 4.1.1.1.3 in the VALR [16]: *"The What-If probes allowed ATCOs to assess the consequences of executing a clearance without affecting the corresponding data for the actual flight. They were invoked in the same way an ATCO would enter a clearance but instead of "executing" the command, ATCOs selected the "probe" option instead."*
The planner controller was able to commit an alternative coordination to the system *[REQ-04.07.02-SPR-CDR2.1080]*	Not delivered	Executive controller will be responsible to execute clearances. DCT executed by planner controllers are not considered as cleared.
The revised coordination was indicated to the upstream planner / executive *[REQ-04.07.02-SPR-CDR2.1090]*	Not delivered	Only when the revised coordination has to be manually accepted by the controller but not for standard coordination automatically accepted.

The PC Aid displayed the severity and geometry of each encounter displayed to the planner *[REQ-04.07.02-SPR-CDR2.1100]*	Not delivered	Severity is only displayed within the conflict risk display in terms of distance and time to the closest point of approach.
When the planner selected a subject flight, the PC Aid displayed any potential speculative encounters at all sector coordination entry and exit levels *[REQ-04.07.02-SPR-CDR2.1110]*	Not delivered	No what-else.
The planner was able to override any automatic coordination decision done by the system *[REQ-04.07.02-SPR-CDR2.1180]*	Delivered	
The planner was able to apply coordination constraints to the coordination trajectory to a flight (as either a heading, speed or direct route) *[REQ-04.07.02-SPR-CDR2.1220]*	Not delivered	See evidence for *[REQ-04.07.02-SPR-CDR2.1230]* in section 3.3.4.1.1.
As soon as a flight of interest to the sector was recognised to the sector, the PC Aid produced a coordination trajectory for that flight *[REQ-04.07.02-SPR-CDR2.1260]*	Delivered	
On interrogation of a coordination offer via what-if or what-else probe, the coordination trajectories of the subject flight and any environmental flights that formed an encounter with the subject flight were displayed within x (usually 500 ms) number of seconds *[REQ-04.07.02-SPR-CDR2.1300]*	Partially delivered	Only fulfilled for What-if, there was no What-else.
The planner was able to revise the flight level of any coordination offer *[REQ-04.07.02-SPR-CDR2.1330]*	Delivered	According to section 4.1.2.4.1.5 in the VALR [16]: *"Throughout the six days, no NFL amendments were made, therefore the analysis of coordinations focussed on the*

		number of times XFLs were amended."
The planner was able to accept a flight via the PC Aid which informed all relevant parties, i.e. the upstream planner and upstream executive *[REQ-04.07.02-SPR-CDR2.1360]*	Delivered	Planner and executive controllers are allowed to assume flights. Planner controller is allowed to accept coordination proposals. This acceptation will be presented to planner and controller CWPs involved in the coordination ("upstream" y "downstream").
The time in which the planner pointed out encounters of tactical interest to the tactical workstation display was x (usually 500 ms) number of seconds *[REQ-04.07.02-SPR-CDR2.1380]*	Not delivered	No point-out functionality.
The ATCOs were able to independently remove the coordination point out from their work positions *[REQ-04.07.02-SPR-CDR2.1390]*	Not delivered	No point-out functionality.
The controllers were able to select/de-select the PC Aid display *[REQ-04.07.02-SPR-CDR2.1410]*	Delivered	Risk Module can be switched on/off globally for all CWPs. When RM is switched on every CWP could set on/off individually every risk type display.

Table 34 PC Aid Success Case Safety Requirements Verification

3.3.4.2.2 Failure Case Safety Requirements

Due to their numerical nature the failure case safety requirements could not be verified/validated in our simulations.

3.3.4.3 TRACT

3.3.4.3.1 Success Case Safety Requirements

Evidence for the verification of the following success case safety requirements for TRACT shown in Table 36 can be found within the following two VALRs:

- P04.07.02 Iteration 1 VALR [12], section 6.1 – VP-170 Report (V2);
- P04.07.02 Iteration 2 VALR [13], section 6.1 – VP-592 Report (V2).

Requirement ID (SPR; SAR) / Text	Verified	Evidence taken/observed from/during the validation exercises

REQ-04.07.02-SPR-TRA3.1010; SR-311 TRACT shall assess the eligibility of all flights of the whole traffic set.	Yes	TRACT assessed the eligibility of each aircraft. 90% of the traffic was considered to be i4D during the main simulation. There was also an additional validation session which contained 40% i4D traffic.
REQ-04.07.02-SPR-TRA3.1020; SR-312 TRACT shall consider the traffic set made of all flight plan data from the FDPS Area of Interest.	Partially	TRACT assessed both i4D and non-i4D (all other aircraft) equipped aircraft when making the calculations. Hence it can be said it was aware of all the flight plan data. However the notion "Area of Interest" was not validated/taken into account in the validation exercises. *"On the other hand, the TC-SA "mixed version" is capable of solving conflicts involving i4D equipped and unequipped aircraft. It sends CTOs to equipped aircraft while the unequipped ones receive neither constraint nor information from TC-SA."* [12]
REQ-04.07.02-SPR-TRA3.1030; SR-313 TRACT shall compute a global resolution by the application of a CTO to those flights that are eligible.	Yes	TRACT sent CTOs only to eligible, i.e. i4D equipped, aircraft.
REQ-04.07.02-SPR-TRA3.1040; SR-315 The TRACT service shall compute a solution that maintains or improves the controller's situational awareness.	Yes	*"ATCOs were confident in the TC-SA* (the TRACT tool) *so that they could focus on the remaining conflicts leading to increased situation awareness on the traffic."* [12]
REQ-04.07.02-SPR-TRA3.1050; SR-316 TRACT shall send a CTO to the aircraft via datalink.	No	Due to the nature of the real-time simulation this was not tested. However it has been taken into account as an assumption regarding the technical environment: *"Assumptions regarding the technical environment:* - *Both voice and data-link communications will be available"* [12]
REQ-04.07.02-SPR-TRA3.1060; SR-317 TRACT shall assess the whole of the traffic set (both eligible and non-eligible aircraft) to detect encounters between pairs of aircraft.	Yes	TRACT assessed both i4D and non-i4D equipped aircraft when making the calculations. *"On the other hand, the TC-SA <mixed version> is capable of solving conflicts involving i4D equipped and unequipped aircraft. It sends CTOs to equipped aircraft while the unequipped ones receive*

		neither constraint nor information from TC-SA." [12]
REQ-04.07.02-SPR-TRA3.1070; SR-318 TRACT shall solve encounters periodically without creating any new unsolved ones.	Yes	TRACT did not create any new conflicts as a consequence of the implementation of a TRACT solution. However this should be further validated.
REQ-04.07.02-SPR-TRA3.1080; SR-3111 TRACT shall warn the controllers when a CTO is not implemented as expected or when any aircraft involved in a TRACT solution deviates from its trajectory.	Partially	The tool warned the controller when an aircraft involved in a TRACT resolution deviated from its trajectory (e.g. by any reason a crossing would not be assured anymore): *"During two runs, one mixed resolution was degraded with a Wizard of Oz technique. In these situations, the unequipped aircraft went out of the assumed uncertainty envelope of the trajectory prediction used to compute the resolution, and the crossing was not assured anymore. A HMI warning was then displayed to alert the ATCOs so that they could regain control over conflict."* [12] However there were no instances when the tool would warn the controller if a CTO was not implemented anymore.
REQ-04.07.02-SPR-TRA3.1100; SR-3110 TRACT shall not attempt to solve a confliction where convergences or divergences between a pair of aircraft are of a small angle.	Yes	No TRACT solution occurred between flights where convergences or divergences between a pair of aircraft are of a small angle.
REQ-04.07.02-SPR-TRA3.1110; SR-3115 TRACT shall apply CTOs on trajectory points that are aligned[19] on the aircraft's FMS trajectory.	No	The FMS trajectory was not modelled during the validation exercises.
REQ-04.07.02-SPR-TRA3.1120; SR-314 TRACT shall only issue CTOs that are achievable by small speed adjustments.	Yes	*"The TC-SA detects potential conflicts 20-25' ahead of time and attempts to resolve them through CTOs that should be achievable though small speed changes (±5%) of the relevant aircraft."* [12]
REQ-04.07.02-SPR-TRA3.1130; SR-3112 The controller shall be informed via HMI to the fact that an aircraft is under a TRACT resolution.	Yes	An indicator in the flight label informed the controller that the flight belonged to a TRACT solution. Conversely, previous studies and

[19] Trajectory Points that are aligned = Trajectory Points that belong to the same Great Circle. Or, considering a trajectory segment, a point is aligned with the extremities of the segment if it is defined as a longitudinal distance from one extremity of the segment (and not as lat-long point).

		exercises at DSNA demonstrated that the performance decreased if the controller was not informed about the TRACT solution. In such a case, most TRACT solutions were automatically suppressed because of an undue controller clearance that was incompatible with the TRACT solution
REQ-04.07.02-SPR-TRA3.1140; SR-3113 The status of the TRACT resolution shall be displayed to the controller.	No	Nothing more than the identification of the flights belonging to an on-going TRACT solution has been displayed to the controller. In particular, there is no indication whether the TRACT constraints have only been sent to the aircraft or the TRACT constraints have been accepted by the involved pilots.
REQ-04.07.02-SPR-TRA3.1150; SR-3116 The TRACT resolution indicator shall not be able to be directly removed by the controllers unless they are discarding the TRACT solution.	Yes	Indeed the controller cannot suppress directly the TRACT indicator, but s/he was capable of discarding the TRACT solution (either explicitly or via a clearance) which lead to the automatic removal of the TRACT indicators.
REQ-04.07.02-SPR-TRA3.1160; SR-3117 It shall be clear to the controller which aircraft pairs are involved in conflict resolution.	Yes	It was possible for the controller to identify which aircraft belong to the cluster of the selected aircraft, on demand. The operational need to identify the pairs of conflicting aircraft **within** a TRACT solution has not been identified yet, but it may raise, notably when the ATCO wants to override a part of a TRACT solution.
REQ-04.07.02-SPR-TRA3.1170; SR-3118 If there is no answer from the flight crew, TRACT shall consider the answer to be 'STAND BY'.	No	The validation exercises never considered the pilots in the loop. The answer of the flight crew has always been modelled as an immediate and positive answer.
REQ-04.07.02-SPR-TRA3.1180; SR-3119 The flight crew shall assess the eligibility of the CTO before committing to the CTO.	No	The validation exercises never considered the pilots in the loop. The answer of the flight crew has always been modelled as an immediate and positive answer.
REQ-04.07.02-SPR-TRA3.1190; SR-3123 The ATCO shall have access to the position and time of any CTO.	Yes	The position and time of the CTO were displayed on demand.
REQ-04.07.02-SPR-TRA3.1200; SR-3120	No	The validation exercises never considered the pilots in the loop.

The flight crew shall have the ability to accept or reject the CTO.		The answer of the flight crew has always been modelled as an immediate and positive answer.
REQ-04.07.02-SPR-TRA3.1220; SR-3122 The flight crew shall have the ability to reply 'STAND BY' if they need more time to consider the acceptability of the CTO.	No	The validation exercises never considered the pilots in the loop. The answer of the flight crew has always been modelled as an immediate and positive answer.
REQ-04.07.02-SPR-TRA3.1230; SR-3124 If the flight crew respond with an 'UNABLE' reply to the CTO, TRACT shall uplink a cancellation message to all other aircraft with a CTO in the cluster.	No	The validation exercises never considered the pilots in the loop. The answer of the flight crew has always been modelled as an immediate and positive answer.
REQ-04.07.02-SPR-TRA3.1240; SR-3125 If the flight crew respond with an 'UNABLE' reply to the CTO, TRACT shall not attempt to send another CTO to the aircraft for at least X (e.g. 15) minutes depending on the ANSP's off-line configuration.	No	The validation exercises never considered the pilots in the loop. The answer of the flight crew has always been modelled as an immediate and positive answer.
REQ-04.07.02-SPR-TRA3.1250; SR-3126 TRACT shall consider any flight that is already subject to an AMAN Time constraint as ineligible for a CTO.	No	AMAN was not considered during the simulations.
REQ-04.07.02-SPR-TRA3.1260; SR-3127 TRACT shall cross check with the FMS to see if the flight is already subject to an AMAN time constraint.	No	Neither the FMS nor the AMAN have been part of the validation exercises.
REQ-04.07.02-SPR-TRA3.1270; SR-3128 TRACT shall only consider those flights to be eligible that are i4D equipped.	Yes	TRACT considered only i4D aircraft as being eligible to receive a CTO.
REQ-04.07.02-SPR-TRA3.1290; SR-3130 TRACT shall discard/delete a resolution whenever the ATCO issues a clearance to change the behaviour of an aircraft under a TRACT resolution.	Yes	The system was made such that as soon as the controller inputs a clearance that aims at modifying the aircraft behaviour, TRACT considers that the ATCO wants to solve the situation on her/his own and it automatically discards the constraint on this aircraft and the constraints on other aircraft if they become now useless.
REQ-04.07.02-SPR-TRA3.1300; SR-3131 TRACT shall alert the flight crew when the TRACT resolution has been discarded.	No	The validation exercises never considered the pilots in the loop. The answer of the flight crew has always been modelled as an immediate and positive answer.
REQ-04.07.02-SPR-TRA3.1310; SR-3114 Any HMI indication related to a TRACT solution shall be removed whenever TRACT discards	Yes	All HMI indication related to the TRACT solution were removed when a TRACT solution was

that solution.		discarded.
REQ-04.07.02-SPR-TRA3.1320; SR-3132 TRACT shall alert the ATCO when the TRACT resolution has been discarded.	No	This has not been validated. The only removal of indicators is not enough. It is important for safety that the ATCO is made aware of a new resolution task to perform.

Table 35 TRACT Success Case Safety Requirements Verification

3.3.4.3.2 Failure Case Safety Requirements

Due to their numerical nature the failure case safety requirements could not be verified/validated in our simulations.

3.3.5 Additional Safety Requirements (functionality and performance) – Normal Operational Conditions

Two additional safety requirements were identified as a result of the past validation exercises' results:

Tool	New Requirement	Rationale	Comments
PC Aid	*REQ-04.07.02-SPR-CDR2.1440; SR-2144* *The planner shall be able to distinguish which of the displayed encounters are pertinent through selective filtering functionality.*	*The controllers will have the possibility to filter their encounters in order to be able to distinguish the ones which are of interest and to avoid misunderstanding of the traffic picture and loss of situational awareness caused by a crowded display.*	This requirement was introduced based on the results gathered from VP-500 and as a result of supressing *REQ-04.07.02-SPR-CDR2.1040 [SR-213];*
TC/PC Aid	*ATCOs shall be able to delete/supress/hide alerts.*	*The TC/PC aid will not negatively impact controller's situational awareness by creating clutter on the situational displays. Therefore the controllers should have means to supress or delete the unwanted/nuisance alerts.*	DFS implemented this feature for TC Aid and it has been agreed this should be captured as a requirement as well.

3.4 Design Analysis – Case of Internal System Failures

The case of internal system failures has been undertaken in two steps:

- Identified all potential hazard causes associated with the system;
- A complete set of logical requirements has been derived (requirements which define the logical way in which each functional block within the service would operate, these are more detailed than the SCSOs, but less detailed than the ORs).

3.4.1 Scenarios for the Failure Case Analysis

The same scenarios used for the derivation of the success case safety requirements, presented in Table 30, Table 31 and Table 32 were used in the workshop to derive the failure case safety requirements. The workshop was held over a period of three days. Each of the three operational services (TRACT, CD/R aid to PC and CD/R aid to TC) were examined in one of the three days.

3.4.2 Derivation of Safety Requirements (Integrity/Reliability)

For each logical requirement, the ways in which each logical element could feasibly fail where identified. This was undertaken in two steps; firstly by brainstorming the ways in which each function could fail and then by applying a structured set of key words which are listed below in order to confirm all failure modes had been identified.

For equipment related functions:

- Loss;
- Delay (outdated/old);
- Undetected corruption;
- Detected corruption.

For operators:

- Misinterpret;
- Misunderstand.

It should be noted that the Functional Hazard Analysis (FHA) did not address the identification of the causes (failures) since this is expected to be undertaken once a physical architecture has been established.

Utilising the expert knowledge in the workshop of the system functions and interfaces, it was possible to determine the safety effect on operations of each hazard. Where possible the exposure time, and ability to detect the failure were recorded.

The probability numbers in each of the Failure Case Safety Requirements in Table 38, Table 39 and Table 40 have been developed using the following methodology:

- The final *Maximum Tolerable Frequency of Occurrence* rate of the hazards presented in Table 11, Table 12 and Table 13 has been divided by the number of times each hazard appeared throughout the FHA (column "*Hazard Resultant"*) presented in Appendix B, for each of the failure cases and a probability of happening has been obtained (note for TRACT two more failure factors have been added – See Table 69)
- For each of the failure cases ("Loss of FDPS", "Corruption of FDPS", etc.) the hazard with the smallest probability of happening has been chosen. This number represents the maximum negative safety contribution that has been used in the integrity safety requirements in Table 38, Table 39 and Table 40.

For the full FHA please see Appendix B.

Table 37 is an example for the purposes of demonstrating the calculation method:

Abnormal Condition	Hazard Identified in FHA analysis[20]	Hazard Maximum Tolerable Frequency of Occurrence Rate (C3)[21]	No. of times hazard has been present throughout PSSA (C4)[22]	Final probability rate (C3/C4)

[20] Can be found in Table 11, Table 12 or Table 13 or Table 68, Table 69, Table 70– for all three operational services.
[21] Can be found in Table 11, Table 12 or Table 13 or Table 68, Table 69, Table 70 – for all three operational services.
[22] The number of times a specific hazard was an outcome of all the failures presented in Table 65, Table 66 and Table 67 (for each operational services) was counted.

Loss of FDPS – PC aid	001	$2*10^{-4}$	21	$9.52*10^{-6}$
	004	$2*10^{-3}$	13	$1.54*10^{-4}$
	005	$2*10^{-3}$	14	$1.43*10^{-4}$

Table 36 Probability numbers calculation - Example

Out of the three hazards identified for the "Loss of FDPS" – PC aid (Hazard 001, 004, 005), Hazard 001 has the lowest probability of happening. Therefore, this will be the maximum negative safety contribution to be taken into account for defining the corresponding failure case safety requirement:

"The probability of loss of FDPS shall be no more than 9.52E-06 per flight hour."[23]

Table 38, Table 39 and Table 40 show the full list of failure case safety requirements and their corresponding FCSOs for each of the three operational services.

TRACT

Ref	Abnormal Conditions		SR ID [FCSO Ref.]	SR Text *[SPR Reference]*
1	Loss of	FDPS	SR-321 [FCSO 31; FCSO 32; FCSO 34; FCSO 35]	The probability of loss of FDPS shall be no more than 2.86E-03 per flight hour. *[REQ-04.07.02-SPR-TRA3.2010]*
		SDPS	SR-322 [FCSO 31; FCSO 32; FCSO 34; FCSO 35]	The probability of loss of SDPS shall be no more than 2.86E-03 per flight hour. *[REQ-04.07.02-SPR-TRA3.2020]*
		ATCO CWP	SR-323	The probability of loss of ATCO CWP shall be no more than 6.25E-02 per flight hour. *[REQ-04.07.02-SPR-TRA3.2030]*
		TRACT	SR-324 [FCSO 31; FCSO 32; FCSO 34; FCSO 35]	The probability of loss of TRACT shall be no more than 2.86E-03 per flight hour. *[REQ-04.07.02-SPR-TRA3.2040]*
		AMAN	SR-325 [FCSO 33]	The probability of loss of AMAN shall be no more than 2.00E-01 per flight hour. *[REQ-04.07.02-SPR-TRA3.2050]*
		FMS	SR-326 [FCSO 34]	The probability of loss of FMS shall be no more than 6.25E-02 per flight hour. *[REQ-04.07.02-SPR-TRA3.2060]*
		ADS-C	SR-327 [FCSO 34]	The probability of loss of ADS-C shall be no more than 6.25E-02 per flight hour. *[REQ-04.07.02-SPR-TRA3.2070]*
		CPDLC	SR-328 [FCSO 34]	The probability of loss of CPDLC shall be no more than 6.25E-02 per flight hour. *[REQ-04.07.02-SPR-TRA3.2080]*
		FDPS	SR-329 [FCSO 31; FCSO 32; FCSO 34;	The probability of corruption of FDPS shall be no more than 2.86E-03 per flight hour. *[REQ-04.07.02-*

[23] Can be found in Table 34.

			FCSO 35]	*SPR-TRA3.2090]*
		SDPS	SR-3210 [FCSO 31; FCSO 32; FCSO 34; FCSO 35]	The probability of corruption of SDPS shall be no more than 2.86E-03 per flight hour. *[REQ-04.07.02-SPR-TRA3.2100]*
2	Corruption of	ATCO CWP	SR-3211 [FCSO 31; FCSO 32; FCSO 34; FCSO 35]	The probability of corruption of ATCO CWP shall be no more than 2.86E-03 per flight hour. *[REQ-04.07.02-SPR-TRA3.2110]*
		TRACT	SR-3212 [FCSO 32; FCSO 35]	The probability of corruption of TRACT shall be no more than 2.86E-03 per flight hour. *[REQ-04.07.02-SPR-TRA3.2120]*
		AMAN	SR-3213 [FCSO 33; FCSO 34]	The probability of corruption of AMAN shall be no more than 6.25E-02 per flight hour. *[REQ-04.07.02-SPR-TRA3.2130]*
		FMS	SR-3214 [FCSO 34; FCSO 35]	The probability of corruption of FMS shall be no more than 2.86E-03 per flight hour. *[REQ-04.07.02-SPR-TRA3.2140]*
		ADS-C	SR-3215 [FCSO 31; FCSO 32; FCSO 34; FCSO 35]	The probability of corruption of ADS-C shall be no more than 2.86E-03 per flight hour. *[REQ-04.07.02-SPR-TRA3.2150]*
		CPDLC	SR-3216 [FCSO 34]	The probability of corruption of CPDLC shall be no more than 6.25E-02 per flight hour. *[REQ-04.07.02-SPR-TRA3.2160]*
		FDPS	SR-3217 [FCSO 31; FCSO 32; FCSO 33; FCSO 34; FCSO 35]	The probability of delay of FDPS shall be no more than 2.86E-03 per flight hour. *[REQ-04.07.02-SPR-TRA3.2170]*
		ATCO CWP	SR-3218 [FCSO 34]	The probability of delay of ATCO CWP shall be no more than 6.25E-02 per flight hour. *[REQ-04.07.02-SPR-TRA3.2180]*
3	Delay of	TRACT	SR-3219 [FCSO 34]	The probability of delay of TRACT shall be no more than 6.25E-02 per flight hour. *[REQ-04.07.02-SPR-TRA3.2190]*
		AMAN	SR-3220 [FCSO 34]	The probability of delay of AMAN shall be no more than 2.00E-01 per flight hour. *[REQ-04.07.02-SPR-TRA3.2200]*
		FMS	SR-3221 [FCSO 34]	The probability of delay of FMS shall be no more than 6.25E-02 per flight hour. *[REQ-04.07.02-SPR-TRA3.2210]*
		ADS-C	SR-3222 [FCSO 33]	The probability of delay of ADS-C shall be no more than 6.25E-02 per flight hour. *[REQ-04.07.02-SPR-TRA3.2220]*
		CPDLC	SR-3223 [FCSO 34]	The probability of delay of CPDLC shall be no more than 6.25E-02 per flight hour. *[REQ-04.07.02-SPR-*

				TRA3.2230]
4	Misunderstanding of	Tactical	SR-3224 [FCSO 31; FCSO 35]	The probability of the Tactical misunderstanding the tool shall be no more than 2.86E-03 per flight hour. *[REQ-04.07.02-SPR-TRA3.2240]*
		Planner	SR-3225 [FCSO 31; FCSO 32]	The probability of the Planner misunderstanding the tool shall be no more than 1.18E-01 per flight hour. *[REQ-04.07.02-SPR-TRA3.2250]*

1489 **Table 37: Safety Requirements or Assumptions - abnormal conditions for TRACT**

1490

1491 # CD/R aid to PC

Ref	Abnormal Conditions		SR ID [FCSO Ref.]	SR Text
1	Loss of	FDPS	SR-221 [FCSO 21; FCSO 24; FCSO 25]	The probability of loss of FDPS shall be no more than 9.52E-06 per flight hour. *[REQ-04.07.02-SPR-CDR2.2010]*
		SDPS	SR-222 [FCSO 21]	The probability of loss of SDPS shall be no more than 9.52E-06 per flight hour. *[REQ-04.07.02-SPR-CDR2.2020]*
		Upstream PC aid	SR-223 [FCSO 23]	The probability of loss of Upstream PC Aid shall be no more than 1.33E-05 per flight hour. *[REQ-04.07.02-SPR-CDR2.2030]*
		PC aid	SR-224 [FCSO 21; FCSO 23]	The probability of loss of PC Aid shall be no more than 9.52E-06 per flight hour. *[REQ-04.07.02-SPR-CDR2.2040]*
		Downstream PC aid	SR-225 [FCSO 21]	The probability of loss of Downstream PC Aid shall be no more than 9.52E-06 per flight hour. *[REQ-04.07.02-SPR-CDR2.2050]*
2	Delay of	FDPS	SR-226 [FCSO 22]	The probability of delay of the FDPS shall be no more than 9.52E-06 per flight hour. *[REQ-04.07.02-SPR-CDR2.2060]*
		SDPS	SR-227 [FCSO 21]	The probability of delay of the SDPS shall be no more than 9.52E-06 per flight hour. *[REQ-04.07.02-SPR-CDR2.2070]*
		Upstream PC aid	SR-228 [FCSO 23]	The probability of delay of the Upstream PC Aid shall be no more than 1.33E-05 per flight hour. *[REQ-04.07.02-SPR-CDR2.2080]*
		PC aid	SR-229 [FCSO 21; FCSO 22; FCSO 23]	The probability of delay of the PC Aid shall be no more than 9.52E-06 per flight hour. *[REQ-04.07.02-SPR-CDR2.2090]*
		Downstream PC	SR-2210 [FCSO 21; FCSO 22]	The probability of delay of the Downstream PC Aid shall be no more than 9.52E-06 per flight hour. *[REQ-*

		aid		*04.07.02-SPR-CDR2.2100]*
3	Corruption of	FDPS (undetected)	SR-2211 [FCSO 21; FCSO 22; FCSO 24]	The probability of corruption (undetected) of the FDPS shall be no more than 9.52E-06 per flight hour. [REQ-04.07.02-SPR-CDR2.2110]
		SDPS (undetected)	SR-2212 [FCSO 21; FCSO 22; FCSO 24]	The probability of corruption (undetected) of the SDPS shall be no more than 9.52E-06 per flight hour. *[REQ-04.07.02-SPR-CDR2.2120]*
		Upstream PC aid (undetected)	SR-2213 [FCSO 23]	The probability of corruption (undetected) of the Upstream PC Aid shall be no more than 1.33E-05 per flight hour. *[REQ-04.07.02-SPR-CDR2.2130]*
		PC aid (undetected)	SR-2214 [FCSO 21; FCSO 22; FCSO 24]	The probability of corruption (undetected) of the PC Aid shall be no more than 9.52E-06 per flight hour. *[REQ-04.07.02-SPR-CDR2.2140]*
		Downstream PC aid (undetected)	SR-2215 [FCSO 21; FCSO 22]	The probability of corruption (undetected) of the Downstream PC Aid shall be no more than 9.52E-06 per flight hour. *[REQ-04.07.02-SPR-CDR2.2150]*
		FDPS (detected)	SR-2216 [FCSO 24]	The probability of corruption (detected) of the FDPS shall be no more than 1.54E-04 per flight hour. *[REQ-04.07.02-SPR-CDR2.2160]*
		SDPS (detected)	SR-2217 [FCSO 24]	The probability of corruption (detected) of the SDPS shall be no more than 1.54E-04 per flight hour. *[REQ-04.07.02-SPR-CDR2.2170]*
		Upstream PC aid (detected)	SR-2218 [FCSO 24]	The probability of corruption (detected) of the Upstream PC Aid shall be no more than 1.54E-04 per flight hour. *[REQ-04.07.02-SPR-CDR2.2180]*
		PC aid (detected)	SR-2219 [FCSO 24]	The probability of corruption (detected) of the PC Aid shall be no more than 1.54E-04 per flight hour. *[REQ-04.07.02-SPR-CDR2.2190]*
		Downstream PC aid (detected)	SR-2220 [FCSO 24]	The probability of corruption (detected) of the Downstream PC Aid shall be no more than 1.54E-04 per flight hour. *[REQ-04.07.02-SPR-CDR2.2200]*
		Upstream Planner	SR-2221 [FCSO 25]	The probability of the Upstream Planner misunderstanding the tool shall be no more than 1.43E-04 per flight hour. *[REQ-04.07.02-SPR-CDR2.2210]*
		Planner	SR-2222 [FCSO 21; FCSO 22; FCSO 25]	The probability of the Planner misunderstanding the tool shall be no more than 9.52E-06 per flight hour.

4	Misunderstanding of			*[REQ-04.07.02-SPR-CDR2.2220]*
		Downstream Planner	SR-2223 [FCSO 25]	The probability of the Downstream Planner misunderstanding the tool shall be no more than 1.43E-04 per flight hour. *[REQ-04.07.02-SPR-CDR2.2230]*
		Upstream Executive	SR-2224 [FCSO 25]	The probability of the Upstream Executive misunderstanding the tool shall be no more than 1.43E-04 per flight hour. *[REQ-04.07.02-SPR-CDR2.2240]*
		Executive	SR-2225 [FCSO 25]	The probability of the Executive misunderstanding the tool shall be no more than 1.43E-04 per flight hour. *[REQ-04.07.02-SPR-CDR2.2250]*
		Downstream Executive	SR-2226 [FCSO 25]	The probability of the Downstream Executive misunderstanding the tool shall be no more than 1.43E-04 per flight hour. *[REQ-04.07.02-SPR-CDR2.2260]*

Table 38: Safety Requirements or Assumptions - abnormal conditions for PC Aid

CD/R aid to TC

Ref	Abnormal Conditions		SR ID [FCSO Ref.]	SR Text
1	Loss of	FDPS	SR-121 [FCSO 12]	The probability of Loss of FDPS shall be no more than 5.33E-06 per flight hour. *[REQ-04.07.02-SPR-CDR1.2010]*
		SDPS	SR-122 [FCSO 11; FCSO 12]	The probability of Loss of SDPS shall be no more than 3.33E-07 per flight hour. *[REQ-04.07.02-SPR-CDR1.2020]*
		TC aid	SR-123 [FCSO 11; FCSO 12; FCSO 13]	The probability of Loss of TC Aid shall be no more than 3.33E-07 per flight hour. *[REQ-04.07.02-SPR-CDR1.2030]*
		FMS	SR-124 [FCSO 12]	The probability of Loss of FMS shall be no more than 5.33E-06 per flight hour. *[REQ-04.07.02-SPR-CDR1.2040]*
2	Delay of	FDPS	SR-125 [FCSO 12]	The probability of Delay of the FDPS shall be no more than 5.33E-06 per flight hour. *[REQ-04.07.02-SPR-CDR1.2050]*
		SDPS	SR-126 [FCSO 11; FCSO 12]	The probability of Delay of the SDPS shall be no more than 3.33E-07 per flight hour. *[REQ-04.07.02-SPR-CDR1.2060]*
		TC aid	SR-127 [FCSO 11; FCSO 12]	The probability of Delay of the TC Aid shall be no more than 3.33E-07 per flight hour. *[REQ-04.07.02-SPR-CDR1.2070]*

		FMS	SR-128 [FCSO 12]	The probability of Delay of the FMS shall be no more than 5.33E-06 per flight hour. *[REQ-04.07.02-SPR-CDR1.2080]*
3	Corruption of	FDPS (undetected)	SR-129 [FCSO 12]	The probability of Corruption (undetected) of the FDPS shall be no more than 5.33E-06 per flight hour. *[REQ-04.07.02-SPR-CDR1.2090]*
		SDPS (undetected)	SR-1210 [FCSO 12; FCSO 13]	The probability of Corruption (undetected) of the SDPS shall be no more than 3.33E-07 per flight hour. *[REQ-04.07.02-SPR-CDR1.2100]*
		TC aid (undetected)	SR-1211 [FCSO 11; FCSO 12; FCSO 13]	The probability of Corruption (undetected) of the TC Aid shall be no more than 3.33E-07 per flight hour. *[REQ-04.07.02-SPR-CDR1.2110]*
		FDPS (detected)	SR-1212 [FCSO 12; FCSO 14]	The probability of Corruption (Detected) of the FDPS shall be no more than 1.00E-05 per flight hour. *[REQ-04.07.02-SPR-CDR1.2120]*
		SDPS (detected)	SR-1213 [FCSO 14]	The probability of Corruption (Detected) of the SDPS shall be no more than 1.00E-05 per flight hour. *[REQ-04.07.02-SPR-CDR1.2130]*
		TC aid (detected)	SR-1214 [FCSO 14]	The probability of Corruption (Detected) of the TC Aid shall be no more than 1.00E-05 per flight hour. *[REQ-04.07.02-SPR-CDR1.2140]*
		FMS(detected)	SR-1215 [FCSO 14]	The probability of Corruption (Detected) of the FMS shall be no more than 1.00E-05 per flight hour. *[REQ-04.07.02-SPR-CDR1.2150]*
4	Misunderstanding of	Executive	SR-1216 [FCSO 15]	The probability of the Executive misunderstanding the tool shall be no more than 5.00E-06 per flight hour. *[REQ-04.07.02-SPR-CDR1.2160]*
		Flight Crew	SR-1217 [FCSO 15]	The probability of the Flight Crew misunderstanding the instruction shall be no more than 5.00E-06 per flight hour. *[REQ-04.07.02-SPR-CDR1.2170]*

Table 39: Safety Requirements or Assumptions - abnormal conditions for TC Aid

3.4.3 Thread Analysis of the SPR-level Model - Abnormal Conditions

Thread Analysis uses a particular graphical presentation in which the actions of the individual elements of the SPR-level Model, and the interactions between those elements, are represented as a continuous 'thread', from initiation to completion.

The thread analysis for abnormal operations has been done using the same graphical presentation and scenarios as for normal operations. Hence the same threads were used to identify the Failure Case Safety Requirements presented in section 3.4.2. The thread analysis was also fundamental in identifying all the possible hazard causes for performing the failure case analysis.

The detailed FHA and analysis is presented in Appendix B.

3.4.4 Additional Safety Requirements – Abnormal Operational Conditions

No additional safety requirements, other than those already presented in section 3.4.2, have been identified from the assessment of the SPR-level model with respect to abnormal operational conditions.

3.5 Achievability of the SAfety Criteria

In section 2.10 of the present document the assessment of the achievability of the Safety Criteria defined in section 2.5 has been performed through the specification of safety objectives.

At SPR-design level, SOs have been mapped versus safety requirements for both normal and abnormal conditions and functional and integrity/reliability safety requirements have been defined.

Therefore, for each of the input SAC, the same conclusions can be derived as reported in section 2.10.

Appendix A Success Case Safety Requirements Derivation

The Safety Requirements (SRs) define the safety related requirements that the concept will perform, in order to achieve the SCSOs. These define the *complete* range of functionality and performance properties which the services provide, and correspond to the E-OCVM lifecycle phase 3 in terms of their level of detail (detailed safety assurance activities to inform the SPR as defined by SESAR safety reference material).

The SRs were defined based on assessment of the SPR level model and threads, and the SCSOs. These were then reviewed by safety experts and concept experts. The SRs are not repeated in this annex, as they are the subject of the main body of the document and this would result in unnecessary duplication. The threads that were assessed in order to generate them are shown in the next subsection.

A.1 Thread Analysis

This sub-section shows the thread diagrams that were developed as part of the SPR analysis in Task 20 (V2). They represent the detailed models and descriptions of the interactions between architectural elements of the concepts (who and what) during specific operational scenarios.

These were used to identify the safety requirements, but were also fundamental in helping to identify all the possible hazard causes when performing the failure case analysis. Note: some alternative flows do not have their own diagrams as they are no different to the main scenario diagram.

A.1.1 TRACT

Scenario 1: TRACT Resolves Conflict

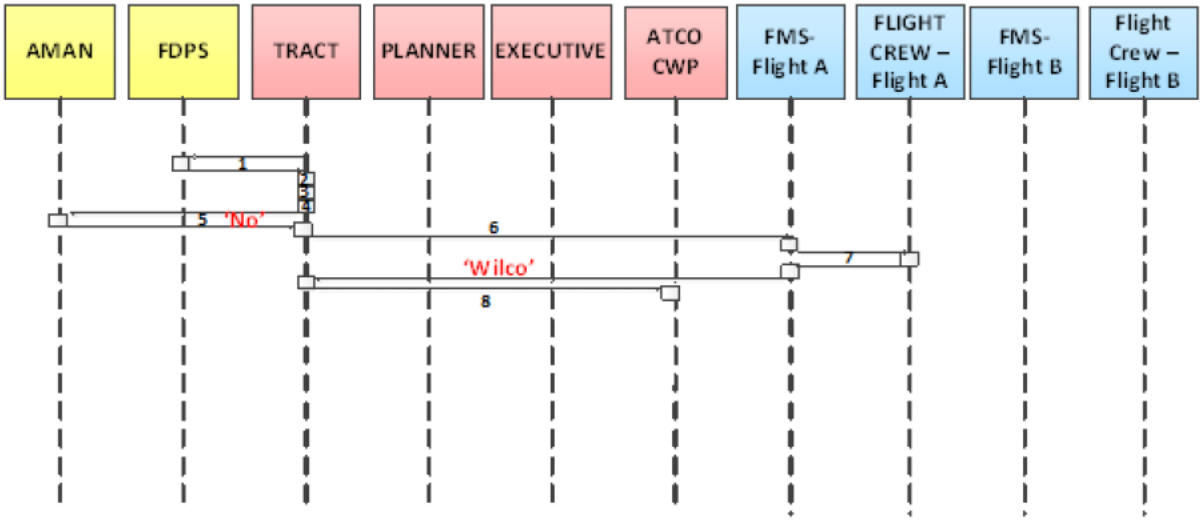


Figure 12: TRACT: scenario 1

Scenario #1: TRACT Resolves a conflict	
1	TRACT obtains the current traffic of the FDPS area of interest and assesses the eligibility of each flight of the current traffic situation (i.e. if it is equipped with i4D and also if any aircraft are already subject to any AMAN time constraints)
2	TRACT then assesses the whole traffic set and detects if there any conflictions between 2 aircraft (eligible or not)
3	TRACT splits potential conflicts into 'TRACT Clusters' by dividing the conflicts into small and independent clusters.
4	TRACT computes a global resolution by the application of time constraints (CTOs) on eligible flights that are i4D equipped.
5	TRACT cross checks with AMAN to see if flight has a higher priority CTA – answer 'no'

6	TRACT sends to the flight FMS (just depicts sending to flight 'A' on thread diagram)
7	Flight crew assesses CTO and accepts – sends a WILCO message
8	TRACT outputs the conflicts that are resolved by an accepted CTO for the subsequent MTCD services to specifically manage them if still detected and to HMI at ATCO CWP??

Table 40: TRACT: scenario 1

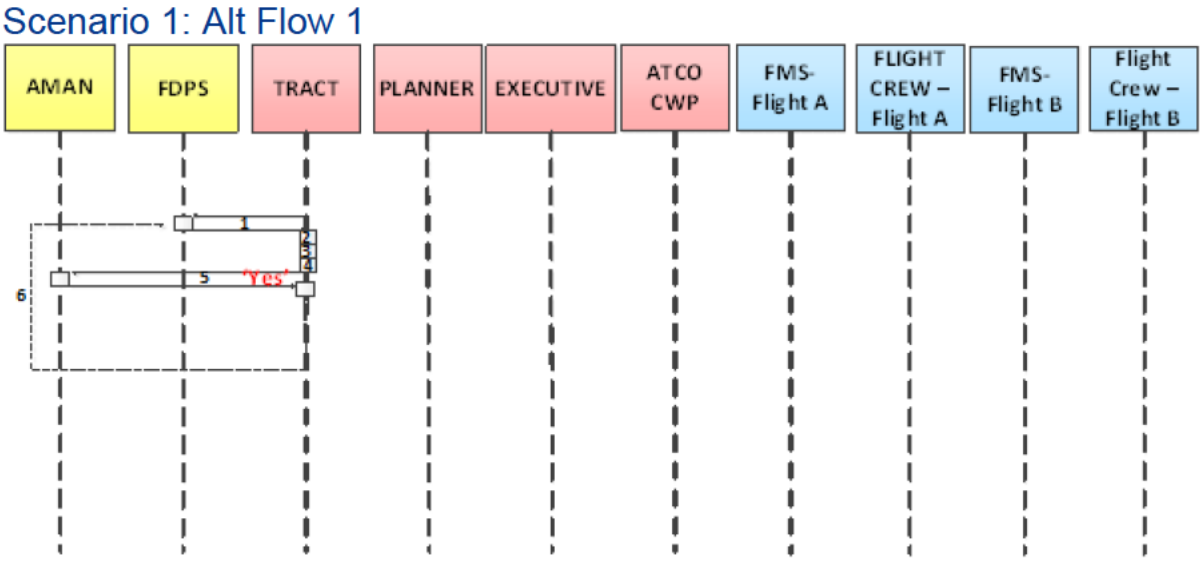


Figure 13:TRACT: scenario 1: Alt Flow 1

Scenario #1: Alternative flow 1: Flight already has a CTO	
	Steps 1-4 the same
5	TRACT cross checks with AMAN to see if flight has a higher priority CTA – answer 'yes'
6	TRACT shall consider the aircraft is no longer considered for a CTO and restarts the cycle of computation for the cluster it belongs to (i.e. starts from Step 1)

Table 41: TRACT: scenario 1: Alt Flow 1

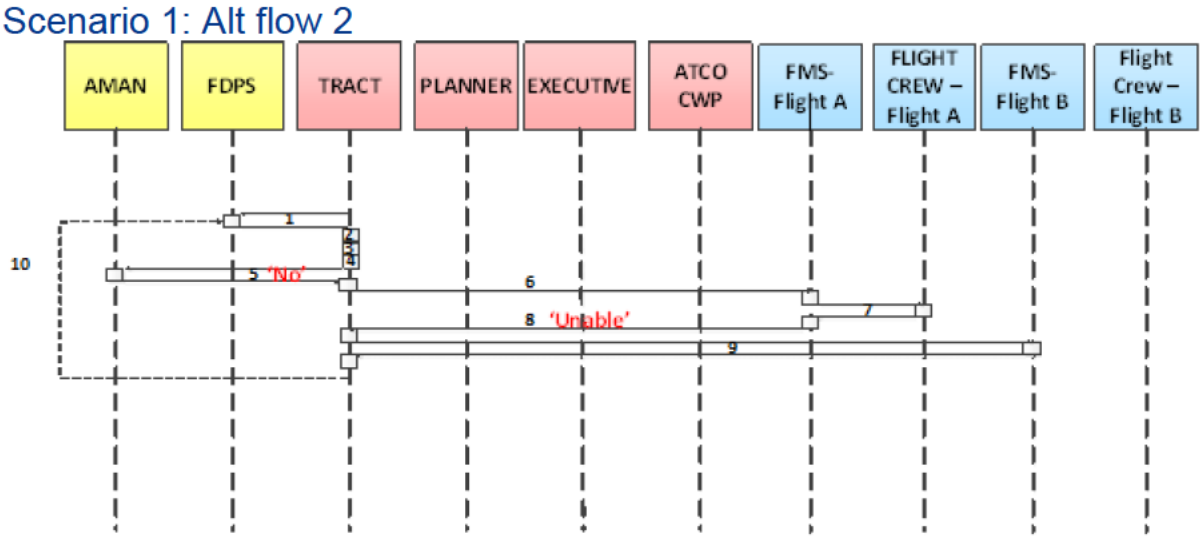


Figure 14: TRACT: scenario 1: Alt Flow 2

Scenario #1: Alternative flow 2: Aircrew cannot accept CTO

	Steps 1-6 the same
7	Flight crew assesses CTO but is unable to accept – Downlinks a UNABLE message
8	Flight crew unable to accept – Downlinks a UNABLE message
9	Following a rejection by the pilot TRACT uplinks a cancellation CPDLC message to all other aircraft in the cluster (in this diagram aircraft 'b')
10	Cluster is not solved, until the next TRACT cycle (i.e. starts from step 1)

Table 42: TRACT: scenario 1: Alt Flow 2

Scenario 1: Alt Flow 3

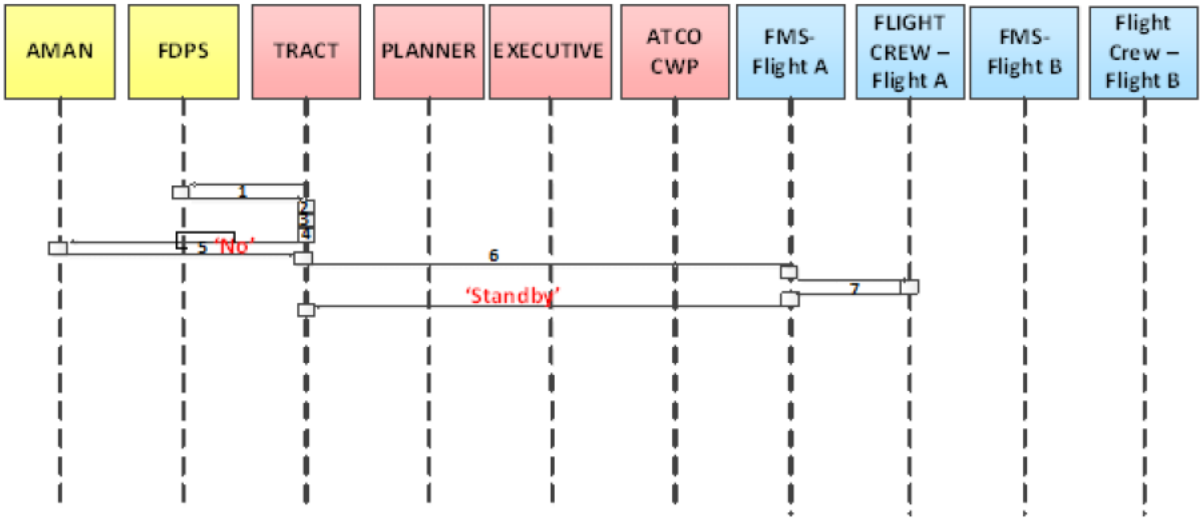


Figure 15: TRACT: scenario 1: Alt Flow 3

Scenario #1: Alternative flow 3: Aircrew reply standby to the CTO	
	Steps 1-6 the same
7	Flight crew assesses CTO – cannot accept immediately - Downlinks a STANDBY message
8	TRACT discards the flight from its former computation cycle until an acceptance or a rejection

Table 43: TRACT: scenario 1: Alt Flow 3

Scenario 2: TRACT Discards a TRACT Flight

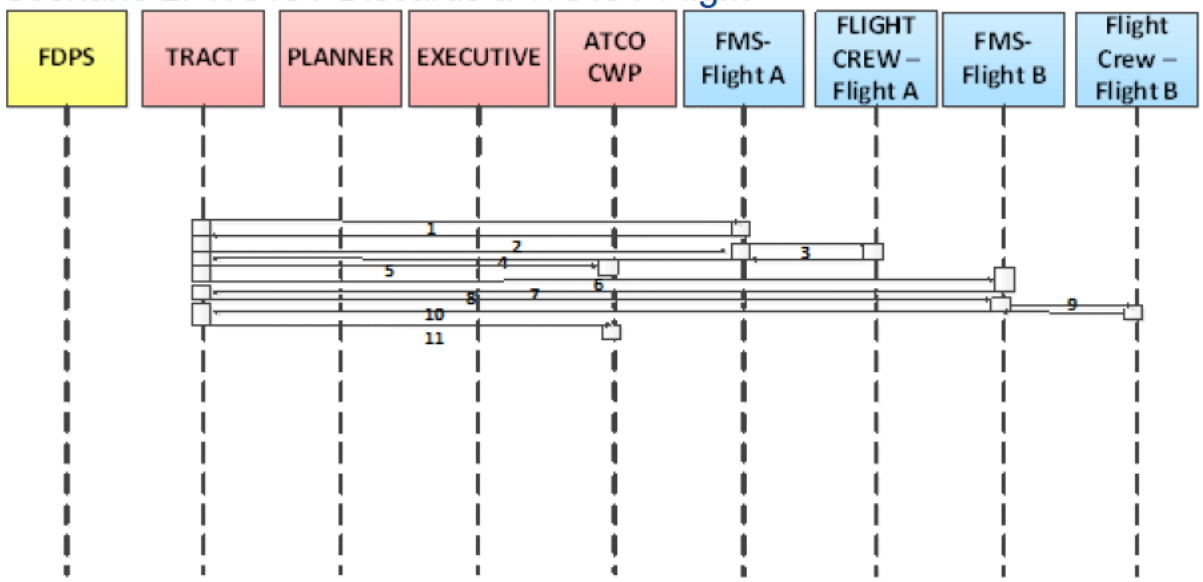


Figure 16: TRACT: scenario 2

Scenario #2: TRACT discards a TRACT Flight	
1	TRACT checks that the primary TRACT Flight (A) has a CTO
2	TRACT uplinks CPDLC 'Cancel Time Constraint' message to flight A
3	The flight crew of flight A removes the CTO from the FMS and sends a 'WILCO' message
4	The air system of flight A downlinks the EPP data with no CTO anymore
5	In parallel, TRACT un-tags the flight A in the CWP so that it appears no longer under TRACT management
The next steps to apply to all other TRACT flight that are involved in the TRACT resolution including the flight to discard i.e. the secondary TRACT flights	
6	TRACT checks that the secondary TRACT flight (B) has a CTO
7	TRACT checks that flight B is not involved in another conflict solved by TRACT
8	TRACT uplinks CPDLC 'Cancel Time Constraint' message to flight B
9	The flight crew of flight B removes the CTO from the FMS and sends a 'WILCO' message
10	The air system of flight B downlinks the EPP data with no CTO anymore
11	In parallel, TRACT un-tags the flight B in the CWP so that it appears no longer under TRACT management

Table 44: TRACT: scenario 2

Scenario 2: Alt Flow 1:

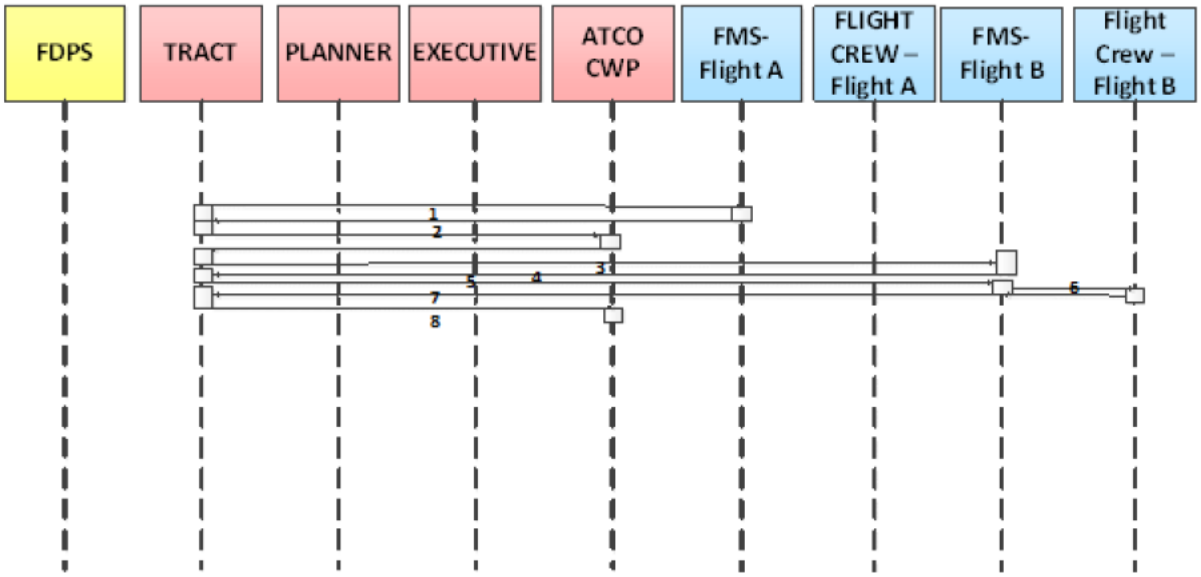


Figure 17: TRACT: scenario 2: Alt Flow 1

Scenario #2, Alternative Flow #1: The primary TRACT flight to discard has no CTO	
1	TRACT checks that the primary TRACT Flight (A) has a CTO- Primary flight has no CTO
2	TRACT un-tags the flight A in the CWP so that it appears no longer under TRACT management
The next steps to apply to all other TRACT flight that are involved in the TRACT resolution including the flight to discard i.e. the secondary TRACT flights	
3	TRACT checks that the secondary TRACT flight (B) has a CTO
4	TRACT checks that flight B is not involved in another conflict solved by TRACT
5	TRACT uplinks CPDLC 'Cancel Time Constraint' message to flight B
6	The flight crew of flight B removes the CTO from the FMS and sends a 'WILCO' message
7	The air system of flight B downlinks the EPP data with no CTO anymore
8	In parallel, TRACT un-tags the flight B in the CWP so that it appears no longer under TRACT management

Table 45: TRACT: scenario 2: Alt Flow 1

Scenario 2: Alt Flow 2

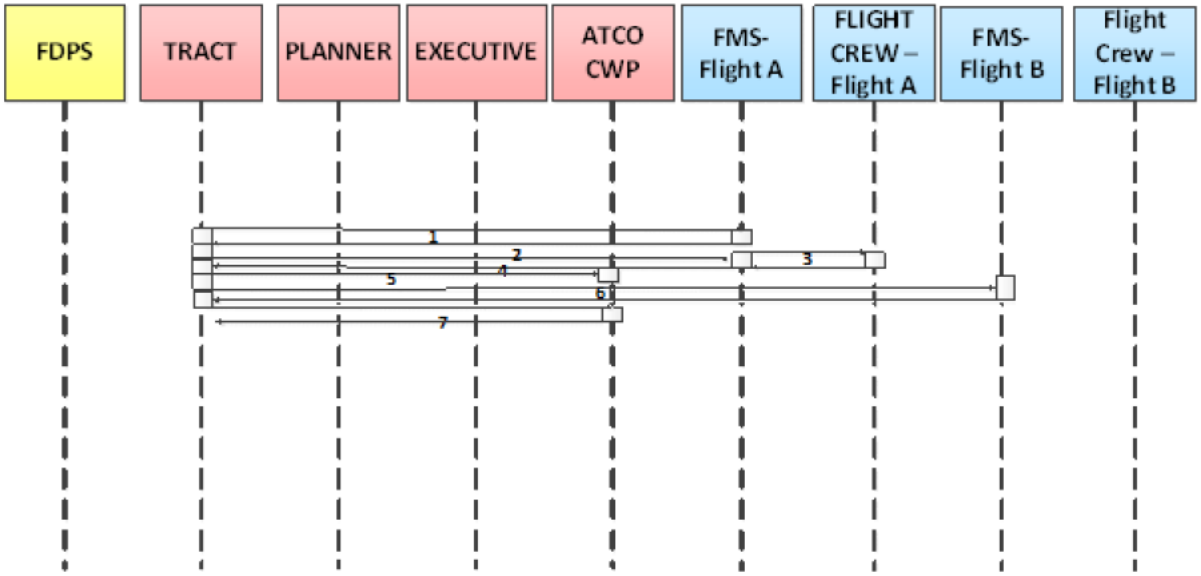


Figure 18: TRACT: scenario 2: Alt Flow 2

Scenario #2, Alternative Flow #2: The secondary TRACT flight to discard has no CTO	
Follow steps 1 – 6 as in scenario #2 @ step 6, flight B has no CTO	
7	TRACT un-tags the flight B in the CWP so that it appears no longer under TRACT management

Table 46: TRACT: scenario 2: Alt Flow 2

Scenario 2: Alt flow 3

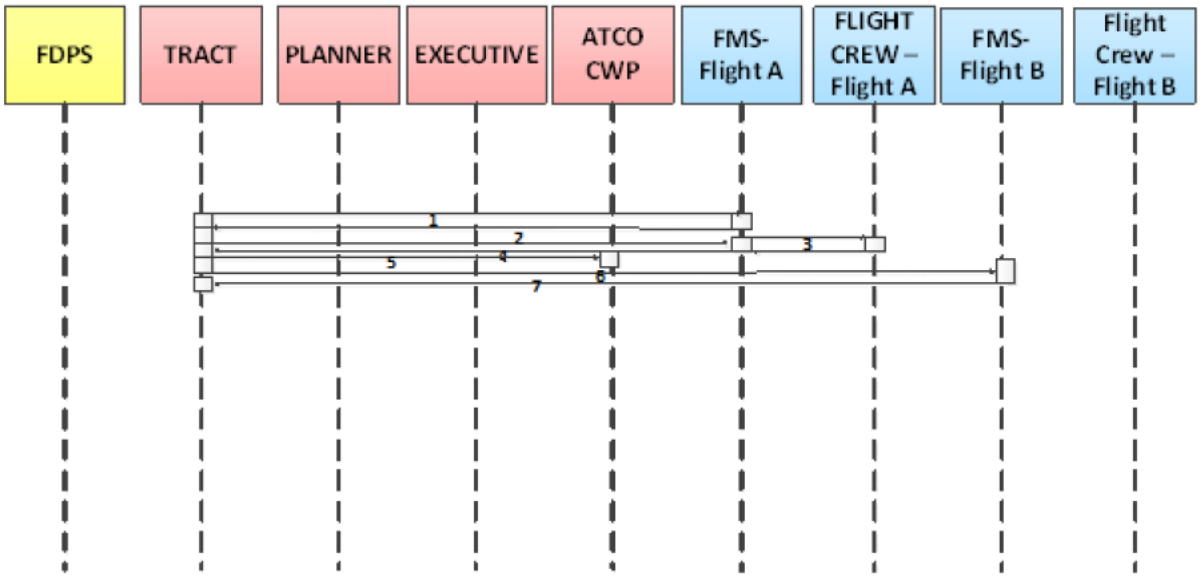


Figure 19: TRACT: scenario 2: Alt Flow 3

Scenario #2, Alternative Flow #3: The secondary TRACT flight is involved in another TRACT resolution

Follow steps 1-7 as in scenario #2
The flow continues at step 6 with another secondary TRACT flight

Table 47: TRACT: scenario 2: Alt Flow 3

Scenario 2: Failure Flow

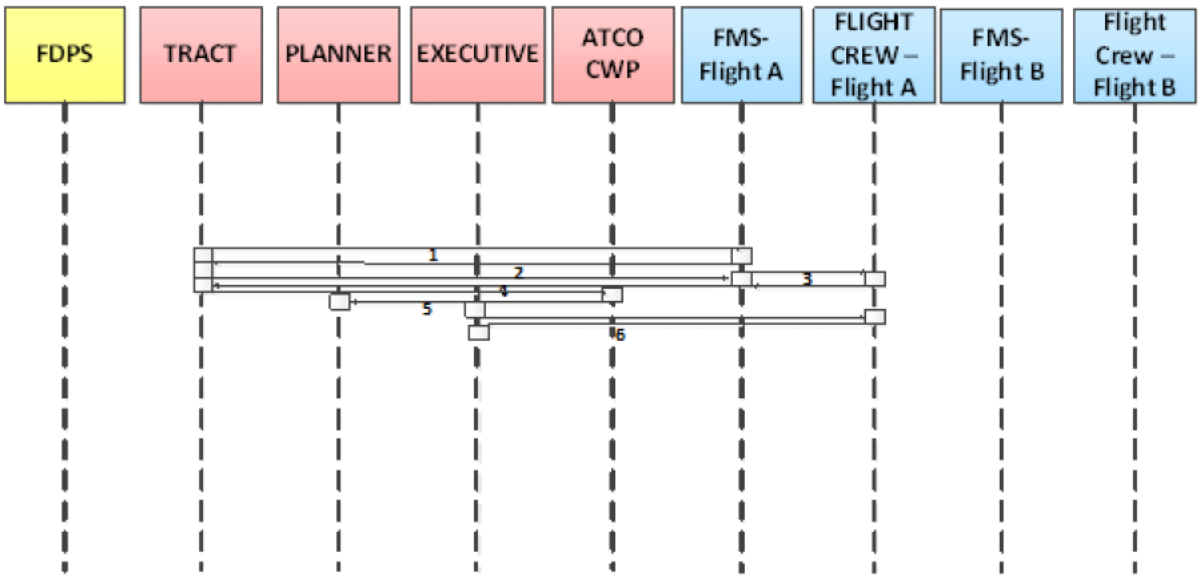


Figure 20: TRACT: scenario 2: Failure Flow 1

Scenario #2, Failure Flow #1: the EPP data still contains the CTO	
Steps 1 - 3	
4	The EPP data still contains the CTO a time threshold after the CTO removal has been uplinked
5	The CWP warns the controller about the inconsistency
6	The controller and the air crew together make the situation consistent by voice

Table 48: TRACT: scenario 2: Failure Flow 1

A.1.2 PC aid

Scenario 1 – Entry Coordination

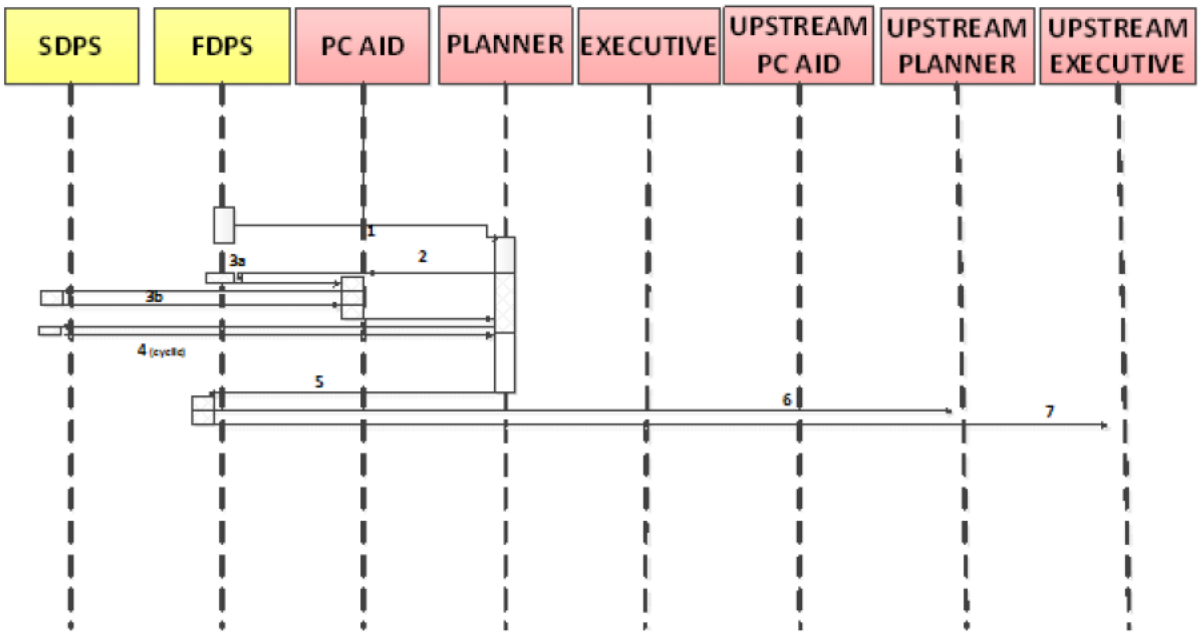


Figure 21: PC Aid scenario 1

Scenario #1: Entry Coordination	
1	FDP alerts Planner that there is a coordination offer
2	When Planner notices offer, makes the flight the subject and invokes PC Aid
3a	PC aid collects information about flights of interest from FDP and displays
3b	PC aid collects information about flights of interest from SDP and displays
4	Planner surveys surveillance info and combines with info from PC Aid (may be cyclic). Period of consideration
5a	If no planning encounters, planner accepts coordination via FDP
5b	If significant planning encounters, planner rejects flights
6	FDP tells upstream planner that the flight is accepted
7	FDP tells upstream executive that the flight is accepted

Table 49: PC Aid scenario 1

Scenario 1; Alt Flow 1; Revised Coordination

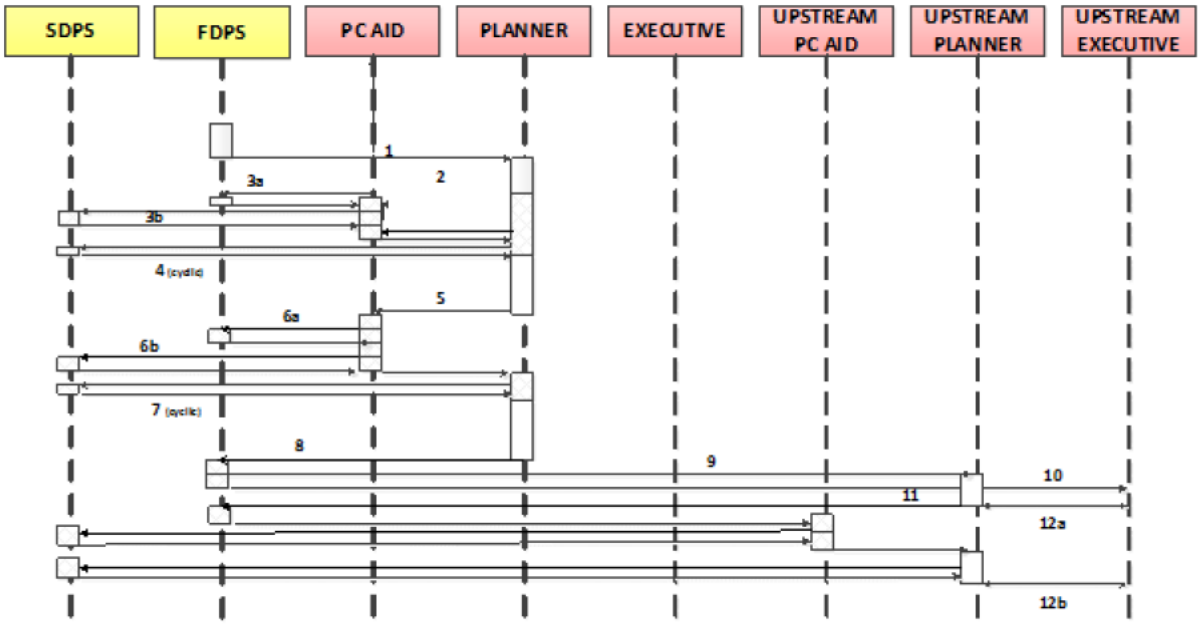


Figure 22: PC Aid scenario 1: alt flow 1

Scenario #1: Alternative Flow #1: Revised Coordination	
	Follow steps 1 – 4 in scenario #1 above
5	Planner invokes a 'What-if' probe via PC Aid
6a	PC aid collects information about flights of interest from FDP and displays
6b	PC aid collects information about flights of interest from SDP and displays
7	Planner surveys surveillance info and combines with info from PC Aid (may be cyclic). Period of consideration
8	Following consideration the planner revises and accepts the coordination via FDP
9	FDP tells upstream planner flight is accepted with revision
10	FDP tells upstream exec that flight is accepted with revision
11	Upstream planner consults PC Aid to verify acceptability of revised coordination
12a & b	Planner and Executive discuss implications of revised coordination on sector plan

Table 50: PC Aid scenario 1: alt flow 1

Scenario 1: Alt Flow 2: Discussion with Exec

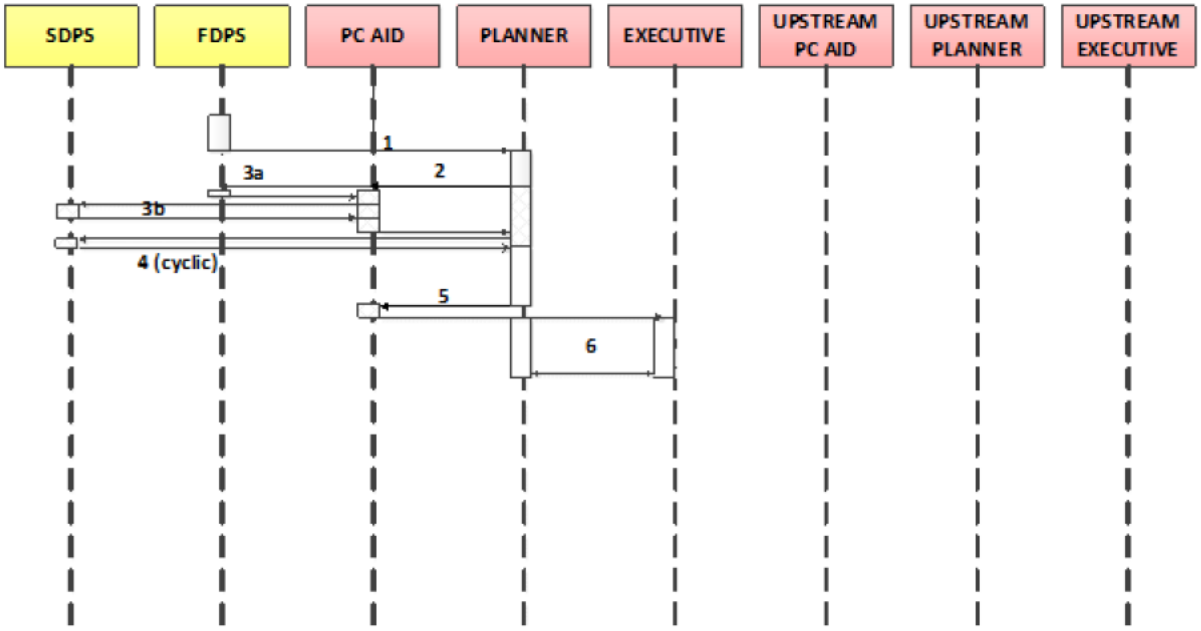


Figure 23: PC Aid scenario 1: alt flow 2

Scenario #1: Alternative Flow #2: Discussion with Exec	
	Follow steps 1- 4 as in Scenario #1
5	Planner instructs PC Aid to send encounter/pointout to Executive
6	Discussion between planner and executive to discuss planning encounter
	Either go to #5 from Scenario #1 or #8 from Scenario #1: Alternative flow #1

Table 51: PC Aid scenario 1: alt flow 2

Scenario 2: Exit coordination: Nominal conditions

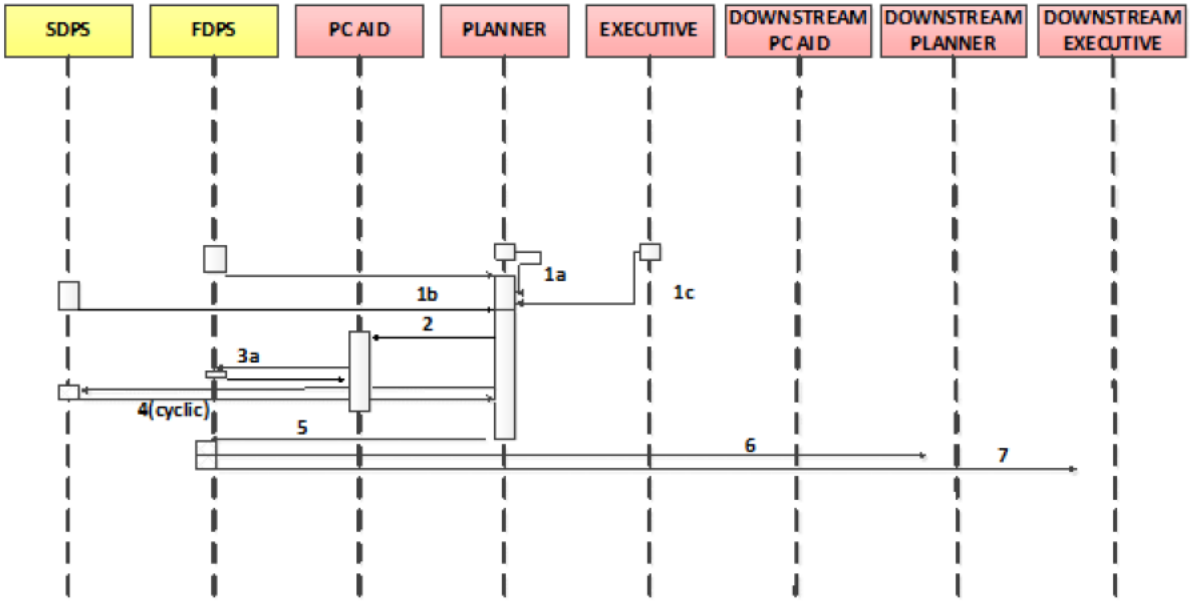


Figure 24: PC Aid scenario 2

Scenario #2: Exit Coordination – Nominal scenario	
	Either:
1a	Planner sets exit level as soon as aircraft is accepted in

1b	System (FDP/SDP) alerts Planner it is time to set a level
1c	Executive prompts planner to set exit level
	Either
2a	Planner chooses a level to 'what-if'
2b	Selects subject flight to perform 'what-else'
3	Planner collects info from FDP and SDP of flights of interest
4	Planner surveys surveillance info and combines with info from PC Aid (may be cyclic). Period of consideration
5	Planner sends offer to FDP
6	FDP sends level to Downstream Planner
7	FDP sends level to Downstream Executive
8	Downstream planner accepts coordination – as in steps 1-7 Scenario #1 Entry Coordination
Scenario #2: Alternative Flow #1 – Revision from downstream planner	
	Same as for Scenario #1: Alternative flow #1

Table 52: PC Aid scenario 2

Scenario #2: Alternative Flow #2 – Rejection from downstream planner	
	Follow steps 1- 7 as in Scenario #2
8	Downstream planner rejects flight
9	FDP informs planner that you have a rejection, but with additional constraint that you have to offer to another sector

Table 53: PC Aid scenario 2: Alt Flow 2

Scenario #2: Alternative Flow #3 – After level has been accepted you have to withdraw offer to downstream planner	
	Same steps as in scenario #1, but at step #10, the exec asks for another level (i.e. 1c)

Table 54: PC Aid scenario 2: Alt Flow 3

Scenario 2: Alt Flow 4: Planner wants to revise exit level

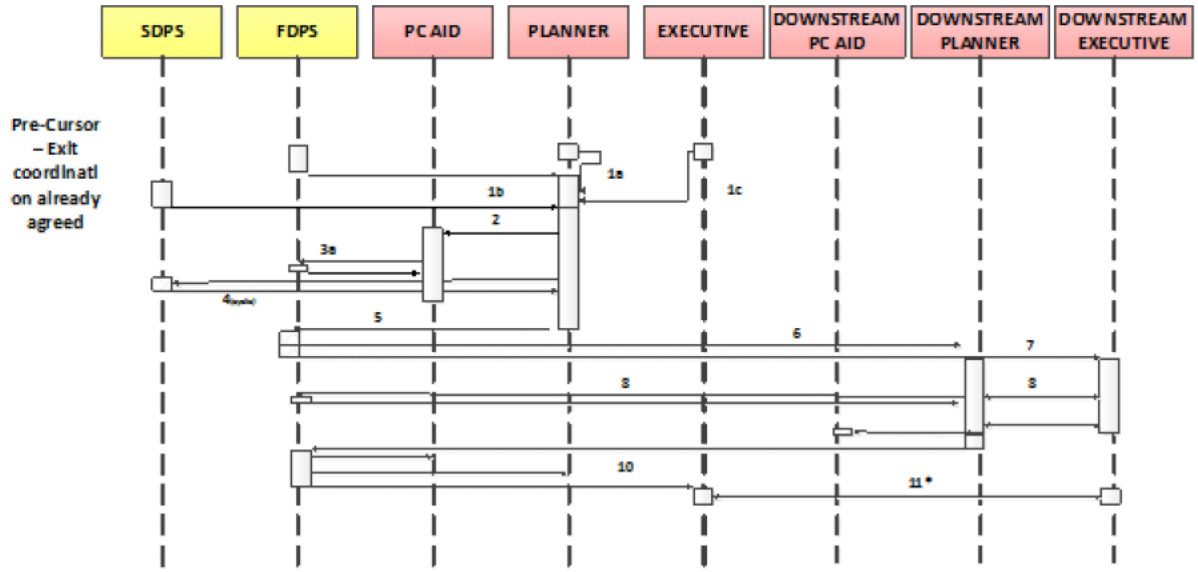


Figure 25: PC Aid: scenario 2: Alt Flow 4

Scenario #2: Alternative Flow #4: After exit flight level has been accepted, planner wants to revise exit level	
	Pre-cursor – Exit flight level is already agreed with the downstream sector
	Same steps as in Scenario #2; nominal up until step #7
8	Downstream Planner assess suitability of revised XFL
9	XFL is rejected by downstream sector

Scenario #2: Alternative Flow #4: After exit flight level has been accepted, planner wants to revise exit level	
10	FDP alerts the Planner and Executive that the coordination has been removed and require re-coordination. The original coordination is also removed from the PC Aid consideration
11*	Possible action – Executive and downstream Exec may try and resolve coordination between themselves.

Table 55: PC Aid: scenario 2: Alt Flow 4

Scenario 3:

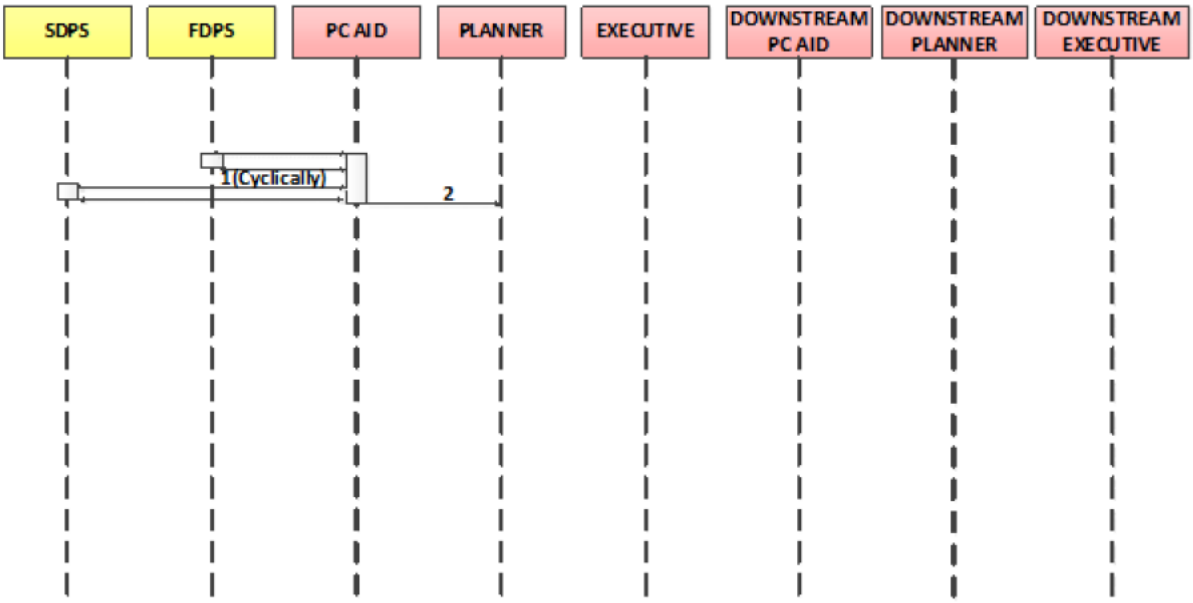


Figure 26: PC Aid: scenario 3

Scenario #3: Encounter arises with already accepted coordination	
1	SDP and FDP cyclically update PC Aid, PC Aid monitors coordinations
2	PC Aid alerts Planner if a problem with an coordination arises*
	*E.g. 2 flights exiting at different exit points, but meeting outside of the FIR Boundary (LACC West End 'Salad Confliction'

Table 56: PC Aid: scenario 3

Scenario 4: Integrated Coordination Entry

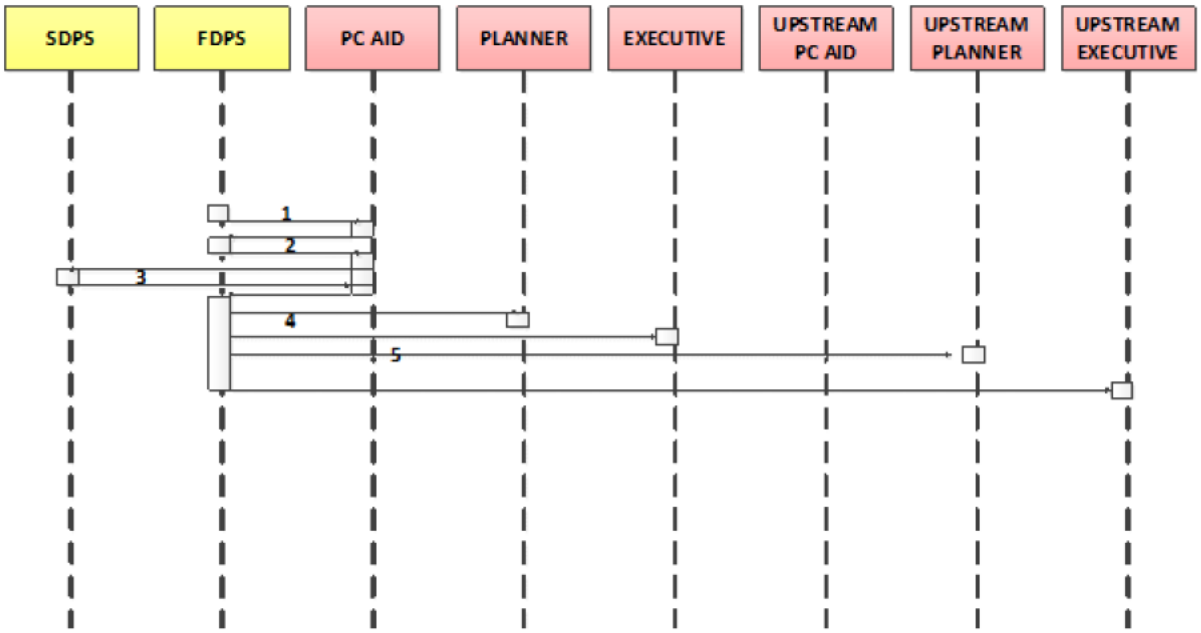


Figure 27: PC Aid: scenario 4

Scenario #4: Integrated Coordination – Entry Boundary	
1	FDP alerts the PC Aid that there is an new coordination received
2	PC Aid retrieves info from SDP and incorporates back into PC Aid
3	PC Aid retrieves info from FDP and returns
4	PC Aid alerts the FDP that the Coordination has been accepted
5	FDP alerts Planner, Executive, Upstream Planner and Upstream Executive that coordination has been accepted.

Table 57: PC Aid: scenario 4

Scenario 5: Integrated Coordination Exit

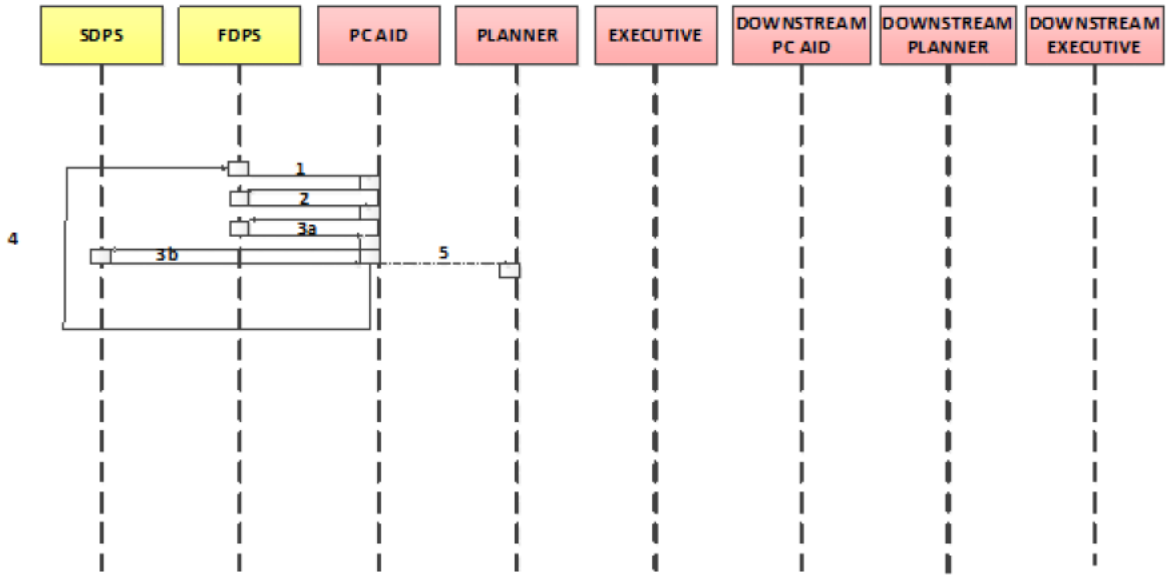


Figure 28: PC Aid: scenario 5

Scenario #5: Integrated Coordination – Exit Boundary	
1	FDP Alerts the PC Aid to coordinate an XFL
2	PC Aid finds potential XFL from FDP and/or internal TP
3	Test potential XFL for acceptability
	a. Collect data from FDP
	b. Collect data from SDP
4	Having found a problem on potential XFL auto-test alternative XFL (Via FDP or internal TP)
5	Refer to Planner if a suitable XFL cannot be found

Table 58: PC Aid: scenario 5

A.1.3 TC aid

Scenario 1: CD/R With TC Aid

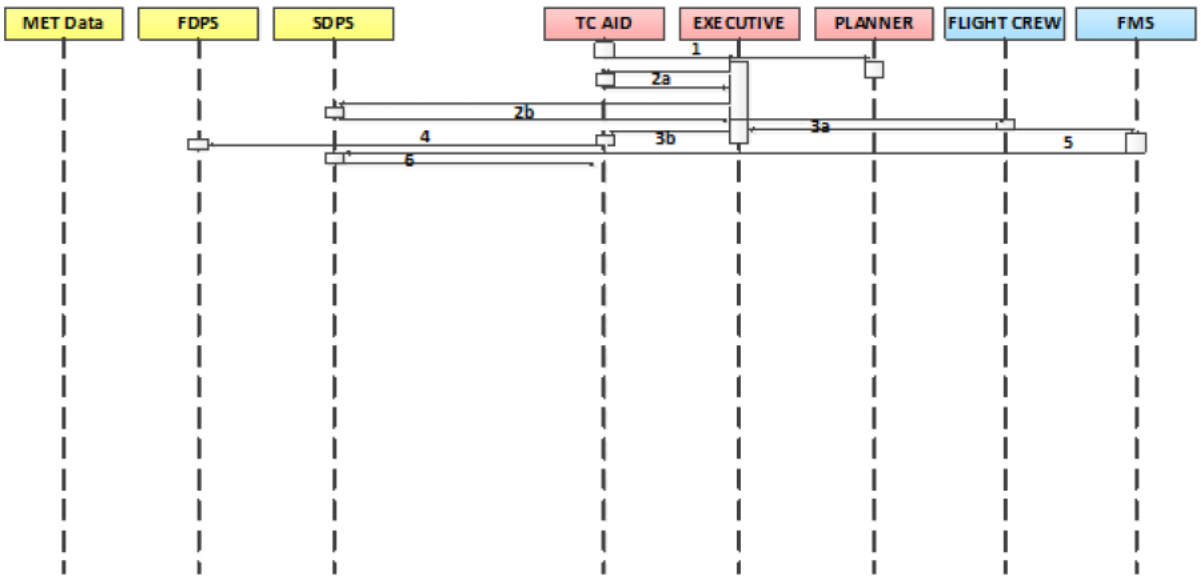


Figure 29: TC Aid: scenario 1

Scenario #1: TC Aid detects conflicts between 2 aircraft	
1	The TC Aid detects conflicting trajectories and shows a warning to the Executive and Planner Controller
2	The Executive and Planner perceive the warning and the Executive checks the validity (correctness) of the warning by looking at the situation display (2b) – alert is valid
3	3a. Tc issues executive instruction to flight crew and simultaneously enters instruction into the TC aid (3b.) whilst listening to the flight crews readback
4	TC Aid updates information based on latest Executive instructions
5	The air crew executes the clearance by modifying the trajectory, i.e. updates the FMS, which in turn updates the SDP
6	TC Aid is updated and the previous alert removed

Table 59: TC Aid: scenario 1

Scenario 1: Alt Flow 1; Conflict not relevant

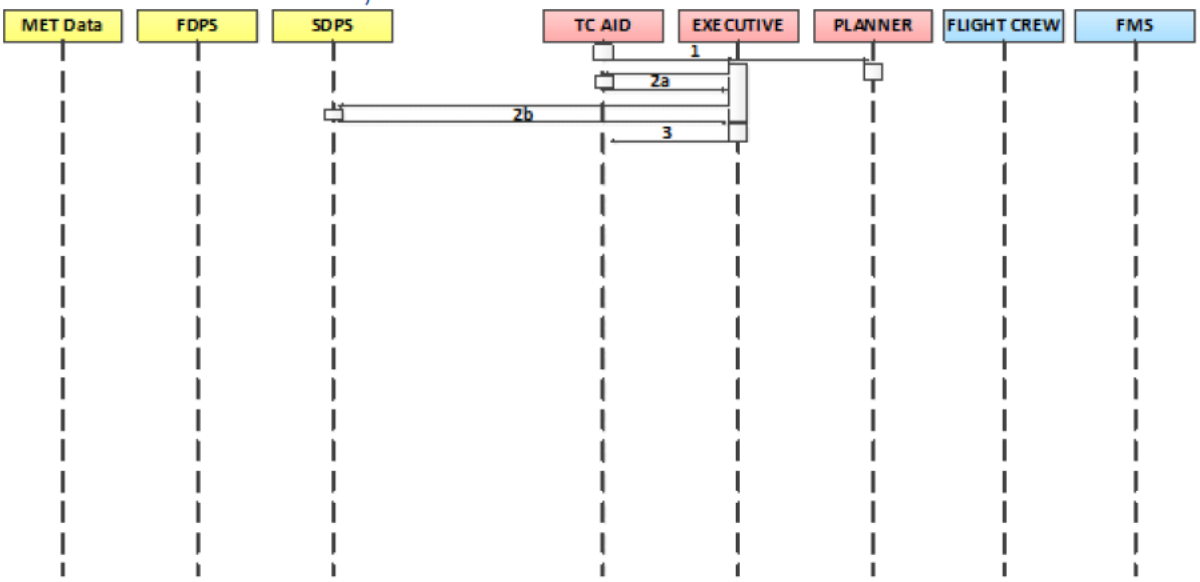


Figure 30: TC Aid: scenario 1: Alt Flow 1

Scenario #1: Alternative Flow #1: Conflict is not relevant	
	Same as Scenario #1 steps 1 & 2
3	Executive supresses the alert in the TC Aid and continues to monitor the traffic

Table 60: TC Aid: scenario 1: Alt Flow 1

Scenario #1: Failure Flow #1: Warning is not valid	
	Same as Scenario #1 steps 1 & 2
3	Executive supresses the alert in the TC Aid and continues to monitor the traffic

Table 61: TC Aid: Scenario 1: Failure Flow 1

Scenario #1: Failure Flow #2: TC ignores warning	
	Same as Scenario #1 steps 1 & 2
3	Executive supresses the alert in the TC Aid and continues to monitor the traffic
4	Conflict remains
5	Other safety nets detect conflict, e.g. STCA, PC Aid

Table 62: TC Aid: scenario 1: Failure Flow 2

Scenario 2: CD/R with What-else Probing

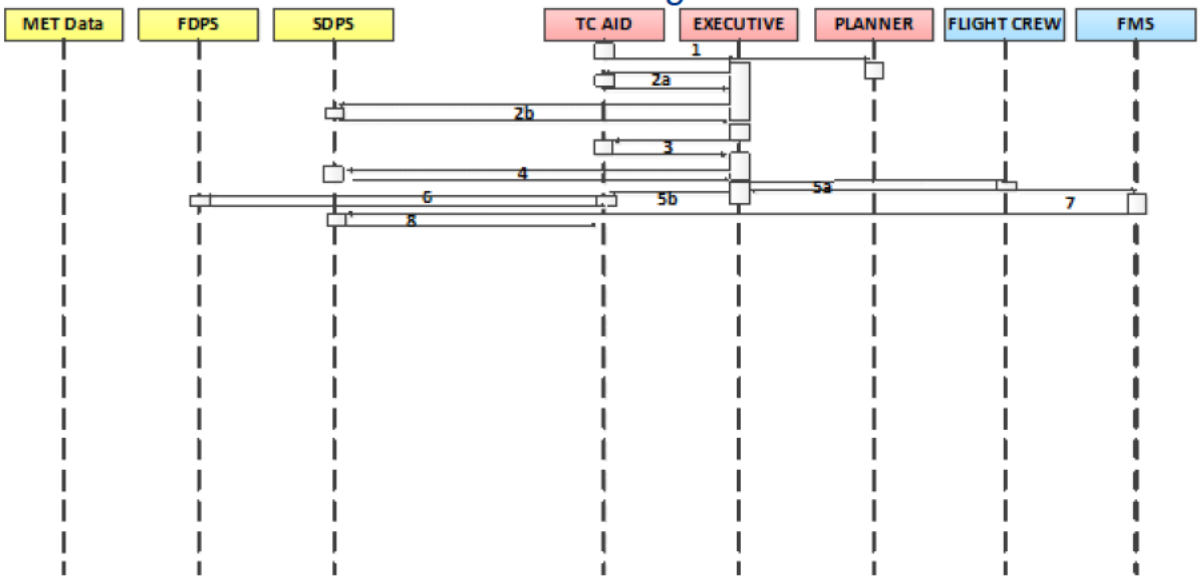


Figure 31: TC Aid: scenario 2

Scenario #2: Conflict resolution with what-else probing	
	Same as Scenario #1 steps 1 & 2
3	The Executive selects one of the conflicting aircraft and applies the a) Flight Level, b) Direct, c) Heading What-Else probing. The conflict free Flight Levels, Directs and Headings will be shown to the Executive
4	The Executive selects one solution and cross checks that the chosen solution is conflict free by surveying the situation display.
5	5a. Executive issues executive instruction to flight crew and simultaneously enters instruction into the TC aid (5b.) whilst listening to the flight crews readback
6	TC Aid updates information based on latest Executive instructions
7	The air crew executes the clearance by modifying the trajectory, i.e. updates the FMS, which in turn updates the SDP
8	TC Aid is updated and the previous alert removed

Table 63: TC Aid: scenario 2

Scenario 3: Detections of Deviations with MONA

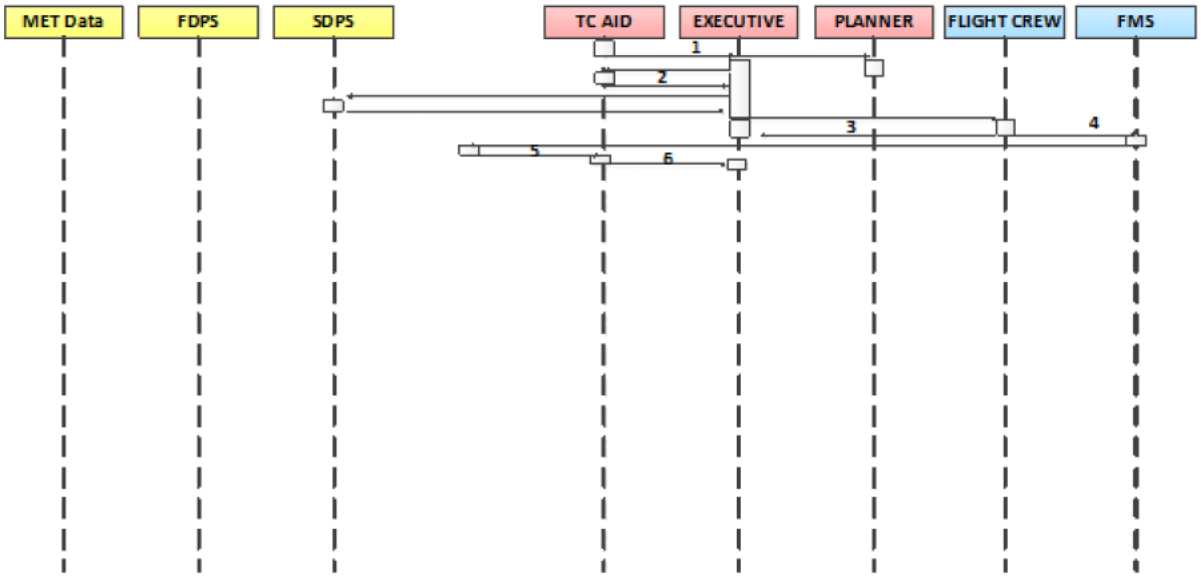


Figure 32: TC Aid: Scenario 3

Scenario #3: Detection of Deviations with MONA	
1	The Monitoring Aids (MONA) functionality detects a deviation and shows a warning to the Executive and Planner Controller indicating the kind of deviation (route, rate, flight level, no valid flight plan, Mode S DAP not consistent with controller clearance)
2	The Executive and Planner perceive the MONA warning and the Executive checks the validity (correctness) of the warning. Additionally, the Executive also checks that the entered system clearance data are correct.
3	In case of route, vertical rate or CFL deviation: the Executive contacts the air crew and asks for confirmation of current clearance data or mode S selected parameter
4	The air crew confirms the current clearance and resumes navigation according to this clearance
5	TC Aid is updated with correct/amended clearance – alert disappears
6	Executive checks deviation alert has disappeared

Table 64: TC Aid: scenario 3

Scenario #3: Alternative Flow #1: MONA is not valid	
	As in steps 1 & 2 for scenario 3
3	Executive deletes the warning and monitors the aircraft

Table 65: TC Aid: scenario 3: Alt Flow 1

Appendix B Failure Case Safety Objectives and Requirements Derivation

The objective of this workshop was to derive failure case safety requirements for the 04.07.02 Separation Task in En Route Trajectory Based Environment project. This workshop was held over three days examining each service for a day. The specific objectives were as follows:

- Identify all potential hazard causes associated with the system;
- Derive a complete set of logical requirements (requirements which define the logical way in which each functional block within the service would operate, these are more detailed than the SCSOs, but less detailed than the V3 ORs).

Attendees of the workshop:

Name	Organisation	Role
Andrew Burrage	Helios (representing NATS)	Safety Expert and Lead for SPR Task
Sarah Broom	Think Research (Representing NATS)	P04.07.02 Validation Support and SPR Task 20 (V2) support
Stephen Pember	NATS	Concept Expert
Michael Teichmann	DFS	ATC Expert
Pascal Deketelaere	DSNA	Concept Expert

B.1 Detailed PSSA results

Based on the graphical presentation and scenarios presented in A.1 the detailed results of the PSSA have been produced. Note for the PC/TC aid PSSA analysis, the steps of the scenarios have been recorded in the PSSA tables.

The tables in sections B.1.1, B.1.2, B.1.3 lists the detailed results of the PSSA for each of the three operational services. The SPR level model element are listed and potential hazard cause are identified for each, along with their hazard effect. Finally the functional hazard(s) to which each hazard cause relates is identified together with any potential mitigations.

As can be seen in Table 38: Safety Requirements or Assumptions - abnormal conditions for TRACT, Table 39 and Table 40 the Failure Case Safety Requirements are grouped and based on the failures of each model element presented in sections B.1.1, B.1.2, B.1.3, namely in the following way:

For equipment related functions:

- Loss *(e.g. "The probability of **loss** of FDPS shall be no more than 2.86E-03 per flight hour.")*;
- Delay (outdated/old) *(e.g. "The probability of **delay** of FDPS shall be no more than 2.86E-03 per flight hour.")*;
- Undetected corruption *(e.g. "The probability of **corruption (undetected)** of the PC Aid shall be no more than 9.52E-06 per flight hour.")*;
- Detected corruption *(e.g. "The probability of **corruption (detected)** of the Upstream PC Aid shall be no more than 1.54E-04 per flight hour.")*.

For operators:

– Misinterpret / Misunderstand *(e.g. "The probability of the Upstream Planner **misunderstanding** the tool shall be no more than 1.43E-04 per flight hour.")*.

As explained in section 3.4.2 the PSSA analysis also helped in deriving the probability numbers for each of the Failure Case Safety Requirements.

B.1.1 TRACT

Model element	Failure Mode	Failure Mode Effects	Functional Hazard Resultant	Mitigations
FDPS	Loss of flight plan data for a single aircraft	TRACT computes a solution without data on a particular aircraft which might be in conflict as a result	Hazard 001, 005 Hazard 002	Highlight a flight with missing flight plan data in the CWP.
	Loss of flight plan data for all aircraft	TRACT is unable to function	Hazard 004	Procedures
	Credible corruption of a flight plan (e.g. ATCO fails to enter clearance into the FDPS after issuing it to the aircraft)	TRACT fails to solve a conflict, solves a non-conflict, or creates/fails to solve a conflict by computing a wrong CTO	Hazard 004 Hazard 003 Hazard 001, 005,002	The ATCO has access to the CTO information, and may identify non-credible resolutions.
	Non-credible corruption of a flight plan	Unlikely: Equipment detects corruption: TRACT cannot compute resolutions for clusters involving a particular aircraft More likely: ATCO detects corruption (ATCO has access to flight plan data, and detects an inconsistency):	No hazard Hazard 004	ATCO has PC Aid to assist in detecting and solving conflicts
	Credible corruption of all flight plans (e.g. faulty trajectory prediction in FDPS)	TRACT fails to solve a conflict, solves a non-conflict, or creates/fails to solve a conflict by computing a wrong CTO	Hazard 004 Hazard 003 Hazard 001, 005,002	Extremely low probability.

	Delay in flight data for a single flight (e.g. controller issues a clearance, but there is a delay in entering it into the CWP, TRACT gets its input data the intervening time)	Most likely to cause TRACT to solve a non-conflict (for controller clearance)	Hazard 004 Hazard 003 Hazard 001, 005,002 (not considered likely)	Pilot may refuse the CTO if it is the aircraft which has just been issued a clearance.
	Delay in flight data for a set of flights (e.g. fall back to manual FDP in neighbouring centre)	As above, but for all affected flights	As above, but for all affected flights	TRACT is overridden by controllers during issue.
SDPS	As FDPS unless otherwise mentioned			
	Credible corruption of a single aircraft	In the worst case, same as corruption of the flight data. Depending upon the architecture and the details of the fault it may have no impact	Hazard 004 Hazard 003 Hazard 001, 005,002	
	Non-credible corruption of a single aircraft	Same as FDPS, except the equipment is more likely to detect corruption than the ATCO	No hazard Hazard 004	
	Delay: not considered as it is covered by corruption (part of surveillance is that it is provided in a timely fashion)			
ATCO CWP	Loss of a single TRACT indicator	Controller will monitor/intervene (perhaps unnecessarily).	Hazard 004	

	Total loss of TRACT indicators	Controller has increase in workload as he monitors and attempts to intervene for all aircraft even though TRACT is trying to manage them.	Hazard 004	
	Credible corruption of TRACT indicator Could be: Wrong aircraft indicated CTO information incorrect	Aircraft identity more important than CTO information. ATCO fail to take action on conflict, or vice versa. If CTO data is credible (e.g. swapped in the case of both a/c being under CTO) the controller workload is increased slightly as the data is inconsistent.	Hazard 001, 005, 002	
	Non-credible corruption of a single TRACT indicator	Controller ignores indicator? In the case of wrong aircraft identified, how does the ATCO know which aircraft should be applied (in this case it becomes loss of an indicator)	None in first case, Hazard 004 for the aircraft that has lost its indicator	
	Credible corruption of all TRACT indicators (not sure how this would happen)	Starts of as above, then quickly becomes non-credible.	Hazard 004	
	Non-credible corruption of all TRACT indicators	Same as total loss	Hazard 004	
	Delay of indicators for a single flight	Either short delay, in which case it is not a problem, or it is long enough to be equivalent to loss	Hazard 004	

	Delay of indicators for all aircraft	Either short delay, in which case it is not a problem, or it is long enough to be equivalent to loss	Hazard 004	
Tactical	Misunderstands TRACT indicators Could be: Wrong aircraft indicated CTO information incorrect	The Tactical may believe that a particular conflict is being solved by TRACT when it is not, or try and solve a conflict that is in fact being solved by TRACT.	Hazard 001, 004, 005	Potentially has the TC Aid to assist in solving conflicts.
Planner	Misunderstands TRACT indicators Could be: Wrong aircraft indicated CTO information incorrect	The Planner may believe that a particular conflict is being solved by TRACT when it is not, or try and solve a conflict that is in fact being solved by TRACT.	Hazard 002	Potentially has the PC Aid to assist in solving conflicts.
Flight Crew	Flight Crew misunderstands CTO information.	Flight crew tells ATCO they are unable to meet CTO – this is nominal situation. Or alternatively Flight crew accepts CTO when they are unable to do so. This may cause unnecessary workload for the controller.	First case: No Hazard. For the second Hazard 001, 005, 002 however this should be mitigated by system (see potential mitigations)	FMS calculations should inform flight crew if able or unable to meet CTO. EPP data should also contain an indication that the CTO is not reachable, so ground system is able to check it.
TRACT	Loss of TRACT for single cluster (failure).	Controller has to resolve conflict	Hazard 004	Has the PC Aid to assist in solving conflicts.

	Loss of TRACT for a single aircraft (e.g. unusual flight)	TRACT provides resolution for other aircraft not taking this flight into consideration. Therefore there are potential missed conflicts. If the controller does not realise that the unusual flights are not separated it could lead to delay in separation assurance	Hazard 001, 005 Hazard 002	Procedures that the controller must follow in the instance of unusual flight. Controller is likely to be paying special attention to this group. Unusual flights should be highlighted to the ATCO. It may be that it is not always the case (e.g. aircraft type that TRACT does not know). On the other hand, such aircraft will never be indicated as "managed by TRACT", so the ATCO should pay attention to them as to the other aircraft.
	Loss of TRACT for all clusters	TRACT doesn't perform its function at all. The controllers therefore have additional conflicts to resolve (compared to today)	Hazard 004	
	Credible corruption for a single cluster	Same as loss for a single aircraft. However the stituation for several aircraft may be very hazardous, and mitigated thanks to PC aid or TC aid. Such situation destroys any trust in TRACT: once it is experienced, ATCOs may disconinue use of TRACT.	Hazard 001, 005 Hazard 002	

	Credible corruption for a single aircraft, could be: CTO time wrong CTO sent to wrong aircraft (unlikely to be credible as it would require several aircraft covering the same point at the same time, on different levels)	In the worst case the corrupt CTO does not resolve conflict but the ATCO believes it will Doesn't resolve conflict (because it is the wrong aircraft)	Hazard 001, 005 Hazard 002	Controller monitors situation. PC aid and TC aid alert controller – note that PC/TC aid alerts may be the nominal situation depending on exact configuration (e.g. if PC /TC aid are more conservative than TRACT), and therefore controllers may still trust TRACT even in the case of PC/TC aid alerts.
	Non-Credible corruption for a single aircraft CTO sent to the wrong aircraft CTO could be outside flight path CTO could be outside performance (ETA min/Max)	The CTO would not be within the aircraft's route and therefore the flight crew should reject it.	No Hazard	
	Delay in TRACT sending CTO to aircraft.	The controller may start to attempt to resolve the confliction if they do not believe TRACT is doing so. This will lead to increased workload for the controller. They also may make decisions to solve the conflict (or the situation has changed for any other reason) that would then mean the TRACT resolution was inappropriate.	Hazard 004	In the case where the controller has taken intervening action the flight crew should reject the CTO. TRACT will remove the CTO if the controller issues a clearance

AMAN	Loss of AMAN link to TRACT (through CDPS)	TRACT is unaware that the flight already has an AMAN CTA restriction and issues CTO to aircraft. Therefore the flight now has a CTO and a CTA to meet which is incompatible.	Hazard 003	Procedures dictate that pilot follows CTA of highest priority then rejects CTO. (Note: In initial-4D, only one Time Constraint can be applied at a given time. The first one will be followed (on pilot's acceptance), the second one will be ignored. The issue is to adopt a logic between TRACT and AMAN: - Either a temporal limit e.g. from 20 minutes before landing, TRACT don't send any CTO, leaving the floor to AMAN - Or a priority system (within CDPS?) that chooses which Time Constraint to send to the aircraft For the moment, nothing has been decided.)
	Credible corruption of AMAN data to TRACT (through CDPS)	TRACT believes that either there is already a CTA for an aircraft and therefore does not issue a CTO (when it in fact could), or TRACT sends a CTO to an aircraft when in fact there is already a CTA (i.e. same as loss). This will cause increased workload for the controller.	Hazard 004	

	Non-credible corruption of AMAN data to TRACT (through CDPS)	TRACT is unable to utilise data from AMAN. Assuming that TRACT still tries to perform its function it is possible to have the same effect as for credible corruption above.	Hazard 004, 003	
	Delay of AMAN data to TRACT (through CDPS)	TRACT issues a CTO for an aircraft when in fact there is already a CTA applied to that aircraft but the data is delayed. When the CTA data does come through there is now conflicting clearances for the flight crew.	No Hazard	Procedures to dictate that pilot follows CTA of highest priority then says unable to comply with CTO
FMS	Loss (total, or loss of TRACT functionality or data)	Before issuing a CTO, TRACT asks the FMS for ETAmin,max interval. Should it miss the information, it wouldn't issue any resolution data, and therefore the ATCOs will be unable to use TRACT.	Hazard 004	

	Credible corruption	The FMS applies a corrupt CTO and therefore the resultant new TP is incorrect. This is undetected by the ATCO, therefore they believe that TRACT is resolving the situation when in fact it may not be. In the worst case the corrupt CTO could be causing a new conflict, and the aircraft downlinks data indicating that it is applying the real CTO (e.g. the corruption is only in the application of the CTO within the FMS). As TRACT receives the EPP data (i.e. the onboard TP) to check that CTO actually applies, and thus has the means to check that the air TP is correct this could a credible corruption by the FMS looks unlikely.	Hazard 001, 005 or Hazard 005	PC Aid TC Aid
	Non-credible corruption	The FMS applies a corrupt CTO which is non-credible and the resultant new TP is incorrect. Either the flight crew detect this directly, or the ATCO informs them when the downlinked data does not match the request from TRACT (which TRACT detects).	Hazard 004	

	Delay	There is a delay in the FMS applying the CTO. Depending on how long the delay is the ATCO may not even be aware, or the ATCO thinks for some time that TRACT is resolving the conflict when in fact this is not yet been put into action.	None – this is part of the nominal case and is equivalent to the flight crew responding with a stand by. Could be Hazard 004 if it were to occur a lot.	
ADS-C	Loss (for a single aircraft)	There is a loss of ADS-C data to TRACT meaning that no EPP data or RTA interval messages can be downlinked. This has the effect of TRACT believing that the CTO has not been applied and therefore being unable to supply resolutions. In the worst case the flight crew have applied the CTO and then subsequently are instructed by the ATCO to do something different leading to further workload for all parties.	Hazard 004	
	Loss (for all aircraft, e.g. the ground reception is non-functional)	If this scenario is a result of a wider datalink failure then TRACT will not be working. If the problem is limited to ADS-C downlinking only then the situation will be as above but resulting in much higher workload for the controller	Hazard 004	

	Credible corruption	Either TRACT will believe a CTO to have been applied when in fact it has not, or more likely the downlinked data will not match the requested CTO and TRACT will cancel the resolution.	In the first case Hazard 001, 002, 005. In the second case Hazard 004	
	Non-credible corruption	TRACT will not be able to confirm via downlink that resolutions have been applied and will therefore cancel them. It may also cause increased workload and confusion while the ATCO and/or flight crew is trying to understand what is happening	Hazard 004	
	Delay	If the delay is short there is no effect. If the delay is long the situation will be the same as delay at the FMS (e.g. equivalent to a standby)	Hazard 004	
CPDLC	Loss	There is a loss of the CPDLC functionality meaning that the CTO message will not be able to uplinked or the answer message to be downlinked. In this scenario TRACT is unusable. This will create increased workload for the controllers until the issue is resolved.	Hazard 004	

	Credible corruption	There is credible corruption of the CTO data and answer message being uplinked and downlinked by CPDLC and this is not detected by the ATCO. This could have the effect of TRACT failing to solve a conflict, as TRACT would have to reject the resolution when the downlinked data was checked and found to be corrupt.	Hazard 004	PC Aid TC Aid
	Non-credible corruption	TRACT will not be able to confirm via downlink that resolutions have been applied and will therefore cancel them. It may also cause increased workload and confusion while the ATCO and/or flight crew is trying to understand what is happening	Hazard 004	

	Delay	There is a delay in either/both the uplinking and downlinking of messages by CPDLC. The effect depends upon the length of the delay and how far out the aircraft/s are from the boundary. If not detected by the ATCO then no hazard. If the delay is significant workload will be increased while the ATCO queries with the flight deck, or they may make attempts to resolve a conflict themselves.	No hazard or Hazard 004	

Table 66 Detailed PSSA Results – TRACT

Taken from Table 67, each failure mode has a number of repetitive hazards which were identified in the FHA analysis. These hazards are presented in Table 68.

	Resultant Hazards for			
Failure Mode	Loss	Corruption	Delay	Misunderstanding
FDPS	Hazards 001, 002, 004, 005	Hazards 001, 002, 004, 005	Hazards 001, 002, 004, 005	
SDPS	Hazards 001, 002, 004, 005	Hazards 001, 002, 004, 005		
ATCO CWP	Hazard 004	Hazards 001, 002, 004, 005	Hazard 004	
Tactical				Hazards 001, 005
Planner				Hazard 002
TRACT	Hazards 001, 002, 004, 005	Hazards 001, 002, 005	Hazard 004	
AMAN	Hazard 003	Hazards 003, 004	Hazard 003	
FMS	Hazard 004	Hazards 001, 004, 005	Hazard 004	
ADS-C	Hazard 004	Hazards 001, 002, 004, 005	Hazard 004	
CPDLC	Hazard 004	Hazard 004	Hazard 004	

Table 67 PSSA Analysis - Resultant Hazards for each failure case TRACT

The number of times each of the hazards associated with TRACT appeared throughout the FHA analysis is then counted. The hazard *Maximum Tolerable Frequency of Occurrence*[24] is then divided by this number and the tolerable failure rate for each hazard is identified. For TRACT, the probability of the

TC/PC aid tools failing and a non-reaction from the controller have been added. The final tolerable failure rate is obtained by dividing the tolerable failure rate to the TC/PC aid failure rates and to the controller non-reaction rate. The final numbers for each hazard are shown in Table 73 PSSA Analysis - Hazard Tolerable Failure Rate PC aid.

Hazard #	Number of times Hazard has been identified throughout the FHA analysis	Tolerable Failure Rate (Hazard *Maximum Tolerable Frequency of Occurrence*[24]/Number of times throughout the FHA analysis	TC/PC aid Fails	Controller does not react	**Final Tolerable Failure Rate** (Tolerable Failure Rate/TC,PC aid Fails/Controller does not react)
001	18	1.11E-05	1.00E-03	1.00E-01	1.11E-01
002	17	1.18E-05	1.00E-03	1.00E-01	
003	10	2.00E-05	1.00E-03	1.00E-01	2.00E-01
004	32	6.25E-06	1.00E-03	1.00E-01	6.25E-02
005	14	2.86E-07	1.00E-03	1.00E-01	2.86E-03

Table 68 FHA Analysis - Hazard Tolerable Failure Rate TRACT

Out of the hazards identified in Table 68, the one with the lowest probability of happening is chosen for each failure case. This will act as the maximum negative safety contribution to be taken into account for defining the corresponding failure case safety requirement. This analysis can be seen in Table 70.

Hazard Rates chosen for the Failure Case Safety Requirements				
Failure Mode	Loss	Corruption	Delay	Misunderstanding
FDPS	Hazard 005 (2.86E-03)	Hazard 005 (2.86E-03)	Hazard 005 (2.86E-03)	
SDPS	Hazard 005 (2.86E-03)	Hazard 005 (2.86E-03)		
ATCO CWP	Hazard 004 (6.25E-02)	Hazard 005 (2.86E-03)	Hazard 004 (6.25E-02)	
Tactical				Hazard 005 (2.86E-03)
Planner				Hazard 002 (1.18E-01)
TRACT	Hazard 005 (2.86E-03)	Hazard 005 (2.86E-03)	Hazard 004 (6.25E-02)	

[24] Can be found in the *Maximum Tolerable Frequency of Occurrence* column in Table 11 or in the *Final Rate* column in Table 74.

AMAN	Hazard 003 (2.00E-01)	Hazard 004 (6.25E-02)	Hazard 003 (2.00E-01)	
FMS	Hazard 004 (6.25E-02)	Hazard 005 (2.86E-03)	Hazard 004 (6.25E-02)	
ADS-C	Hazard 004 (6.25E-02)	Hazard 005 (2.86E-03)	Hazard 004 (6.25E-02)	
CPDLC	Hazard 004 (6.25E-02)	Hazard 004 (6.25E-02)	Hazard 004 (6.25E-02)	

Table 69 PSSA Analysis - Resultant Hazards Selection for the FCSR TRACT

B.1.2 CD/R aid to PC

Model element/Scenario	Failure Mode	Failure Mode Effects	Functional Hazard Resultant	Mitigations
Scenario 1, step 1- **FDP** alerts Planner that there is a coordination offer	Loss	Receiving sector never receives the offer to agree or reject, this would cause the offering sector to have to call the receiving. Might mean a late coordination, leading to fewer available options, which might lead to an induced conflict. Worst credible effect is that the receiver cannot accept the flight (and there is no viable alternative) – so the offering sector has to deal with it.	004	If the offering planner on top of his workload within the sector, he is likely to make the call with plenty of time to coordinate the aircraft.
		Additionally the receiving sector does not have functional tools (because they don't have the data), which might lead to missed conflict.	001	Similarly, if the receiving sector is monitoring for traffic approaching the sector they should wonder why they haven't received an offer for the aircraft and then investigate. The Tacticals on both sides can also notice that the coordination has not been done and alert the planner or make the coordination themselves.

	Delay	There is a delay in the coordination offer being sent to the receiving sector. The receiving sector during this time will be making coordination decisions that are not based upon including the delayed coordination offer, which therefore may affect these plans. This can therefore cause increased workload for the Planners if when the coordination offer does appear, it means that other coordination have to be amended, or as in loss, the available options for the offer are now reduced.	001	As above, the fact that the offer has been delayed may be picked up by either Planner or by wither Tactical.
	Corruption (goes to the wrong sector, or the aircraft is wrong or trajectory is wrong)	Wrong along track information: could show a potential conflict as no conflict or vice versa. Wrong aircraft is not credible. Wrong sector: Increased workload. Intended receiving sector: same as loss. Actual receiving sector: increased workload (detected), if they didn't detect and accepted there would be a coordination agreed which the receiving sector was unaware. Could be caused by splitting sectors after you coordinate something.	001 Or 002	Assumption that TC Aid is working correctly to monitor and pick up any potential encounters.

Scenario 1, step 2 – **Planner** notices offer, and makes the flight the subject and invokes PC Aid	Misinterpret/mis understand	Planner makes the wrong flight the subject of the PC Aid. This would cause confusion for the Planner and increased workload while trying to work out the 'odd response' You may induce Tactical workload as your confusion leads you to make a less inefficient decision.	005	Tactical may question decision When you select the next offer, you may realise what you've done (or continued confusion is possible!)
Scenario 1, step 3a + b – **PC aid** collects info from SDP and FDP and displays	Loss	Some data is lost completely e.g. an encounter and therefore this is not displayed to the Planner, Planner may make an unsafe decision based upon the data available E.g. TP at local CWP could fail (for speculative), even though primary TP is working OK.	001	The Planner may see the encounter on the radar or HMI Flight display (e.g. EFS- sees 2 flights @ 370) TC Aid will eventually pick up encounter Monitoring Mode aspect of PC Aid may pick up encounter eventually (may find after PC Aid in decision making mode fails to)
	Delay	Depends if planner makes decision before info is displayed, in which case same as loss. If planner is making decision as info is appearing, this could be a workload/frustration issue.	001	Requirements must specify how quickly info is displayed on radar display and PC Aid.

	Corruption	If undetected, essentially same as loss, but could lead to Hazard 1 or 2, Planner is making decisions based on info he doesn't know is incorrect. Workload increase for planner and/or tactical If detected – Planner has to stop using tool while he knows it is giving him incorrect information – increased workload (both Planner and Tactical), reduced flow rate	001 or 002 004	As for loss Use TC Aid, Radar, other Flight information until problem fixed Move workstations
Scenario1, step 4 – **Planner** surveys surveillance info and combines with info from PC Aid (may be Cyclic). Period of consideration	Misunderstand: controller sees a picture of what is happening now on the surveillance compared to intent on PC aid	Controller refuses a coordination offer which is actually ok, but doesn't look ok on surveillance or vice versa	005	
	Misinterpret: controller thinks that the tool has more data than it does (e.g. departing aircraft)	Equivalent to delay in step 1	005	Training on the tools limitations

Scenario 1,step 1, 5a + b – **Planner** either accepts of rejects flight	Misinterpret/mis understand	Assumption that in step 4 planner will have gone through the consideration making process. However planner may accept flight believing there is no encounter, when in fact there is Planner misinterprets flight, and rejects it when it does not need to be rejected; this causes workload to the previous sector as they have to re-offer the flight to another sector. The rejection could be entirely inappropriate, causing increased workload for all concerned, worst case, lead to overload (quite unlikely however)	001 002	As in loss, step 3. Previous sector challenges decision (depending on sector boundary) HMI requirements – how simple is it to reject a flight, is it easy to do by mistake?

Scenario 1, Step 1, 6 + 7 – **FDP** tells upstream planner and executive that flight is accepted	Loss	FDP doesn't tell offering sector that flight is accepted, planner thinks upstream knows it is. Eventually upstream will notice flight is not coordinated and probably make a telephone to resolve. Increased workload, possibly would result in a late climb, due to late coordination. In this case it's the FDP (or whatever sends the coordination message) that has failed, not the PC Aid	Doesn't fit in to any hazards, however will be increased workload potentially leading to hazardous workload demand. So therefore 005 After all, the tool is not misleading the controller, it is displaying the right info as to what is being input.	Upstream sector will know that flight has not been coordinated. Telephone call can resolve.
Scenario 1, alt flow #1 revised coord. Step 5 – **Planner** invokes a 'what-if' probe on an alternative NFL using the PC Aid	Misinterpret/mis understand	Planner invokes a what-if on an alternative level. In this case the info output is correct from the PC Aid, but the Planner may be confused about the level they have typed in and what they are expecting to be displayed.	Workload Hazard 005?? As all this would lead to increased workload.	Human Factors/controller training/HMI design

Scenario 1, alt flow 001 revised coord. Step 9 + 10 – **FDP** tells upstream Planner and Executive of revised coordination and acceptance	Loss	The fact that the coordination is revised is lost, but the fact it's accepted is not. The flight is transferred to the receiving sector at an potentially unsafe level The receiving sector NFL will be diff from offering sector XFL.	001 with little/late mitigation	Note: the way the current NERC coord works is that when a revision is sent, it's automatically saying the coordination is now accepted – will this be the design of the system?? Conformance monitoring functions and MTCD alerts, but possibly quite late and possibly showing imminent hazards.
	Delay	There is a delay in the coordination revision being sent to the upstream sector. This may lead to increased workload for both sides concerned, as the upstream sector may have climbed the aircraft to the original XFL, when actually, the receiving sector wanted it stopped off for e.g./ This will then result in telephone calls and negotiations etc.	001 or 002	Mops – e.g. as an offering sector do not clear flight all the way to XFL if the coordination has not yet been agreed.
Scenario 1, alt flow #1 revised Coord, Step 11 – **Upstream Planner** consults PC Aid to verify acceptability of revised coordination.	Misinterpret/mis understand	Planner may accept revised coordination and misunderstand the situation which increases tactical workload. E.g. revision is unachievable	Workload Hazard 005?? As all this would lead to increased workload.	Tactical may realise it's an inappropriate revision (i.e. Step 12 is a mitigation for Step 11) TC aid will highlight any unsafe clearances that they will potentially make. This scenario is not a late coordination, so still time to resolve

Scenario 1, alt flow #2, step 5 – Planner instructs **PC Aid** to send encounter pointout to Executive	Loss	Planner sends Pointout to the Tactical for the flights in question and the Pointout does not appear on the flights on the Tactical workstation. Planner for some reason forgets to talk to Tactical and accepts flights. Tactical is not aware of the encounter until the flights are within the sector and notices from his TC Aid and/or radar scan that there is a potential unsafe encounter to deal with	001	MOPs to dictate process. E.g. in what scenarios a telephone call should be made – after every pointout or just some depending on nature of encounter? TC Aid will pick up encounter eventually. The nature of accepting 2 flights in at the same level would prob be such that there is plenty of time to take action, even if Tactical is not aware until within the sector.
	Delay	There is a delay in sending the Pointout to the Tactical workstation. If appears in time to support decision the outcome would be no more than frustration. However, if delayed until after the decision is made it would be like loss scenario.		Requirement to say pointout shall be displayed in a certain time parameter.

	Corruption	Planner sends Pointout but they are different flights that are pointed out on the Tacticals screen. Undetected by both Tactical and Planner. If detected, increased workload due to the fact that the planner will have to verbally communicate with the Tactical – either by telephone or to physically get up to speak to them. (this gets worse as the ratio of Tactical to Planners decreases).	002 004	Following conversation would likely to resolve – i.e. detection of the situation
Scenario #2: Exit Coordination Steps 1a – **Planner** sets exit level as soon as aircraft is accepted in	Misinterprets/misunderstands	Planner does not set the exit level coordination, this results in the exit coordination being set late which can create high workload for the tactical and/or the next sector.	005 – new hazard	1b and 1c Next sector prompts for a level Depends how system works – may default to RFL or NFL MOPS- as soon as flight accepted in, set XFL immediately.
Scenario #2: Exit Coordination Steps 2a + 2b – **Planner** choses level to 'what-if' or 'what-else'	Misinterprets/misunderstands	We have already covered this in previous scenarios.		

Scenario 2, Step 3 – **PC Aid** collects info from FDP and SDP for flights of interest	Loss	E.g. PC Aid fails to show context flights for an XFL what-if, this can result in planner setting unachievable XFL, therefore creating high workload for the Tactical, worst case creating an overload.	005	TC Aid highlights if TC is about to make any unsafe clearances TC will recognise if plan is unachievable
	Corruption – undetected	PC Display of data is corrupted and is undetected by the Planner. This may lead the Planner to make inefficient and/or unsuitable XFL Coordinations.	001	TC Aid highlights if TC is about to make any unsafe clearances TC will recognise if plan is unachievable
	Corruption – detected	Planner is aware that the PC is not displaying the correct output of information in the PC Aid, therefore cannot rely on using the PC Aid until the issue is resolved. This has the result of increasing the workload for the Planner	004	
Scenario 2, Step 4 – **Planner** surveys surveillance data and combines with info from PC Aid (may be cyclic). Period of consideration	Misinterprets/misunderstands	Same as collecting info for entry but not as hazardous as this is for setting XFL's, for many flights they are not necessarily at those levels yet. If he misunderstands or misinterprets what the PC aid is showing, this can cause high workload for the tactical	005	TC recognise if plan is unachievable Split sector for overload

Scenario 2, Step 5/6/7 – Planner sends offer to **FDP**, FDP sends level to downstream Planner and executive.	Loss	PC Aid does not send the offer to the next sector. Tactical is not sure the XFL planned is accepted, flight is getting closer to the boundary. The downstream sector does not have an offer, they may be unaware of this flight and making plans not taking this flight into consideration.	005	Depends on HMI Controllers awareness of the sector and flights approaching their boundary so therefore could alert offering sector
	Delay	May create increased workload/confusion, especially if the offer arrives late, you could have made another planning decision based on this	005	
	Corruption - undetected	System corrupts the message, e.g. the XFL is changed or some aspect of the coordination and Planner is unaware. The downstream sector makes a decision on that and accepts it, however the actual coordination is unsafe	001 with little/late mitigation	Some kind of deviation monitoring may pick up error TC Aid/Tactical may pick this up if all info for the Tactical tools is correct.
	Corruption - detected	Planner is aware the PC Aid is sending false info, therefore stops using until fixed, however causing increased workload	004	
Scenario 2, alt flow #1 – revision from downstream planner	Already covered when Planner sends a revision to upstream planner in scenario 1, alt flow #1			

flow #2, rejection from **downstream planner**, step 8 – downstream planner rejects flight	Loss	Downstream Planner rejects the flight, but the offering Planner does not receive this message. The resultant scenario depends on how the system works – if the system shows this flight as accepted, and then this is very hazardous as the offering sector will transfer the aircraft when the receiving sector is unable to accept it – this could have safety consequences in terms of conflicting traffic and/or traffic overload If the system does not receive the rejection but the flight is showing as not yet accepted, then the Planner is unable to transfer this flight until he is sure the coordination has been accepted. This causes increased workload for both the offering and receiving sectors	001	Situational awareness of Planner and Tactical on both sides monitoring the traffic that is approaching the sector boundaries.

	Delay	The downstream sector rejects the flight and this message is delayed in reaching the offering sector. This may cause increased workload, as the planner is delayed in re-coordinating the aircraft e.g. having to offer to an alternative sector. In this time the Tactical may have already given the aircraft a certain level or route clearance which is no longer appropriate. The re-coordinated of the aircraft may become quite tricky.	001 or 002	Situational awareness of Planner and Tactical on both sides monitoring the traffic that is approaching the sector boundaries e.g. the downstream tactical or planer may notice that the flight in question is climbing to an inappropriate level or taking an inappropriate routing.
	Corruption – undetected	The downstream planner rejects the flight, but this message is corrupted e.g. rejects the wrong flight. This has safety consequences as the offering sector may think that the subject flight is coordinated/accepted when it is in fact not and consider that flight safe to transfer to the next sector (again, depends how the system will deal with rejection messages). It will also increase workload as the Planner now has to re-coordinate the flight that is being shown as rejected. Inevitably this will lead to confusion between the offering and downstream planners.	001 or 002	Situational awareness of Planner and Tactical on both sides monitoring the traffic that is approaching the sector boundaries When Planner tries to re-coordinate the wrongly rejected flight, they should soon detect the error

	Corruption - detected	The downstream planner rejects the flight and the wrong aircraft is shown as rejected. This is detected by the planner. This causes increased workload as the planner is unable to use the planner support tools until the issue is resolved.	004	Use TC Aid, Radar, other flight information until problem fixed Move workstations
Scenario 2, alt flow #2, rejection from downstream planner, step 9 – FDP informs **planner** that you have a rejection, but with additional constraint that you have to offer to another sector.	Misinterprets/misunderstands	I feel like we have covered this sufficiently in the scenarios above. However, the Planner may misinterpret or misunderstand the rejection message. This may result in the Planner trying to re-offer the flight back to the original downstream sector which will increase workload and inevitable lead to telephone discussion between offering and downstream sector.	005	As long as the HMI is clear and understandable for a rejected flight, cannot really see the Planner being confused by this

Scenario 2, alt flow #3, at step 10 in scenario 1, exec asks the **planner** for another XFL to be coordinated	loss	A coordination offer has already been sent to the downstream sector and accepted, however the Tactical controller then asks for the XFL to be changed (e.g. change of RFL from the pilot). The planner withdraws the offer to the downstream sector so he can re-coordinate a new level. This withdrawal message does not reach the downstream sector PC Aid. The downstream sector is still expecting the flight at the original XFL. This could be potentially unsafe as the downstream sector could have conflicting traffic at the new XFL	001	The TC Aid would show an NFL? Alert if the flight is not at the coordinated NFL. Planner and Tactical may both notice the disparity between NFL and AFL.
	Delay	There is delay in the time between the planner withdrawing the offer to the downstream sector and them receiving it. This may cause some confusion for a short period of time, and potentially increased workload when the withdraw message does come through.	001 or 002	MOPs to dictate always make a telephone call with a withdrawal of an offer?
	Corruption-undetected	The planner withdraws an offer from the downstream sector and the wrong flight is withdrawn. This is undetected by both parties. This will cause increased workload and potential confusion when the planner tries to re-coordinate the offer. However the situation should be detected fairly quickly	001 or 002	

	Corruption - detected	The planner withdraws an offer from the downstream sector and detects that the data is corrupt. He therefore can no longer use the PC Aid until the problem is rectified. This will cause increased workload.	004	Use TC Aid, Radar, other flight information until problem fixed Move workstations
Scenario 2, alt flow #4, planner wants to revise XFL	Scenario already covered			
Scenario 3, Encounter arises with already accepted coordination, Step 1 SDP and FDP Cyclically update the **PC aid**, PC Aid monitors coordinations.	Loss	The component of the PC Aid that monitors coordinations within the sector (Coordination Monitor – CM) does not display information about a specific encounter. Therefore the planner is unaware that a certain coordination within the sector is not being monitored. They will therefore be unaware if this specific encounter severity worsens.	001	TC Aid will pick on the encounter when it is within TC Aid separation parameters Tactical or planner may pick up on encounter from radar monitoring
	Delay	The CM delays displaying information about a specific encounter. Depending on how long it takes for the encounter to appear in the CM will determine the outcome of this scenario.	001	The encounter will be displayed eventually, possibly before it even appears in the TC Aid. TC Aid will pick on the encounter when it is within TC Aid separation parameters Tactical or planner may pick up on encounter from radar monitoring

	Corruption - undetected	The CM is displaying incorrect encounter information to the Planner and this is undetected, therefore may be showing encounters that do not actually exist or missing encounters completely.	001 or 002	TC Aid will pick on the encounter when it is within TC Aid separation parameters Tactical or planner may pick up on encounter from radar monitoring
	Corruption - detected	The Planner detects that the CM is not displaying the correct information and therefore cannot use the PC Aid	004	Other aspects of the PC Aid may still be functionality be working e.g. TP and MTCD.
Scenario 3, step 2, PC Aid alerts **Planner** if a problem with a coordination arises	Misinterprets/misunderstands	The Planner misinterprets or misunderstands the information that the CM is displaying. Therefore this may lead them to make some inefficient and or/inappropriate coordination decisions. This will in turn create confusion and increased workload	005	Tactical and/or upstream and downstream planners may question inappropriate coordination decisions
Scenario 4, Integrated Coordination Entry Boundary, step 1, 2 + 3 – FDP alerts the **PC Aid** that a new coordination received.	Loss	The PC Aid does not receive an alert that there is a new coordination offer to consider. Therefore the flight is not coordinated into the sector. The planner may be making other coordination decisions that could be affected by the flight that IC has failed to coordinate.	003	Eventually the upstream sector should realise that the flight has not been accepted and will contact the planner to coordinate the aircraft – however this is now a late coordination and will increase workload
	Delay	There is a delay in the PC aid receiving and considering a new coordination offer. Planner is unaware of this delay and may be making other coordination decisions that could be affected by the flight that IC is delaying to coordinate	003	If when the flight is coordinated by IC, the PC Aid monitoring functionality should alert the planner to any previous coordinations that are no longer suitable

	Corruption – undetected	The wrong aircraft is sent to the IC part of the PC Aid functionality to be coordinated. This means that the MTCD output is based up upon the wrong aircraft set, hence will give misleading encounter information.	003	TC Aid will pick on the encounter when it is within TC Aid separation parameters Tactical or planner may pick up on encounter from radar monitoring
	Corruption - detected	The wrong aircraft is sent to the IC part of the PC Aid functionality to be coordinated. This is detected by the planner. The planner can no longer rely on IC functionality. This may result in increased workload.		Even though the IC functionality part of the toolset is no longer functioning properly, the MTCD support still will be so the planner can assess each coordination using the MTCD support.
Scenario 4, step 4 – **PC Aid** alerts the FDP that the coordination has been accepted, and step 5 – FDP alerts planner, executive and upstream planner and executive that the coordination has been accepted	Loss	The PC Aid does not inform the planner that coordination has been made by IC. This would result in the flight approaching the sector and the planner wondering why it has not been coordinated. This would result in increased workload and possibly confusion and frustration, as they are effectively coordinated the flight twice.	003	The situation would be resolved when the planner makes action to coordinate the flight.
	Delay	There is a delay in the PC aid in informing the planner that a coordination has been accepted by IC. This would have the same effect as the loss scenario above, as the planner would make moves to coordinate the flight when they saw that it was approaching the sector		The situation would be resolved when the planner makes action to coordinate the flight, or when the system actually coordinates the flight

	Corruption – undetected	The IC functionality informs the planner that a flight has been automatically coordinated safely, when in fact there is an issue with the flight, or vice versa. The planner is unaware of this corrupt information and may be making other coordination decisions that could be affected by the flight.	003	PC Aid monitoring functionality should alert the planner to any previous coordinations that are no longer suitable The planner or the Tactical may pick up on the unsuitable coordination from either the TC Aid, or from radar scan
	Corruption - detected	The IC functionality part of the PC Aid is not working correctly and presenting corrupt information to the planner. They detect this so no longer rely on IC functionality. This may result in increased workload.	004	Even though the IC functionality part of the toolset is no longer functioning properly, the MTCD support still will be so the planner can assess each coordination using the MTCD support.
	Misinterpret/mis understand	IC automatically accepts a flight into the sector and alerts the controller that it is accepted. The controller misunderstands this and thinks that they have to manually coordinate the aircraft. This creates increased workload.	005	The controller will realise his/her mistake when they go to manually coordinate the flight
Scenario #5 Integrated Coordination on Exit boundary Step 1 – FDP alerts the	Loss	The FDP does not alert the PC Aid to coordinate a flights XFL, therefore IC does not automatically perform this task. This would mean that the XFL has to be set manually which will increase workload	003	The Planner or Tactical would notice that an XFL had not been set for the flight and take action to set this manually

PC Aid to coordinate an XFL	Delay	There is a delay in the FDP alerting the PC to automatically set an XFL by IC. This would mean that the planner may start to take action to set the XFL manually which will increase workload	003	If the Planner or Tactical notice that the XFL has not been set by IC they would take action to set this manually
	Corruption - undetected	The FDP alerts the PC Aid to automatically coordinate an XFL for the wrong aircraft. This would result in incorrect MTCD output	003	Planner or Tactical picks up encounters from radar scan and/or from TC Aid
	Corruption - detected	The IC functionality part of the PC Aid is not working correctly and presenting corrupt information to the planner. They detect this so no longer rely on IC functionality. This may result in increased workload.	004	Even though the IC functionality part of the toolset is no longer functioning properly, the MTCD support still will be so the planner can assess each coordination using the MTCD support.
Scenario #5, step 2 – PC Aid finds potential XFL from **FDP** and/or internal TP, also relates to step 3a + b – Test potential XFL for acceptability from FDP and SDP.	Loss	The PC aid is unable to find XFL from FDP and /or internal FDP, therefore no XFL is able to be coordinated automatically by IC. This would mean that the XFL has to be set manually which will increase workload	003	If the Planner or Tactical notice that the XFL has not been set by IC they would take action to set this manually
	Delay	There is a delay in the PC Aid finding the XFL from the FDP and/or internal FDP therefore a delay in IC automatically coordinating an XFL for the aircraft. This would mean that the planner may start to take action to set the XFL manually which will increase workload	003	If the Planner or Tactical notice that the XFL has not been set by IC they would take action to set this manually

	Corruption - undetected	The PC Aid probes an incorrect XFL from FDP and/or internal TP but will actually display the XFL that should have been probed. Therefore the MTCD output will be incorrect	003	Planner or Tactical picks up encounters from radar scan and/or from TC Aid
	Corruption - detected	The IC functionality part of the PC Aid is not working correctly and presenting corrupt information to the planner. They detect this so no longer rely on IC functionality. This may result in increased workload.	004	Even though the IC functionality part of the toolset is no longer functioning properly, the MTCD support still will be so the planner can assess each coordination using the MTCD support.
Scenario #5 step 4, Having a potential problem on potential XFL auto-test alternative XFL (via **FDP** or internal TP)	Loss	PC Aid after finding a problem with original XFL does not auto-test an alternative, so therefore no XFL is coordinated. This would mean that the XFL has to be set manually which will increase workload	003	If the Planner or Tactical notice that the XFL has not been set by IC they would take action to set this manually
	Delay	There is a delay between the PC Aid auto testing the original XFL, finding a problem and then auto-testing an alternative XFL. This would mean that the planner may start to take action to set the XFL manually which will increase workload	003	If the Planner or Tactical notice that the XFL has not been set by IC they would take action to set this manually
	Corruption – undetected	I think this is the same as for 'corruption – undetected' in the previous step		
	Corruption - detected	The IC functionality part of the PC Aid is not working correctly and presenting corrupt information to the planner. They detect this so no longer rely on IC functionality. This may result in increased workload.	004	Even though the IC functionality part of the toolset is no longer functioning properly, the MTCD support still will be so the planner can assess each coordination using the MTCD support.

Scenario #5, step 5 – Refer to Planner if a suitable XFL cannot be found	Loss	The PC does not refer to the planner if a suitable XFL cannot be found. The Planner is not aware that the flight has not yet been coordinated, and may be making other coordination decisions based upon this knowledge which may no longer be relevant.	003	If the Planner or Tactical notice that the XFL has not been set by IC they would take action to set this manually. The coordination monitor functionality would alert the planner to any coordinations that are no longer suitable
	Delay	There is a delay in the PC aid referring the coordination to the planner as IC cannot find a suitable XFL. The Planner may not be aware that the flight has not yet been coordinated. They may be making other coordination decisions based upon this knowledge which may no longer be relevant.		If the Planner or Tactical notice that the XFL has not been set by IC they may take action to set this manually if they notice in the time of the delay. The coordination monitor functionality would alert the planner to any coordinations that are no longer suitable
	Corruption - undetected	The PC Aid refers the wrong aircraft to the planner, or refers the right aircraft when in fact there are no potential XFL issues. This may create increased workload and confusion while the planner tries to make sense of the situation.	003	Planner or Tactical picks up encounters from radar scan and/or from TC Aid The coordination monitor functionality would alert the planner to any coordinations that
	Corruption - detected	The IC functionality part of the PC Aid is not working correctly and presenting corrupt information to the planner. They detect this so no longer rely on IC functionality. This may result in increased workload.	004	Even though the IC functionality part of the toolset is no longer functioning properly, the MTCD support still will be so the planner can assess each coordination using the MTCD support.

Table 70 Detailed PSSA Results - PC aid

Results for PC aid

Taken from Table 71, each failure mode has a number of repetitive hazards which were identified in the FHA analysis. These hazards are presented in Table 72.

	Resultant Hazards for				
Failure Mode	Loss	Delay	Corruption (undetected)	Corruption (detected)	Misinterpret/Misunderstand
FDPS	Hazards 001, 004, 005	Hazards 001, 002	Hazards 001, 002, 004	Hazard 004	
SDPS	Hazard 001	Hazard 001	Hazards 001, 002, 004	Hazard 004	
Upstream PC aid	Hazard 003	Hazard 003	Hazard 003	Hazard 004	
PC aid	Hazards 001, 003	Hazards 001, 002, 003	Hazard 001, 002, 004	Hazard 004	
Downstream PC aid	Hazard 001	Hazards 001, 002	Hazards 001, 002	Hazard 004	
Upstream Planner					Hazard 005
Planner					Hazards 001, 002, 005
Downstream Planner					Hazard 005
Upstream Executive					Hazard 005
Executive					Hazard 005
Downstream Executive					Hazard 005

Table 71 PSSA Analysis - Resultant Hazards for each failure case PC Aid

The number of times each of the hazards associated with the PC aid appeared throughout the FHA analysis was then counted. The hazard maximum tolerable frequency of occurrence[25] was then divided by this number and the tolerable failure rate for each hazard was identified. This is shown in Table 73 PSSA Analysis - Hazard Tolerable Failure Rate PC aid.

Hazard #	Number of times Hazard has been identified throughout the FHA analysis	Tolerable Failure Rate (Hazard maximum tolerable frequency of occurrence[25]/Number of times throughout the FHA analysis
001	21	9.52E-06
002	10	4.00E-04
003	15	1.33E-05
004	13	1.54E-04
005	14	1.43E-04

Table 72 PSSA Analysis - Hazard Tolerable Failure Rate PC aid

Out of the hazards identified in Table 72 PSSA Analysis - Resultant Hazards for each failure case PC Aid, the one with the lowest probability of happening was chosen for each failure case. This will act as the maximum negative safety contribution to be taken into account for defining the corresponding failure case safety requirement. This analysis can be seen in Table 74.

[25] Can be found in the *Maximum Tolerable Frequency of Occurrence* column in Table 12 or in the *Final Rate* column in Table 75.

Hazard Rates chosen for the Failure Case Safety Requirements					
Failure Mode	Loss	Delay	Corruption (undetected)	Corruption (detected)	Misinterpret/Misunderstand
FDPS	Hazards 001 (9.52E-06)	Hazards 001 (9.52E-06)	Hazards 001 (9.52E-06)	Hazard 004 (1.54E-04)	
SDPS	Hazard 001 (9.52E-06)	Hazard 001 (9.52E-06)	Hazards 001 (9.52E-06)	Hazard 004 (1.54E-04)	
Upstream PC aid	Hazard 003 (1.33E-05)	Hazard 003 (1.33E-05)	Hazard 003 (1.33E-05)	Hazard 004 (1.54E-04)	
PC aid	Hazards 001 (9.52E-06)	Hazards 001 (9.52E-06)	Hazard 001 (9.52E-06)	Hazard 004 (1.54E-04)	
Downstream PC aid	Hazard 001 (9.52E-06)	Hazards 001 (9.52E-06)	Hazards 001 (9.52E-06)	Hazard 004 (1.54E-04)	
Upstream Planner					Hazard 005 (1.43E-04)
Planner					Hazards 001 (9.52E-06)
Downstream Planner					Hazard 005 (1.43E-04)
Upstream Executive					Hazard 005 (1.43E-04)
Executive					Hazard 005 (1.43E-04)
Downstream Executive					Hazard 005 (1.43E-04)

Table 73 PSSA Analysis - Resultant Hazards Selection for the FCSR PC aid

B.1.3 CD/R air to TC

Model element/Scenario	Failure Mode	Failure Mode Effects	Functional Hazard Resultant	Mitigations
TC Aid Scenario #1: **TC Aid** detects conflicts between 2 aircraft. Step 1 – The TC Aid detects conflicting trajectories and shows a warning to the Executive and Planner Controller.	Loss	The TC Aid detects conflicting trajectories between 2 aircraft but does not display a warning to the Executive or Planner controller. Both may not pick up on the impending loss of separation which is gaining severity as time progresses. The Executive controller may also be making other tactical decisions which would be affected by the impending loss of separation.	001	Executive and/or Planner controller pick up encounter from radar scan. Other tools (STCA etc.) can help.
	Delay	The TC Aid detects conflicting trajectories between 2 aircraft but there is a delay in this being displayed to the Executive and Planner controllers. This may lead to increased workload for the controller as it is taking them longer to make decisions	001	Performance requirement should specify that conflicting trajectories are displayed to the controller within x no of seconds.
	Corruption – undetected	The TC detects conflicting trajectories between 2 aircraft but displays the encounter incorrectly – e.g. on the wrong aircraft. This is undetected by the controller. The ~~MTCD~~ TC Aid's output displayed is incorrect and therefore worst case scenario there is a severe loss of separation.	001	TC and or PC pick up on confliction from radar. Ground based safety nets – e.g. STCA Airborne safety nets – e.g. TCAS

	Corruption - detected	The TC Aid detects conflicting trajectories between 2 aircraft but does not display the encounter to the controllers. This is detected by the controllers. Therefore the TC Aid cannot be utilised until the issue is resolved. This will greatly increase the workload of the Executive controller in particular and also the flow rates to the sector may need to be restricted, or the sectors split to the maximum number.	004	Assume that the PC Aid is working correctly to detect and monitor flights entering and exiting the sector. Working without this tool. Reduce flow rates through sectors.
Executive Scenario #1, step 2 - the executive and planner perceive the warning and the Executive checks the validity of the warning by interrogating the TC Aid and cross checking with the situation display.	Misinterpret/misunderstand	The TC aid detects conflicting trajectories between aircraft and displays to the controller. The controller then misinterprets /misunderstands the information that is being shown to them. This causes confusion and increased workload. The controller may end up issuing an unsafe clearance which creates an additional conflict.	005	The PC is also monitoring the sector and any encounters – they clear up the Executive controllers confusion. 4 – eyes - principle The monitoring functionality of the TC will keep on alerting the Executive to encounters.

Executive Scenario #1, step 3 – TC issues executive instruction to flight crew and simultaneously enters instructions into the TC Aid whilst listening to flight crews' read back.	Misinterpret/misunderstand	While the Executive is issuing the instruction to the flight crew, he mistypes the clearance into the TC aid. Therefore the aircraft is not performing as the TC aid predicts it to. There are many possible outcomes depending on the exact implementation and use of the system, but in the worst case this results in more workload for the controller. This should be investigated further in the next iteration. Alternatively, the TC enters the correct information, but either misspeaks or the pilot mishears, and reads back the instruction incorrectly. The controller does not pick up on this, and again the aircraft is not performing as the TC aid predicts it to.	005	The tool itself is a safety benefit in some cases of this scenario. For example if the controller enters the correct information into the system, but the aircraft does not receive the correct instruction, the tool will alert the controller. Deviation trajectories and alerts will alert the controller if the pilot is not complying with the clearance that the TC aid has programmed into it. Mode S may show the controller that the pilot is not following the correct clearance.

TC Aid Scenario #1, step 4 – TC Aid updates information based upon latest Executive instructions	Loss	The executive controller types instructions into the TC Aid but the TC Aid does not register the new instructions. Therefore the aircraft will not be performing as the TC Aid is predicting. This will mean that the Monitoring aids will present alerts to the controller saying the aircraft is not following the entered instructions when it actually is. This will increase the workload as he attempts to clarify the clearances with the pilot and attempts to re-enter the correct information into the TC Aid.	002	The deviation alerts will at least alert the controller to the fact that the most up to date clearances have not been entered correctly.
	Delay	The executive controller types instructions into the TC Aid but there is a delay in the TC Aid updating these instructions. Therefore if the delay is significant the above scenario as for loss would happen. If the executive controller is trying to resolve this scenario and then the instructions update, this will cause further confusion and workload issues. Additionally the controller may be late in entering the instructions, in this scenario there is unlikely to be an issue, as the difference between the TC Aid display and the controller's perception of the situation will simply remind the controller to enter the clearance.	002	Alert of the monitoring aids is a big help in such a situation! Procedures will specify that the ATCO should enter clearances into the system as they instruct aircraft. (New safety requirement) Requirement needed to specify how quickly the TC Aid will model new clearances once entered.

	Corruption – undetected	The executive controller enters instructions into the TC Aid and this data is corrupted. This may have the effect of the TC aid modelling the aircraft following different clearances than the aircraft is actually following. Alternatively it could send the right instructions to the wrong aircraft, again having the same effect. This will increase the workload for the Executive as he attempts to clarify the clearances with the pilot and attempts to re-enter the correct information into the TC Aid	002 001	The deviation alerts will at least alert the controller to the fact that the most up to date clearances have not been entered correctly
	Corruption - detected	The executive controller enters instructions into the TC Aid and this data is corrupted, and is detected by the ATCO. Therefore they cannot use the TC Aid for conflict detection and resolution. This will greatly increase the workload of the Executive controller in particular and also the flow rates to the sector may need to be restricted, or the sectors split to the maximum number.		Assume that the PC Aid is working correctly to detect and monitor flights entering and exiting the sector. Working without this tool. Reduce flow rates through sectors.

FMS Scenario #1, step 5 - The air crew executes the clearance by modifying the trajectory, i.e. updates the FMS, which in turn updates the SDP.	Loss	The FMS loses the data and does not update the trajectory. This means that the aircraft will not behave as predicted by the TC Aid, meaning that the resultant conflict detection is inaccurate.	002	Deviation alert/trajectories to alert the controller to the fact that the aircraft behaviour does not match that of the TP prediction in the TC Aid
	Delay	There is a delay in the FMS modifying the trajectory after the flight crew enters new clearances. Depending on the length of the delay, the TC Aid will begin to display deviation alerts to the controller. This will increase workload for the controller as they intervene to clarify the clearances with the flight crew.	002	Deviation alert/trajectories to alert the controller to the fact that the aircraft behaviour does not match that of the TP prediction in the TC Aid
	Corruption – undetected.	The FMS corrupts the clearance data which is undetected by the ATCO. This means that the resulting trajectory is inaccurate and will not match the clearance, but a Deviation Trajectory will be generated and the controller will be alerted by FPM.	002 001	Deviation alert/trajectories to alert the controller to the fact that the aircraft behaviour does not match that of the TP prediction in the TC Aid

	Corruption – detected	The FMS corrupts the clearance data but this is detected by the flight crew/and or the ATCO (note no alert was issued to indicate the corruption). The TC Aid cannot be used for conflict detection and resolution for that particular aircraft until the issue is resolved.	004	
SDP Scenario #1 – step 6, TC aid is updated and the previous alert is removed.	Loss	The confliction between 2 aircraft is resolved but the conflict alert remains. This increases workload for the controller.	002	The controller can delete an unwanted alert
	Delay	The confliction between 2 aircraft is resolved, but there is a delay in removing the alert. Depending on the delay there may be no hazard, but if significant, the effect would be the same as for loss. → No	No hazard	The controller can chose to delete an unwanted alert Other ground and airborne safety nets
	Corruption - undetected	The confliction between 2 aircraft is solved, but the alert is removed for the wrong confliction, not the one that has just been solved. The Executive is lead to believe that there is still a confliction between the original pair, and also are now unaware of another confliction within the sector.	002	The controller can chose to suppress an unwanted alert
	Corruption - detected	The confliction between 2 aircraft is resolved and the alert data is corrupted. This is detected by the controller. Therefore they can no longer rely on the alerting functionality of the TC Aid	004	The TP and CD aspects of the TC still functioning correctly. Other ground and airborne safety nets

Executive Scenario #1, alt flow #1: Conflict is not relevant. Step 3 – Executive supresses the alert in the TC Aid and continues to monitor the traffic	Misinterpret/misunderstand	The Executive controller misinterprets/misunderstands a conflict alert and suppresses when it is in fact a genuine alert. The controller is no longer aware of an impending conflict.	005	There are rules to say that a suppressed alert will re-appear if TC aid deems to be getting more severe Other ground and airborne safety nets
TC Aid Scenario 002: Conflict resolution with what-else probing. Step 003 – The Executive selects one of the conflicting aircraft and applies the what-else probing. The conflict free flight levels/directs/headings will be shown to the Executive.	Loss	The TC aid does not produce any speculative trajectories for the what-else probe, therefore no conflict free levels/headings etc. will be displayed to the controller. This will create workload for the controller. When W-e-P is not producing any trajectories, it is possible that the whole system does not work with trajectories (depends on the reason of the failure).	003 001	The Executive can use their radar awareness. When W-e-P is not working, W-i-P does also not work! Depending on the reason of the failure it may be that CD is still working properly.
	Delay	The TC Aid Delays in producing speculative trajectories for the what-else probe. This will cause frustration and increased workload for the Executive as their decision making process is being delayed. See above	001	The Executive can use their radar awareness.

	Corruption - undetected	The TC Aid corrupts the speculative trajectories displayed to the controller during a what-else probe. This is not detected by the controller and could mislead the controller into making an unsafe clearance.	001 003	If an unsafe clearance was made then the conflict detection would alert controller to the confliction (depends on the reason of the failure / look above).
	Corruption – detected	The TC Aid corrupts the speculative trajectories displayed to the controller during a what-else probe. This is detected by the controller. They can no longer use the what-else functionality until the issue is resolved, therefore creating increased workload for the controller and increasing their decision making time.	004	If an unsafe clearance was made then the conflict detection would alert controller to the confliction.
Executive Scenario #2: Conflict resolution with what-else probing. Step #3 – The Executive selects one of the conflicting aircraft and applies the what-else probing. The conflict free flight levels/directs/headings will be shown to the Executive.	Misinterpret/misunderstand	The controller misinterprets/misunderstand the speculative what-else trajectories that are displayed during the what-else probe, in the worst case meaning they issue an unsafe clearance , or best case issue an un-expeditious clearance, with no safety impact, but would increase workload	005	If an unsafe clearance was made then the conflict detection would alert controller to the confliction.

SDP Scenario #2, step 4 – the executive selects one solution and cross checks that the chosen solution is conflict free by surveying the situation display as well as the TC-Aid what-else results.	Misinterpret/misunderstand	The controller misinterprets/misunderstand s the information presented when cross checking the solution selected with the information on the situation display. They may issue an unsafe clearance in the worst case scenario, or best case issue an un-expeditious clearance which would increase controller workload.	005	If an unsafe clearance was made then the conflict detection would alert controller to the confliction.
	Loss of information on situation display	There is a loss of information on the situation display, so while the controller is cross checking the what-else solution selected with the radar info, there is some important information missing. Therefore the controller could be misled into making an unsafe decision.	001	If an unsafe clearance was made then the conflict detection would alert controller to the confliction.
	Delay of information on situation displayed.	There is a delay of displaying information on the situation display so while the controller is cross checking the what-else solution selected with the radar info the information is missing at first. Therefore the controller could be misled into making an unsafe decision, if the delay is significant. If the delay is fairly short, then this will cause frustration and increased workload as decision making time is increased.	001	Requirement needed to specify time between solution being selected and corresponding information being displayed on the situation display.

	Corruption – undetected	Same as for scenario #2, step 3	001 003	
	Corruption – detected	Same as for scenario #2, step 3	004	
TC Aid Scenario #3: Detections of Deviations with MONA, Step 1 – MONA detects a deviation and shows a warning to the executive and planner controller indicating the kind of deviation	Loss	MONA detects a deviation but does not display an alert to the controllers. The controllers are unaware that a flight is deviating, potentially leading to a loss of separations. Depends on different things! If it is only the display function of the MONA alerts and all other things are working correctly, the system would calculate with the deviation trajectory and would recognize conflicts.	002	Ground based and airborne safety nets e.g. STCA The controller has less situation awareness than when the system is working perfectly, however the conflict detection function will still be working fine, so the controller still has better information than today. The CD is still working properly.
	Delay	MONA detects a deviation but delays displaying an alert to the controllers. The severity of the hazard depends upon how long the delay is to display the alert. It may be short enough that no hazard occurs, but if it is significant the controller may not be aware of the deviation until it causes a potential loss of separation.	001	Ground based and airborne safety nets e.g. STCA CD is still working correctly and will alert controller.

	Corruption – undetected	The MONA functionality detects deviation but applies the alert to the wrong aircraft, or applies the wrong deviation alert e.g. says a HDG deviation when it is fact cleared level for example.	001 003	Ground based and airborne safety nets e.g. STCA CD is still working correctly and will alert the controller if this situation would lead to a conflict.
	Corruption – detected	The MONA functionality is detecting deviations but corrupting the display of the alerts. This is detected by the controllers. They can no longer rely or use the MONA functionality.	004	Conflict detection still operating correctly.
Executive Scenario #3 step 2 - The Executive and Planner perceive the MONA warning and the Executive checks the validity (correctness) of the warning. Additionally, the Executive also checks that the entered system clearance data are correct.	Misinterpret/misunderstand	The Executive controller checks the validity of the MONA deviation alert and misunderstands the alert. Therefore they believe there to be no deviation by the aircraft and no don't cross check the clearance data. They supress the alert. The deviation continues causing a potentially unsafe situation.	005	If Executive suppress alert and it is still valid, will it still show on planner workstation? It will still be shown at the Planner CWP. Conflict detection and resolution functionality of TC aid still operating correctly.

Scenario #3 step - In case of route, vertical rate or CFL deviation: the Executive contacts the air crew and asks for confirmation of current clearance data or mode S selected parameter	Already covered checking of confirming flight crew clearances in scenario #1 step 4			
FMS **FDP** Scenario #3 step 4 – the aircrew confirms the current clearance and resumes navigation according to the clearance and step 5 – The TC Aid is updated with correct/amended clearance – alert disappears	Loss	The flight crew confirm they are following the clearances as issued by the Executive controller (and matches what the TC aid is showing), but this does not update the MONA alert and it remains. This leads to increased workload and frustration for the Executive and they try and resolve the situation	002	
	Delay	This scenario is the same as loss, if the Executive notices that the alert has not disappeared and attempts to resolve before the alert disappears.	002	There is a requirement needed to specify the time in which alerts take to disappear once resolved.
	Corruption - undetected	The flight crew confirm they are following the clearances that have been issued by the Executive but the data to the TC aid is corrupted. The Deviation alert remains. Increased workload for the controller as they try to resolve the situation.	002	
	Corruption - detected	The flight crew confirm they are following the clearances that have been issued by the Executive but the data to the TC aid is	004	

		corrupted and the MONA alert remains. This is detected by the controllers. Therefore they cannot use the MONA deviation alert functionality. If it is only concerning one ac it is not important.		
Executive Scenario #3 Step 6 – Executive checks that deviation alert has disappeared	Misinterpret/misunderstand	The executive controller misinterprets the disappeared deviation alert – e.g. they think it has disappeared when in fact it has not. Or alternatively they think it still remains when it has disappeared. This will increase confusion and workload for the controller as they try to make sense of the alerts.	005	When such things occurs in several times, controllers cannot work any longer with them. The tool is working improperly and the controllers do not trust this tool.
Executive Scenario #3: Alternative flow #1: MONA is not valid. Step 3 – Executive deletes the warning and monitors the traffic	Misinterpret/misunderstand	Executive controller deletes the MONA alert when it is in fact valid. They are no longer aware of a potentially unsafe scenario evolving.	005	Is alert still on Planner workstation? It will still be shown at the planner CWP. Rules to say that an alert will reappear if increases in severity? There are rules to say that a suppressed alert will reappear if TC Aid deems to get more severe

TC Aid Scenario #3: Alternative flow #1: MONA is not valid. Step 3 – Executive deletes the warning and monitors the traffic	Loss	Executive controller deletes a MONA deviation alert but the alert is not removed. This will cause increased workload and frustration for the Executive controller.	002	
	Delay	Executive controller deletes a MONA deviation but there is a delay in it being removed. This will cause increased workload and frustration for the Executive controller.	002	There is a requirement needed to specify the time in which alerts take to disappear once removed by the Executive.
	Corruption - undetected	Executive controller deletes a MONA deviation but the alert is removed for a valid alert on another aircraft. This means that the controller is unaware of a valid deviation for another aircraft anf is wondering why the alert has not been removed from the original aircraft. This will increase the controllers workload and cause confusion.	002	CD is still working correctly and will alert the controller if this situation would lead to a conflict.
	Corruption – detected	Executive controller deletes a MONA deviation but the alert is removed for a valid alert on another aircraft. The controller detects this corruption. They can no longer use the MONA functionality of the TC Aid	004	Conflict detection and resolution aspects of TC Aid still functioning correctly. CD is still working correctly and will alert the controller if this situation would lead to a conflict.

Table 74 Detailed PSSA Results TC aid

Results for TC aid

Taken from Table 75, each failure mode has a number of repetitive hazards which were identified in the FHA analysis. These hazards are presented in Table 76.

	Resultant Hazards for				
Failure Mode	Loss	Delay	Corruption (undetected)	Corruption (detected)	Misinterpret/Misunderstand
FDPS	Hz 002	Hz 002	Hz 002	Hz 004	
SDPS	Hz 001, 002	Hz 001, 002	Hz 001, 002, 003	Hz 004	
TC aid	Hz 001, 002, 003	Hz 001, 002	Hz 001, 002, 003	Hz 004	
Executive					Hz 005
FMS	Hz 002	Hz 002	Hz 002, 004	Hz 004	
Flight Crew					Hz 005

Table 75 PSSA Analysis - Resultant Hazards for each failure case TC Aid

The number of times each of the hazards associated with the TC aid appeared throughout the FHA analysis was then counted. The hazard *Maximum Tolerable Frequency of Occurrence*[26] was then divided by this number and the tolerable failure rate for each hazard was identified. This is shown in Table 77.

Hazard #	Number of times Hazard has been identified throughout the FHA analysis	Tolerable Failure Rate (Hazard *Maximum Tolerable Frequency of Occurrence*[26]/Number of times throughout the FHA analysis
001	12	3.33E-07
002	15	5.33E-06
003	4	1.00E-04
004	8	1.00E-05
005	8	5.00E-06

Table 76 PSSA Analysis - Hazard Tolerable Failure Rate TC aid

Out of the hazards identified in Table 76, the one with the lowest probability of happening was chosen for each failure case. This will act as the maximum negative safety contribution to be taken into account for defining the corresponding failure case safety requirement. This analysis can be seen in Table 78.

Hazard Rates chosen for the Failure Case Safety Requirements					
Failure	Loss	Delay	Corruption	Corruption	Misinterpret/Misunderstand

[26] Can be found in the *Maximum Tolerable Frequency of Occurrence* column in Table 13 or in the *Final Rate* column in Table 76.

Mode			(undetected)	(detected)	
FDPS	Hz 002 (5.33E-06)	Hz 002 (5.33E-06)	Hz 002 (5.33E-06)	Hz 004 (1.00E-05)	
SDPS	Hz 001 (3.33E-07)	Hz 001(3.33E-07)	Hz 001 (3.33E-07)	Hz 004 (1.00E-05)	
TC aid	Hz 001 (3.33E-07)	Hz 001 (3.33E-07)	Hz 001 (3.33E-07)	Hz 004 (1.00E-05)	
Executive					Hz 005 (5.00E-06)
FMS	Hz 002 (5.33E-06)	Hz 002 (5.33E-06)	Hz 002 (5.33E-06)	Hz 004 (1.00E-05)	
Flight Crew					Hz 005 (5.00E-06)

Table 77 PSSA Analysis - Resultant Hazards Selection for the FCSR TC aid

B.2 System generated hazards – maximum tolerable frequency of occurrence calculations

The full calculus of the *Maximum Tolerable Frequency of Occurrence* for each of the system generated hazards are presented in Table 79, Table 80 and Table 81.

Hazard ID	Description	MAC SC	Tolerability Rate (TR)	Hazard Number (HN)	Impact Modifier (IM)	Final Rate (=TR/HN/IM)
001	Executive controller delaying separation assurance as he/she believes TRACT to be the separating actor.	SC4	10^{-2}	50	1	$2*10^{-4}$
002	Planner controller delaying or failing to assuring separation as he/she believes TRACT to be the separating actor.	SC4	10^{-2}	50	1	$2*10^{-4}$
003	TRACT managing aircraft unnecessarily, resulting in increased workload for the controller.	SC4	10^{-2}	50	1	$2*10^{-4}$
004	TRACT being unable to provide resolutions leading to workload increase for controller.	SC4	10^{-2}	50	1	$2*10^{-4}$
005	Tactical fails to assure separation as he/she believes TRACT to be the separating actor.	SC3	10^{-4}	25	1	$4*10^{-6}$

Table 78 System Generated Hazards maximum tolerable frequency of occurrence calculations – TRACT

Hazard ID	Description	MAC SC	Tolerability Rate (TR)	Hazard Number (HN)	Impact Modifier (IM)	Final Rate (=TR/HN/IM)
001	The tool misleads the controller such that he fails to take appropriate action for a pre-tactical encounter.	SC4	10^{-2}	50	1	$2*10^{-4}$
002	The tool misleads the controller such that he takes unnecessary action for a pre-tactical encounter.	SC4	10^{-2}	50	0.05	$4*10^{-3}$
003	Flights automatically coordinated inappropriately, resulting in an induced tactical or pre-tactical encounter.	SC4	10^{-2}	50	1	$2*10^{-4}$
004	The tool suffers a detected failure resulting in increased workload for the controller, potentially leading to a missed encounter, or unnecessary action.	SC4	10^{-2}	50	0.1	$2*10^{-3}$
005	The tools are working correctly, however the controller may misunderstand/misinterpret the data shown and make a bad planning decision. This therefore increases work load to an unacceptable level, and may increase the risk of causing a safety related incident.	SC4	10^{-2}	50	0.1	$2*10^{-3}$

Table 79 System Generated Hazards maximum tolerable frequency of occurrence calculations - PC aid

Hazard ID	Description	MAC SC	Tolerability Rate (TR)	Hazard Number (HN)	Impact Modifier (IM)	Final Rate (=TR/HN/IM)
001	The tool misleads the controller into missing a tactical conflict.	SC3	10^{-4}	25	1	$2*10^{-4}$
002	The tool presents nuisance alerts to the controller which increase workload, potentially leading to a missed tactical conflict.	SC3	10^{-4}	25	0.05	$4*10^{-3}$
003	The tool presents nuisance resolution proposals leading to a missed tactical conflict.	SC3	10^{-4}	25	0.01	$2*10^{-4}$

004	The tool suffers a detected failure resulting in increased workload for the controller, potentially leading to a missed encounter, or unnecessary action.	SC3	10^{-4}	25	0.05	$2*10^{-3}$
005	The tools are working correctly, however the controller may misunderstand/misinterpret the data shown and make a bad tactical decision. This therefore increases work load to an unacceptable level, and may increase the risk of causing a safety related incident.	SC3	10^{-4}	25	0.1	$2*10^{-3}$

Table 80 System Generated Hazards maximum tolerable frequency of occurrence calculations - TC aid

Appendix C Task 20 – Review Safety Workshop

The main objectives of this two days workshop were to:

- Review and update already exiting safety requirements (changes for clarity or even suppressions/merging);
- Manage unaddressed comments left from outside reviewers;
- Integrate past validation exercises' results in the safety material (through reviewing which of the existing requirements were and which were not validated/verified or through creating new safety requirements if needed).

Attendees at the workshop:

Name	Organisation	Role
[redacted]	NATS	[redacted]
	Think Research (representing NATS)	
	NATS	
	DSNA	
	DSNA	
	DSNA	
	DFS	
	DFS	

C.1 Main Results

C.1.1 Suppressed Requirements

TC Aid		
Requirement	**Action**	**Comment**
REQ-04.07.02-SPR-CDR1.1240 [SR-118]; The TC Aid shall compare the proposed tactical tentative or speculative trajectory of a subject flight against the actual traffic situation at the time of the probe.	Suppressed	Duplication of *REQ-04.07.02-SPR-CDR1.1300 [SR-1114].* The TC Aid shall compare the proposed tactical trajectory of a subject flight against the actual traffic situation when the controller requests a what-if or what-else probe. *Speculative trajectory = What-else probe trajectory* *Tentative trajectory = What-if probe trajectory*
REQ-04.07.02-SPR-CDR1.1310 [SR-1131]; The TC Aid shall provide what-else probing on the request of a controller for a subject aircraft.	Suppressed	Already contained in *REQ-04.07.02-SPR-CDR1.1300 [SR-1114].* The TC Aid shall compare the proposed tactical trajectory of a subject flight against the actual traffic situation when the controller

		requests a what-if or what-else probe.
PC Aid		
Requirement	Action	Comment
REQ-04.07.02-SPR-CDR2.1040 [SR-213]; The PC Aid shall display planning interactions to allow the planner to prioritise actions based on the severity of the interactions.	Suppressed	Part of it contained in *REQ-04.07.02-SPR-CDR2.1020 [SR-212].* The PC Aid shall continuously display any planning encounters that are being monitored within the sector. *Planning encounters = planning interactions* *A new requirement has been created to express to need of the planner to prioritise the displayed encounters. See C.1.2.*
REQ-04.07.02-SPR-CDR2.1290 [SR-2128]; When the Planner interrogates a coordination offer via what-if or what-else probe, the coordination trajectory of that subject flight will be displayed on the radar screen and the trajectories of any environmental flights that form an encounter with the subject flight.	Suppressed	Already contained in *REQ-04.07.02-SPR-CDR2.1300 [SR-2129].* On interrogation of a coordination offer via what-if or what-else probe, the coordination trajectories of the subject flight and any environmental flights that form an encounter with the subject flight shall be displayed within x number of seconds.
REQ-04.07.02-SPR-CDR2.1370 [SR-2139]; The Planner shall be able to point out planning encounters of interest to his executive.	Suppressed	Already contained in *REQ-04.07.02-SPR-CDR2.1380 [SR-2132].* The time between which the planner points out encounters of tactical interest to the tactical workstation display shall be x number of seconds.
TRACT		
Requirement	Action	Comment
REQ-04.07.02-SPR-TRA3.1090 [SR-319]; TRACT shall not attempt to solve a confliction where two aircraft trajectories are head on.	Suppressed	Already contained in *REQ-04.07.02-SPR-TRA3.1100 [SR-3110].* TRACT shall not attempt to solve a confliction where convergences or divergences between a pair of aircraft are of a small angle. *Head-on trajectories are considered to be small angle divergences.*
REQ-04.07.02-SPR-TRA3.1210 [SR-3121]; The flight crew shall have the ability to accept the CTO if they deem it to be acceptable.	Suppressed	Already contained in *REQ-04.07.02-SPR-TRA3.1200 [SR-3120].* The flight crew shall have the ability to accept or reject the CTO.
REQ-04.07.02-SPR-TRA3.1280 [SR-3129]; Any flights that are performing unusual or abnormal manoeuvres (e.g. supersonic flight) shall not be considered as eligible by TRACT.	Suppressed	Questionable. Any aircraft for which the behaviour can be predicted could be managed by TRACT. Remove for the moment and analyse it again in the next iteration.

C.1.2 Additional Requirements

Two additional safety requirements were found during the workshop.

Tool	New Requirement	Rationale	Comments
PC Aid	*REQ-04.07.02-SPR-CDR2.1440; SR-2144* *The planner shall be able to distinguish which of the displayed encounters are pertinent through selective filtering functionality.*	*The controllers will have the possibility to filter their encounters in order to be able to distinguish the ones which are of interest and to avoid misunderstanding of the traffic picture and loss of situational awareness caused by a crowded display.*	This requirement was introduced based on the results gathered from VP-500 and as a result of supressing *REQ-04.07.02-SPR-CDR2.1040 [SR-213];*
TC/PC Aid	*ATCOs shall be able to delete/supress/hide alerts.*	*The TC/PC aid will not negatively impact controller's situational awareness by creating clutter on the situational displays. Therefore the controllers should have means to supress or delete the unwanted/nuisance alerts.*	DFS implemented this feature for TC Aid and it has been agreed this should be captured as a requirement as well.

There were discussions about defining a new safety requirement which would establish the relationship between TC Aid and STCA due to the overlap the two tools would have during operations (in the 0-2 min prior to the conflict time range). However this has not been defined yet because the interactions between the two tools was not tested until now. This will be tested when the TC Aid will be fully developed therefore a requirement defining the relationship between TC Aid and STCA should be considered prior to that.

C.1.3 Changes in existing SPRs

Changes for clarity of the requirements have been made during this workshop as well. These meant rewording of some of the requirements or providing explanations for some of the terms contained in their text (e.g. *Increase in severity = the distance between the two a/c involved in the conflict diminishes faster than usual; one or both the a/c deviate from their trajectories such that the time until the conflict diminishes faster; or any other sudden change in the time/distance until the conflict*).

It is to be noted that the meaning of all the requirements that have clarification changes remained the same therefore these changes did not have any impact on the concept as a whole.

To maintain the neutral impact on the concept, it has been considered that SPRs which are the same or similar with the OSED requirements will not be changed (even if they needed to be) without, in the same time, making the corresponding change in the OSED as well. As a consequence these requirements were left unchanged during this workshop but they will have to be reviewed by concept experts at the next update of the OSED.

Appendix D **Deleted requirements – TC Aid**

The following requirements have been deleted in accordance with the last OSED [4] update. They represent SPR requirements which are similar or the same with the OSED requirements that have been deleted from the OSED.

ID	Requirement
REQ-04.07.02-SPR-CDR1.1020; SR-112	The TC Aid shall produce a Tactical trajectory for a flight when track data and either a cleared flight level or entry flight level is available for a flight.
REQ-04.07.02-SPR-CDR1.1180; SR-1126	The calculated trajectory shall be a Tactical Trajectory if valid flight plan data is available and if no deviation, as detected by Flight Path Monitoring occurred. Otherwise it is referred to as a deviation trajectory.
REQ-04.07.02-SPR-CDR1.1210; SR-1129	The TC Aid shall detect if a deviation no longer exists and remove the display of the alert to the controller.
REQ-04.07.02-SPR-CDR1.1230; SR-117	The TC Aid shall provide what-if probing for the controllers.
REQ-04.07.02-SPR-CDR1.1250; SR-119	When the controllers request a what-if probe for a flight level the TC Aid shall display if the flight level is conflict free or not, and if a vertical rate is necessary to achieve a level.
REQ-04.07.02-SPR-CDR1.1270; SR-1111	The TC Aid shall discard an encounter between a pair of aircraft if vertical or horizontal separation is not infringed anymore.
REQ-04.07.02-SPR-CDR1.1280; SR-1112	If two aircraft are involved with more than one encounter with each other the TC Aid shall only display the first encounter.

Table 81 TC Aid - Deleted Requirements