



SESAR Solution PJ10-02a: SPR-INTEROP/OSED for V3 Part II - Safety Assessment Report (SAR)

Deliverable ID:	[DeliverableID]
Dissemination Level:	[PU/CO/CL]
Project Acronym:	PROSA
Grant:	734143
Call:	H2020-SESAR-2015-2
Topic:	Separation Management En-Route and TMA
Consortium Coordinator:	DFS
Edition Date:	16 September 2019
Edition:	00.01.01
Template Edition:	02.00.01

Founding Members



PROSA

SEPARATION MANAGEMENT EN-ROUTE AND TMA

This SESAR Solution PJ.10-02a SAR is part of a project that has received funding from the SESAR Joint Undertaking under grant agreement No 734143 under European Union's Horizon 2020 research and innovation programme.



Abstract

This document is the SAR for Solution PJ.10-02a.

The SESAR Solution PJ.10-02a is about the provision of Separation in En-route and TMA airspace. It focuses on Conflict Detection and Resolution aids for the Air traffic Controllers, e.g. MTCD, TCT, and also on flight conformance monitoring, e.g. MONA.

Regarding the existing CD/R services, the improvement is namely due to the use of a better Trajectory Prediction thanks to additional input data. Among those new supporting data, the Aircraft Derived Data are of prime importance.

Table of Contents

Abstract	2
1 Executive Summary.....	8
2 Safety specifications at the OSED Level.....	9
2.1 Scope	9
2.2 Solution Operational Environment and Key Properties	9
2.2.1 E.g. Airspace Structure and Boundaries	9
2.2.2 Types of Airspace – ICAO Classification.....	9
The airspace types is “Class C”: Instrument Flight Rules (IFR) and Visual Flight Rules (VFR) flights are permitted, all flights are provided with air traffic control service and IFR flights are separated from other IFR flights and from VFR flights. VFR flights are separated from IFR flights and receive traffic information in respect of other VFR flights.	9
2.2.3 Traffic Levels and complexity	10
2.2.4 Aircraft ATM capabilities	10
2.2.5 CNS Aids	11
2.2.6 Separation Minima	12
2.2.7 Operational services.....	13
3 Introduction.....	14
3.1 Background	14
3.2 General Approach to Safety Assessment	14
3.3 Scope of the Safety Assessment	15
3.4 Airspace Users Requirements.....	16
3.5 Relevant Pre-existing Hazards	16
3.6 Safety Criteria.....	17
3.6.1 Selection of the of AIM Barrier Model	17
3.6.2 Refinement of the Safety Criteria according to the operational services	18
3.6.3 Conflict Detection for the Planner	19
3.6.4 Conflict Detection for the Tactical.....	19
3.6.5 Conflict Resolution for the Planner	19
3.6.6 Conflict Resolution for the Tactical	19
3.6.7 Conformance Monitoring.....	20
3.7 Mitigation of the Pre-existing Risks – Normal Operations	20
3.7.1 Operational Services to Address the Pre-existing Hazards	20
3.7.2 Derivation of Safety Objectives (Functionality & Performance – success approach) for Normal Operations.....	20
3.7.3 Analysis of the Concept for a Typical Flight	26
3.8 Solution Operations under Abnormal Conditions.....	26
3.8.1 Identification of Abnormal Conditions	26
3.8.2 Potential Mitigations of Abnormal Conditions.....	26
3.9 Mitigation of System-generated Risks (failure approach)	29
3.9.1 Identification and Analysis of System-generated Hazards	31
3.9.2 Derivation of Safety Objectives (integrity/reliability)	34

4	<i>Safe Design at SPR Level</i>	38
4.1	Scope	38
4.2	The PJ10.02a Solution SPR-level Model	38
4.2.1	Scope and notations of the SPR level Models	38
4.2.2	SPR-level Model for EXE001 and EXE002	40
4.2.3	SPR-level Model for EXE003	41
4.2.4	SPR-level Model for EXE004 and EXE005	42
4.2.5	SPR-level Model for EXE006	43
4.2.6	SPR-level Model for EXE007	44
4.3	Derivation of Safety Requirements (Functionality and Performance – success approach)	45
4.3.1	Safety Requirements derived from EXE001 (DSNA) and EXE002 (COOPANS).....	45
4.3.2	Safety Requirements derived from EXE003 (ENAV)	45
4.3.3	Safety Requirements derived from EXE004 (Skyguide) and EXE005 (ANS-CR/Eurocontrol).....	47
4.3.4	Safety Requirements for ADS-C EPP data (success approach)	48
4.3.5	Safety Requirements derived from EXE006 (PANSAs, INDRA).....	57
4.3.6	Safety Requirements derived from EXE007 (BULATSA)	59
4.4	Analysis of the SPR-level Model – Normal Operational Conditions	60
4.4.1	Context of the Analysis.....	60
4.4.2	Analysis for EXE001	61
4.5	Analysis of the SPR-level Model – Abnormal Operational Conditions	65
4.6	Design Analysis – Case of Internal System Failures	65
4.6.1	Causal Analysis	65
4.6.2	Common Cause Analysis	66
4.6.3	Safety Requirements (integrity/reliability)	66
5	<i>Detailed Safe Design at Physical Level</i>	74
6	<i>Acronyms and Terminology</i>	75
7	<i>References</i>	80
Appendix A	<i>Safety Objectives</i>	81
A.1	Safety Objectives (Functionality and Performance).....	81
A.2	Safety Objectives (Integrity).....	82
Appendix B	<i>Consolidated List of Safety Requirements</i>	84
B.1	Safety Requirements (Integrity)	86
Appendix C	<i>Assumptions, Safety Issues & Limitations</i>	87
C.1	Assumptions log	87
C.2	Safety Issues log	88
C.3	Operational Limitations log.....	89
Appendix D	<i>Key Additional Information</i>	90

List of Tables

Founding Members





Table 1 Pre-existing hazards for the “Conflict Detection, Resolution and Monitoring” system.....	16
Table 2: ATM and Pre-existing Hazards.....	20
Table 3: PJ10.02a Solution Operational Services & Safety Objectives (success approach)	21
Table 4: List of Safety Objectives (success approach) for Normal Operations – CD aid to PC.....	21
Table 5: List of Safety Objectives (success approach) for Normal Operations – CR aid to PC	22
Table 6: List of Safety Objectives (success approach) for Normal Operations – CD aid to TC.....	23
Table 7: List of Safety Objectives (success approach) for Normal Operations – CR aid to PC	25
Table 8: List of Safety Objectives (success approach) for Normal Operations – Conformance Monitoring aid	26
Table 9: List of Safety Objectives (success approach) for Abnormal Conditions	29
Table 10: System-Generated Hazards and Analysis for CD/R aid to PC	32
Table 11: System-Generated Hazards and Analysis for CD/R aid to TC	33
Table 12: System-Generated Hazards and Analysis for the Trajectory deviation Aid.....	34
Table 13: Risk Classification Scheme for MAC in En-Route & TMA.....	35
Table 14: Maximum Hazard Numbers per Severity Class per Accident Type	36
Table 15: Safety Objectives (integrity/reliability).....	37
Table 16: Safety Objectives (integrity/reliability).....	37
Table 17: Safety Objectives (integrity/reliability).....	37
Table 18: Mapping of Safety Objectives to SPR-level Model Elements	46
Table 19: Derivation of Safety Requirements (functionality and performance) from Safety Objectives	47
Table 20: Mapping of Safety Objectives to SPR-level Model Elements	48
Table 21: Derivation of Safety Requirements (functionality and performance) from Safety Objectives	48
Table 22: Mapping of Safety Objectives to SPR-level Model Elements	58
Table 23: Derivation of Safety Requirements (functionality and performance) from Safety Objectives	58
Table 24: Assumptions made in deriving the above Safety Requirements.....	58
Table 25: Mapping of Safety Objectives to SPR-level Model Elements	59



Table 26: Derivation of Safety Requirements (functionality and performance) from Safety Objectives 60

Table 27: Operational Scenarios for EXE001 – Normal Conditions..... 64

Table 28: Additional Safety Requirement from Scenarios for Normal Operations for EXE001 65

Table 29: Acronyms and terminology 79

Table 30: Assumptions log 88

Table 31: Safety Issues log..... 89

Table 32: Operational Limitations log 89

List of Figures

Figure 1..... 18

Figure 2: SPR level Model for EXE001 and EXE002 40

Figure 3: SPR level Model for EXE003 41

Figure 4: SPR level Model for EXE004 and EXE005 42

Figure 5: SPR level Model for EXE006 43

Figure 6: SPR level Model for EXE007 44

Figure 7..... 51

Figure 8..... 52

Figure 9..... 53

Figure 10..... 55

Figure 11..... 56

Figure 12..... 60

Figure 13..... 61

Figure 14..... 62

Figure 15..... 62

Figure 16..... 63

Figure 17..... 64

Figure 18..... 69





Figure 19..... 70

Figure 20..... 71



1 Executive Summary

This document contains the Specimen Safety Assessment for a typical application of the PJ10.02a Solution in Improved Performance in the Provision of Separation operations. The report presents the assurance that the Safety Requirements for the V1-V3 phases are complete, correct and realistic, thereby providing all material to adequately inform the PJ10.02a Solution OSED/SPR/INTEROP.

It has to be noted that the EPP related exercises (Exercises 6 and 7) target V2 maturity. So this SAR will be completed in a future V3.

It impacts the following Operational Improvement steps:

- CM-0206 “Conflict Detection and Resolution in the TMA using trajectory data”
- CM-0208A “Automated Ground Based Flight Conformance Monitoring in the TMA ”
- CM-0209 “Conflict Detection and Resolution in En-Route using enhanced ground predicted trajectory in Predefined and User Preferred Routes environments”
- CM-0209b “Conflict Detection and Resolution in En-Route using aircraft data in Predefined and User Preferred Routes environments”
- CM-0210 “Ground Based Flight Conformance Monitoring in En-Route using enhanced ground predicted trajectory”
- CM-0210b “Ground Based Flight Conformance Monitoring in En-Route using aircraft Data”
- CM-0211 “Advanced Support for Conflict Detection and Resolution for ATC planning in En Route”

The aim of the PJ10.02a safety assurance activities is to ensure that the PJ10.02a is adequately specified from a safety perspective, thereby providing a complete, correct and consistent set of safety requirements for the V1-V3 phases to adequately inform the PJ10.02a Solution OSED/SPR/INTEROP.

This SAR is mainly aimed at reporting the Safety Assurance activities outputs undertaken by the PJ10.02a.

Six Safety Criteria have been identified being applicable for both TMA and En-route airspace. It is expected to reduce several potential safety mitigating events like “ATC induced conflicts” by the improved separation management supporting tools/functionalities which are under scope of this Solution.

2 Safety specifications at the OSED Level

2.1 Scope

This section addresses the following activities:

- Description of the key properties of the Operational Environment that are relevant to the safety assessment – sections 2.2
- Identification of the pre-existing hazards that affect traffic in approach/ landing and guided take-off operations in the relevant operational environment (airspace) and the risks of which operational services provided by the ATS System may reasonably be expected to mitigate to some degree and extent – section 0
- Setting of the Safety Criteria – section 3.6
- Comprehensive determination of the operational services that are provided by the OFA to address the relevant pre-existing hazards and derivation of Safety Objectives (success approach) in order to mitigate the pre-existing risks under normal operational conditions – section 3.7.
- Assessment of the adequacy of the operational services provided by the OFA in the case of internal failures and mitigation of the system-generated hazards (derivation of Safety Objectives (failure approach)) – section 3.9.13.9.

2.2 Solution Operational Environment and Key Properties

The detailed operational environment is described in the §3.2 of the OSED (Ref [11]).

2.2.1 E.g. Airspace Structure and Boundaries

The airspace considered by the current document is a managed airspace, where a separation service is provided by ATM services providers.

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

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

A further phase of the SESAR Solution PJ.10-02a will need to take into account more dynamic airspace structure, based on moving areas and flight centric concepts, as studied by SESAR Solutions PJ.08-02 and PJ.10-01b.

2.2.2 Types of Airspace – ICAO Classification

The airspace types is “Class C”: Instrument Flight Rules (IFR) and Visual Flight Rules (VFR) flights are permitted, all flights are provided with air traffic control service and IFR flights are separated from

other IFR flights and from VFR flights. VFR flights are separated from IFR flights and receive traffic information in respect of other VFR flights.

2.2.3 Traffic Levels and complexity

The vertical scope considered by SESAR Solution PJ.10-02a extends from FLO to FL660 wherever traffic is controlled except airspace dedicated to final approach and aerodrome vicinity.

The airspace is RVSM up to FL410.

2.2.4 Aircraft ATM capabilities

The aircraft capabilities will remain heterogeneous in the target environment.

As a minimum they will comply with existing capabilities and standards as described in the Minimum Aviation System Performance Specification (MASPS) [42].

It is assumed that the highest level of aircraft capabilities available in the scope of the current document can be summarized as follows:

- **Data link:**
 - CPDLC and ADS-C for ATC via ACARS (oceanic flights) and via ATN (continental flight) ED 110B/120 for continental ATN B1, and ED 228A[50]/229A[51] for continental Europe ATN B2);
 - FIS: ATIS with ATC via ACARS;
 - MET data (winds/temperatures, TEMSI, etc.) with 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 [42] 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 VSO with wing-flaps extended and 1.8 VS1 with wing-flaps retracted. However, the error need not be less than ± 30 ft”;
- **Surveillance:**
 - ADS-B in/out via Mode-S 1090 transponder and ATSAW applications;
 - TAWS;
 - ACAS for the safety net.

The focus here is mainly on Commercial aircraft (legacy, low fare, regional) and on Business aircraft¹.

There is generally less capability for GA-VLJ-Helicopter and Military aircraft however they have at least minimum equipage for airspace class they use.

It may be noticed that, despite ADS-C EPP is mentioned here, the use of this data is not part of the V3 validation exercises and therefore ADS-C EPP data does not appear in the current Solution V3 requirements. Only Mode-S capabilities support the PJ.10-02a solution at V3 level.

2.2.5 CNS Aids

We reproduce here the main features explained in the OSED ([11]). The highest level of aircraft capabilities available in the scope of the current document can be summarized as follows:

- **Data link:**
 - CPDLC and ADS-C for ATC via ACARS (oceanic flights) and via ATN (continental flight) ED 110B/120 for continental ATN B1, and ED 228A[50]/229A[51] for continental Europe ATN B2);
 - FIS: ATIS with ATC via ACARS;
 - MET data (winds/temperatures, TEMSI, etc.) with 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);
 - RVSM performance.
- **Surveillance:**
 - ADS-B in/out via Mode-S 1090 transponder and ATSAW applications;
 - TAWS;
 - ACAS for the safety net.

It may be noticed that, despite ADS-C EPP is mentioned here, the use of this data is not part of the V3 validation exercises and therefore ADS-C EPP data does not appear in the current Solution V3 requirements. Only Mode-S capabilities support the PJ.10-02a solution at V3 level.

¹ Mainline and BGA equipage level can be very different

2.2.5.1 Air-Ground Communication

A great deal of work related to Air-Ground Communications is achieved within the WG78 and WG85 for EUROCAE and SC214 for RTCA which are conjointly in charge of the standards for advanced ATS supported by data communication.

The operational needs expressed by SESAR, NEXTGEN and ICAO OPLINK panel have been considered, in particular the following new air-ground data exchanges required to support initial 4D operations:

- **CPDLC** message as voice alternative if not time critical;
- **ADS-C** Extended Projected Profile (ADS-C EPP) to support the automatic downlink of trajectory data (1 to 128 published and/or computed waypoints with associated constraints and/or estimates in the 4 dimensions, etc.). ADS-C EPP data are needed to get the predicted aircraft's behaviour from aircraft's point of view, which enable the enhancement of separation services. ADS-C data are downlinked according to the contract that is negotiated between Ground and Air parties. Three types of contract exist for ADS-C EPP report: "on event, on demand & periodic". The "on event" form of contract is used to allow the on-board predicted trajectory to be downlinked when it has changed by a specified threshold from the previously downlinked version;
- **Mode-S** Enhanced Surveillance (EHS) permits to receive downlinked airborne parameters (DAPs) into the ground surveillance system. EHS is mandated in Europe for most airline aircraft. Local wind speed and direction for instance, may be very valuable data that EHS can provide.

2.2.6 Separation Minima

Separation minima are expected to continue to be based on guidance, regulations, and factors used in today's environment (ICAO Doc 4444 Procedures for Air Traffic Management [39], especially Chapter 5):

- Vertical separation: FL< 410 → 1000ft separation (RVSM);
- Horizontal separation: different separation minima apply in different airspace, depending on the kind of airspace (very often it is 5NM in En-Route airspace and 3NM in TMA airspace) and on the airspace itself (e.g. in Warsaw FIR, the separation minima are currently 7NM in En-Route and 5NM or 3NM in TMA)

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

- A non-RVSM flight that is authorized to fly within an RVSM airspace remains subject to separation standard that is applicable above the RVSM limit (i.e. in a non-RVSM airspace);
- At the edges of multi-sensor cover or in the case of a reduction in surveillance sensor service where the separation minimum may be increased up to 10 NM;
- The sectors that interface the lower En-Route sectors may be operating a lower separation standard (procedures ensure that the separation is established prior to transfer of control in this case).

Therefore the choice of separation standard is made on a case-by-case basis depending on both the pair of elements to assess and the airspace where the separation is assessed, and it may not be homogeneous throughout the whole controlled sector. Conflicting aircraft may be in airspace volumes with different separation minima.



2.2.7 Operational services

PJ10.02A deals with the Separation Assurance operational service, both at the planner level (Planning separation assurance) and at the tactical level (Tactical separation assurance)

3 Introduction

3.1 Background

When performing separation assurance, both the Planner Controller and the Tactical controller are assisted by tools (called ATC tools), which provide support in the identification and in the resolution of conflicts.

PJ10.02A does not introduce any new ATC tool, it addresses the improvement of some tools, with the help of additional data sources (ADS-C EPP data, Mode S surveillance data) aiming at increasing the performance of these tools.

As a consequence, the expected benefits lie in a reduction of some tools shortcomings, such as (for instance):

- False alarms, or nuisance alarm;
- Late detection (in the case of a trajectory deviation).

As a general rule, safety activities are expected to scope the change brought into the system, and not to redo a safety assessment of the overall system. Here, the change is more of a technical than of an operational nature.

3.2 General Approach to Safety Assessment

This safety assessment has been conducted in accordance with the SESAR Safety Reference Material ([1]) and associated Guidance ([2]). The SRM is based on a twofold approach:

- a new *success approach* which is concerned with the safety of Improved Performance in the Provision of Separation operations in the absence of failure; and
- a conventional *failure approach* which is concerned with the safety of Improved Performance in the Provision of Separation operations in the event of failure within the end-to-end System.

These two approaches are applied to the derivation of safety properties at each stage of the development of Improved Performance in the Provision of Separation operations, as follows:

Safety specification at the OSED Level

This is defined as what Improved Performance in the Provision of Separation operations has to achieve at the ATM operational level in order that the requirements of the airspace users are satisfied.

The users' requirements are expressed in the form of Safety Criteria (see section 3.6 below) and the Specification is expressed in the form of Safety Objectives (functionality & performance and integrity/reliability properties).

The safety specification at OSED level comprises the determination of:

- Safety Criteria (SAC) which are described in section 3.6 of this report
- Safety objectives (to satisfy Safety Criteria) which are defined at that stage and include:
 - Safety Objectives (functionality and performance) described in section 3.7.2;

- Safety Objectives (Integrity/reliability) relative to failure aspects described in section 3.9.2.

Safe Design at the SPR Level

This phase assesses whether the proposed design of Improved Performance in the Provision of Separation operations is able to achieve the level of safety required. Its purpose is to derive Safety Requirements (sub-divided into functionality & performance and integrity/reliability properties) in order to comply with the Safety Objectives that were derived during the safety specification at the OSED level

The Safe design at SPR level includes:

- Functional Models for each exercises are defined and described in section 4.2.
- Safety Requirements (to satisfy Safety Objectives) are defined at that stage, subdivided into:
 - Safety Requirements relative to the success case described in section 4.3
 - Safety Requirements relative to failure aspects described in section **Error! Reference source not found.**4.6.

3.3 Scope of the Safety Assessment

The safety assurance activities to be carried out during this safety assessment are specified in the Safety Plan [3]. In the remaining of this subsection we detail the scope of the safety requirements, which depends on the nature of the operational improvement. Within PJ10.02a several different operational environments (OE) coexist in the different exercises, with specific operational improvements. Whenever OE and exercises where of a similar nature, the resulting safety assessments have also been merged.

The SESAR Solution PJ.10-02a proposes to improve the functions of the separation services as follows:

- The **“CD aid to the PC”** enhancement consists in focusing on the most probable conflicts, during the sector planning timeframe (usual magnitude between 20 and 30 minutes), while conflicts that have lower probabilities of persisting are more discreetly displayed. This offers the opportunity for a new task sharing between the TC and the PC. The PC can now decide to solve high-probability encounters in advance by negotiating entry/exit coordination conditions or by taking in charge some conflict resolutions by up-linking CPDLC clearances to conflicting aircraft if operational procedures support it;
- The **“CD aid to the TC”** in En-Route has been V3-validated in SESAR1 through Solution#27. It thus looks the most relevant to stabilize its functions, and to increase both its scope and its accuracy. It takes advantage of the use of improved ground trajectory prediction, and its application scope may now include environments where almost all flights are climbing/descending i.e. in TMA
- The **Conflict Resolution** aids (What-If and What-Else) based on tactical trajectory in En-Route have been V3-validated in SESAR1 through Solution#27. To increase scope and functionalities, they now take advantage of the use of improved prediction data, particularly in lower airspace where new probe services based e.g. on climb/descent rates, may be proposed. In a mix traffic where equipped and non-equipped aircraft share the same ATC volume, the Conflict

Resolution aids may implement an optimised conflict resolution system considering flight efficiency and providing best service for flights contributing the most to predictability and conformance monitoring.

- **Conformance monitoring** service based on tactical trajectory in En-Route has been V3-validated in SESAR1 through Solution#27. Based on improved ground trajectory prediction, it can raise additional alerts thanks namely to aircraft intentions (e.g. ToD, ToC, etc.) that can be downlinked by the aircraft. The MONA shall consider relevance and quality of available data depending on the situation (e.g. open loop clearance).

We now explain the dependency between the scope of the assessment and the improvement of the above functions. Basically, for each function, two cases may arise:

- 1) If the improvement consists of enhancing some function of the separation services (such as the monitoring) by providing extra data which will improve its performance, then the change is purely technical (ATC working methods should not change significantly, only the training may be adapted in order to teach controllers how the tool has been improved, and the possible new failures);
- 2) If the improvement consists of modifying only the Trajectory Prediction, the CD /R Aid will be unchanged for a technical viewpoint, so the change will be limited to the impact, on the function, of the trajectory prediction change.

Depending on the two cases above, the scope of the safety requirements will be different. If we are in 1), technical safety requirements will only apply to the part of the function impacted by the technical change. If we are in 2), then we assume that for engineering reasons the function should not be modified, it is rather the trajectory prediction which will have to comply with the change. In other words, the technical safety requirements will be for the trajectory prediction, and not for the function.

3.4 Airspace Users Requirements

No specific requirements from Airspace Users have been considered in this document.

3.5 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.

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 unauthorized areas
Hp#4	Aircraft encounters with severe weather conditions
Hp#5	Aircraft encounters with wake vortices

Table 1 Pre-existing hazards for the “Conflict Detection, Resolution and Monitoring” system

Hp#1: P10.02a 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 trajectory adjustments made by PJ10.02a are limited to and so should have no impact on the likelihood of a controlled flight into terrain (i.e. CFIT) or obstacle.

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 due to the changes in trajectory. However, these timing differences will be so small that they can be considered to have a negligible impact.

Hp#4: The conflict resolution adjustments should 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 conflict resolution adjustments should not have any impact on the likelihood of aircraft encounters with wake vortices.

Only the following aviation pre-existing hazard is of relevance for the operational change addressed by PJ10.02a:

- Hp#1. Conflicts between pairs of trajectories / clusters

No specific impact on Controlled Flight Into Terrain, Wake Vortex Encounters, Taxiway Incursions, Runway Incursions.

3.6 Safety Criteria

The Safety Criteria (SAC) have been determined in [8], and we reproduce them here. We recall that PJ10.02a is a continuation of former SESAR1 WP 4.7.2 and WP 05.07.2, so in order to be consistent with the safety work done in SESAR1 we have chosen a version of the Accident Incident Model (AIM) which is applicable both [8] and for WP 4.7.2 and 5.7.2. The AIM that we have retained ([9]) includes ATC induced pre-tactical conflicts, a category which has been removed in the most recent versions.

3.6.1 Selection of the of AIM Barrier Model

The SESAR SRM uses a number of accident incident models (AIM) to describe the ATM processes which can result in an accident or incident. These models are based on a barrier model representation of ATM. The nature of the pre-existing hazards (only HP#1 applies to PJ10.02a) orients the choice of the model towards the MAC ER (mid-air collision for en-route), illustrated below.

Barrier Model of Mid-Air Collision

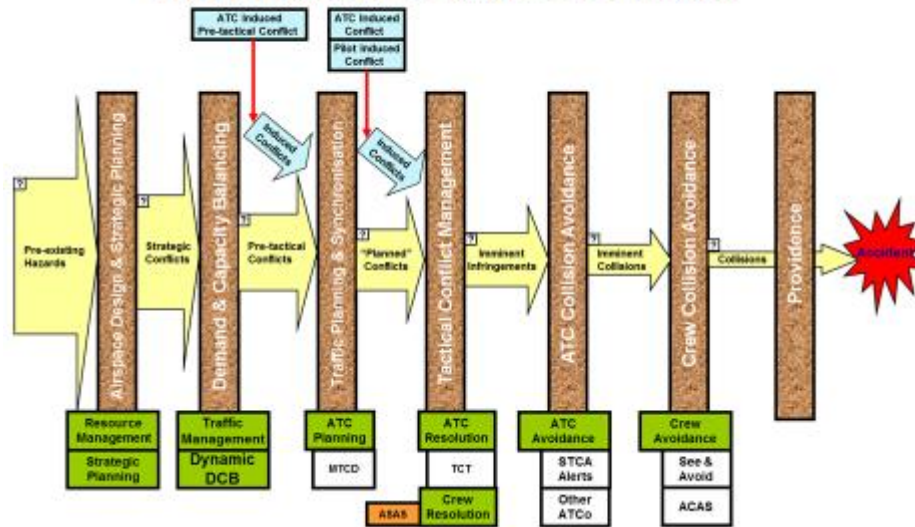


Figure 1

3.6.2 Refinement of the Safety Criteria according to the operational services

The Safety Criteria (SAC) correspond to high level safety objectives, expressed at the level of the barriers of the model illustrated in Figure 1. As explained in section 3.3, PJ10.02a implements different operational improvements, within different operational environments. This is why we decided to refine the SAC according to a taxonomy of operational services impacted by PJ10.02a. The word “operational” refers to the fact that our operational services aggregate the human and the technical together, without specifying any further. The operational services that we have distinguished are the following:

- ▶ Conflict Detection for the Planner;
- ▶ Conflict Detection for the Tactical;
- ▶ Conflict Resolution for the Planner;
- ▶ Conflict Resolution for the Tactical;
- ▶ Monitoring of trajectories.

The five operational services listed above are more detailed than the ones listed in the V2 SAR ([8]), where the Conflict Detection and Conflict Resolution were not distinguished, leading to only two operational services:

1. Conflict Detection & Resolution (CD/R) for Planner Controller (PC)
2. Conflict Detection & Resolution (CD/R) for Tactical Controller (TC)

In ([8]) the Monitoring of trajectories was part of the CD/R aid for the TC.

We have chosen to consider the conflict detection and the conflict resolution as different operational sub services, in order to clarify the determination of the Safety Criteria (SAC) below. As we will see,

the events of the Accident Incident Model are differently impacted whether we address the conflict detection, the conflict resolution or the detection of trajectory deviations.

3.6.3 Conflict Detection for the Planner

Traffic Planning & Synchronisation Barrier

An improvement of the conflict detection by the planner is expected to reduce the failure frequency of event MB10.1.1.2.1.1 - "Failure to identify conflict".

In addition, if the conflict detection is improved by the use of additional data, this is expected to reduce the failure frequency of event MB10.1.1.1 - "Inadequate Planning Info".

3.6.4 Conflict Detection for the Tactical

Tactical Conflict Management Barrier

An improvement of the conflict detection by the tactical is expected to reduce the failure frequency of event MB 5.1.2.3 - "Failed to detect conflict" and MB 5.1.3.1 - "ATCo misjudgement of separation".

In addition, if the conflict detection is improved by the use of additional data, this is expected to reduce the failure frequency of event MB 5.1.1 - "Inadequate information for conflict management".

3.6.5 Conflict Resolution for the Planner

Traffic Planning & Synchronisation Barrier

The improvement of the conflict resolution for the planner is expected to improve the efficiency of planning resolution, and consequently to result in a reduction in the number of planned conflicts.

ATC Induced Pre-Tactical Conflict

The improvement of the conflict resolution for the planner will also reduce the likelihood of planner controller 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 MF 9.1.2 - "Conflict resolution leads to knock-on PreTactical conflict " and MF 9.1.3 - "Traffic Management Instruction creates PreTactical conflict".

In addition, if the conflict detection is improved by the use of additional data, this is expected to reduce the failure frequency of event MB10.1.1.1 - "Inadequate Planning Info".

3.6.6 Conflict Resolution for the Tactical

Tactical Conflict Management Barrier

The improvement of the conflict resolution for the tactical is expected to reduce the failure frequency of event MB5.1.3 - "Inadequate "ATCo conflict management" (i.e. the controller issues fewer and better conflict resolution instructions)

In addition, if the conflict detection is improved by the use of additional data, this is expected to reduce the failure frequency of event MB 5.1.1 - "Inadequate information for conflict management".

ATC Induced Tactical Conflict

The implementation of the enhanced conflict detection, resolution and monitoring was expected to provide substantial safety benefits and reduce the workload of the tactical controller and the opportunity for controller error. It was expected that the number of induced conflicts would be reduced.

The improvement of the conflict resolution for the tactical will reduce the likelihood of induced conflicts since they provide the controller with a view of all the predictable knock-on conflicts. Within the AIM model it is expected that occurrences of events MF7.1.1 – “Conflict resolution leads to knock on conflict” and MF7.1.2– “Traffic management Instruction creates Tactical conflict” will be reduced.

3.6.7 Conformance Monitoring

Crew/Aircraft Induced Tactical Conflict

The improvement of the conformance monitoring will result in an enhanced detection of trajectory deviations by the crew or by the aircraft, which will allow to reduce the frequency of crew/Aircraft induced tactical conflicts MF6.1.2 - "Conflict due to Crew/ac Deviation".

3.7 Mitigation of the Pre-existing Risks – Normal Operations

3.7.1 Operational Services to Address the Pre-existing Hazards

From the EATMA classification, the operational service addressed by Solution PJ10.02a is:

ID	Service Objective	Pre-existing Hazards [Hp xx]
ATM/1	Provide Separation Assurance: Planning and Tactical Separation	Hp#1 Conflicts between pairs of trajectories / clusters

Table 2: ATM and Pre-existing Hazards

3.7.2 Derivation of Safety Objectives (Functionality & Performance – success approach) for Normal Operations

The safety benefits identified in §3.6 result from improvements of the five operational services listed from §3.6.3 till §3.6.7. These five improvements correspond to technical tools which provide support to the associated services. These five improvements are the one listed in Table 3, they are referred similarly to §3.6, but we have added the word “aid” at the end of each one in order to clarify that we address an improvement, and not the function itself.

Ref	Phase of Flight / Operational Service	Related AIM Barrier	Achieved by / Safety Objective [SO xx]
	Planning conflict detection aid	Traffic planning & Synchronisation Barrier	SO#021, SO#201, SO#211

	Planning conflict resolution aid	Traffic planning & Synchronisation Barrier	SO#022, SO#023, SO#029, SO#201, SO#211, SO#212
	Tactical conflict detection aid	Tactical Conflict Management	SO#011, SO#014, SO#016
	Tactical conflict resolution aid	Tactical Conflict Management	SO#013, SO#014, SO#015, SO#016
	Conformance monitoring aid	Tactical Conflict Management	SO#012, SO#016, SO#024, SO#027,

Table 3: PJ10.02a Solution Operational Services & Safety Objectives (success approach)

We now list the Safety objectives for the Success Case for each of the five aids listed in Table 3.

3.7.2.1 Safety objectives for the Planning conflict detection aid

ID	Description	Rationale
SO#021	The Planning conflict detection 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.
SO#201	Planning conflict detection aid calculations should permit to display an encounter even if one aircraft is outside the sector (AOI crossing)	This safety objective is derived from PJ06 requirements, expressing a need for such a possibility, especially in Free-Route environment.
SO#211	The Planning conflict detection aid tool shall be active at all CWP's at all times.	Correct assumption, but needs to be validated.

Table 4: List of Safety Objectives (success approach) for Normal Operations – CD aid to PC

3.7.2.2 Safety objectives for the Planning conflict resolution aid

ID	Description	Rationale
----	-------------	-----------

SO#022	The Planning conflict resolution 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.
SO#023	The Planning conflict resolution 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
SO#029	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 MF7.1.2.3.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
SO#201	Planning conflict resolution aid calculations should permit to display an encounter even if one aircraft is outside the sector (AOI crossing)	This safety objective is derived from PJ06 requirements, expressing a need for such a possibility, especially in Free-Route environment.
SO#211	The Planning conflict resolution aid tool shall be active at all CWPs at all times.	Correct assumption, but needs to be validated.
SO#212	The Planning conflict resolution 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.

Table 5: List of Safety Objectives (success approach) for Normal Operations – CR aid to PC

3.7.2.3 Safety objectives for the Tactical conflict detection aid

ID	Description	Rationale
SO#011	The Tactical conflict detection 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.	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 Tactical conflict detection aid detects all relevant interactions within the sector therefore reducing the risk of the Tactical failing to detect conflicts. It also relates to MBX1.1.1 Inadequate traffic picture as the Tactical conflict detection 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
SO#014	TC Aid shall support the TC to correctly prioritise and resolve conflicts indicated to the ATCO by TC aid in a timely way.	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 conflicts and will indicate the severity/geometry of those interactions, therefore indicating the highest priority of tasks
SO#016	The Tactical conflict detection aid tool shall be active at all CWP's at all times.	This is a correct assumption, but will need to be validated during the simulation

Table 6: List of Safety Objectives (success approach) for Normal Operations – CD aid to TC

3.7.2.4 Safety objectives for the Tactical conflict resolution aid

ID	Description	Rationale
----	-------------	-----------

SO#013	For the subject aircraft the Tactical conflict resolution aid shall identify conflicts for any probed clearances.	This safety objective relates to the AIM Barrier MB5.1.3.1 ATCO misjudgement of separation due to the fact that the Tactical conflict resolution aid would automatically identify conflicts which still exist after an inadequate resolution is applied. It also relates to MB51.1.1 Inadequate traffic picture due to the fact that the Tactical conflict resolution 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 Tactical conflict resolution aid, via the what if probing would identify a new conflict created by the proposed resolution
SO#014	The Tactical conflict resolution aid shall support the Tactical Controller to correctly prioritise and resolve conflicts indicated to the ATCO by TC aid in a timely way.	This safety objective relates to the AIM Barrier MB5.1.3.2 ATCO failure to act. The Tactical conflict resolution aid shall display to the controller all conflictions and will indicate the severity/geometry of those interactions, therefore indicating the highest priority of tasks
SO#015	The Tactical conflict resolution 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 Tactical conflict resolution 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 Tactical conflict resolution 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
SO#016	The Tactical conflict resolution aid tool shall be active at all CWP's at all times.	This is a correct assumption, but will need to be validated during the simulation

Table 7: List of Safety Objectives (success approach) for Normal Operations – CR aid to PC

3.7.2.5 Safety objectives for the Conformance monitoring aid

ID	Description	Rationale
SO#012	The Conformance monitoring 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)	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
SO#016	The Conformance monitoring aid tool shall be active at all CWP's at all times.	This is a correct assumption, but will need to be validated during the simulation
SO#024	The Conformance monitoring 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.
SO#027	The Conformance monitoring 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

		<p>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.</p>
--	--	---

Table 8: List of Safety Objectives (success approach) for Normal Operations – Conformance Monitoring aid

3.7.3 Analysis of the Concept for a Typical Flight

PJ10.02A does not bring about a new concept, since it is limited to enhancing the performance of some ATC tools by providing additional data. Therefore we have not developed this section.

3.8 Solution Operations under Abnormal Conditions

The purpose of this section is to assess the ability of the PJ.10-02a solution to work through (robustness), or at least recover from (resilience) any abnormal conditions, external to the System, that might be encountered relatively infrequently

3.8.1 Identification of Abnormal Conditions

The following list of abnormal conditions has been identified as relevant for PJ.10-02a solution by operational experts:

- ABN-01: Bad weather (CBs, turbulences, icing)
- ABN-02: Severe ATC technical system failure - Total loss of surveillance system
- ABN-03: Severe ATC technical system failure - Total loss of air/ground communication system
- ABN-04: Severe ATC technical system failure - Total loss of FDPS
- ABN-05: Severe ATFCM technical system failure - Total loss of local DCB tool
- ABN_06: Aircraft in emergency
- ABN_07: Severe aircraft technical system failure - Radio communication failure
- ABN_08: Severe aircraft technical system failure - Loss RVSM capability
- ABN-09: Severe aircraft technical system failure - Transponder failure

3.8.2 Potential Mitigations of Abnormal Conditions

Ref	Abnormal Conditions	Operational Effect	Mitigation of Effects / [SO xx]
ABN-01	Bad weather (CBs, turbulences, icing)	<p><u>Effects in planning phase</u></p> <p>In case of bad weather, some DCB measure might be implemented in planning phase, for instance reduction of the capacity (<i>existing mitigation means</i>).</p> <p><u>Effects in execution phase</u></p> <p>Case of CBs: Aircraft will possibly avoid the area with lateral deviation. Flight crew asks the ATCO before deviation. It will be a problem for MTCD encounters, relying on planning TPs, which are useless in such a situation. Aircraft in deviation won't fly anymore accordingly to their planning TPs.</p>	<p>MTCD has to be switched off if needed (cf SR-2142), or at least has to clearly identify aircraft in deviation so that ATCOs are aware of the discrepancy between system known data and aircraft real trajectories. Moreover, ATCOs could rely on other tools, like TCT for instance which is still fully operative even in adverse weather conditions. (cf SR-1115)</p>
ABN-02	Severe ATC technical system failure - Total loss of surveillance system	<p>In case of failure of the surveillance system:</p> <ul style="list-style-type: none"> - tracks are no more displayed to the ATCO (a symbol indicates the last position received for each aircraft), - radar separation (5NM) cannot be applied anymore - TCT and STCA are in degraded mode - Display of the planned trajectory is still possible - MTCD (based on flight plan trajectory) is still working <p>At the moment of the failure, the only fall back consists in using 500ft vertical separation to manage the critical situation (<i>existing mitigation means</i>, not specific to solution PJ.10-02a).</p> <p>Increase of the workload of the ATCO to manage the aircraft of the sector without surveillance display. Possible loss of separation between aircraft.</p> <p>When the short term situation has been managed, control services are provided in degraded mode:</p> <ul style="list-style-type: none"> - ATCO can no more apply radar separation and have to go back to procedural separation (<i>existing mitigation means</i>) based on flight plan information, pilot reports and display of the trajectory - capacity thresholds are reduced. 	<p>Use of 500 ft vertical separation (<i>existing mitigation means</i>)</p> <p>Procedural control (<i>existing mitigation means</i>)</p>


Ref	Abnormal Conditions	Operational Effect	Mitigation of Effects / [SO xx]
ABN-03	Severe ATC technical system failure - Total loss of air/ground communication system	<p>In case of loss of radio, CPDLC can be used as a backup If CPDLC is not available, then:</p> <ul style="list-style-type: none"> - In the absence of ground instruction, aircraft will continue on their flight plan - ATCO will contact adjacent centre to ask them to relay the messages to the aircraft (<i>existing mitigation means</i>) - Capacity of the sector/ATSU is reduced. 	No specific safety objective for this abnormal condition
ABN-04	Severe ATC technical system failure - Total loss of FDPS	<p><i>Remark: Assessment of this hazard on a general basis appears to be very difficult considering that operational effects depend upon the local architecture of the ATC system.</i></p> <p>In case of failure of FDPS, all trajectory derived information are impacted. Depending on local implementation, impacts could be:</p> <ul style="list-style-type: none"> - No more flight strip, - Impossible to display the planned trajectory of the aircraft on the HMI - Detection tool based on flight plan information (MTCD and TCT) are unavailable or degraded - Degradation / loss or automatic coordination functions - Surveillance information should be displayed as long as possible - Radar tracks are not correlated anymore <p>Mitigation means shall be defined depending upon local architecture for the management of the short term degraded situation.</p> <p>When the short term situation has been managed, control services are provided in degraded mode:</p> <ul style="list-style-type: none"> - capacity thresholds are reduced. 	No specific safety objective for this abnormal condition
ABN-05	Severe ATFCM technical system failure - Total loss of local DCB tool	<p>In case of loss of local DCB tool, FMP is not able to perform the local demand and capacity balancing activities in nominal conditions. FMP can ask NM to put regulations (<i>existing mitigation means</i>).</p>	No specific safety objective for this abnormal condition

Ref	Abnormal Conditions	Operational Effect	Mitigation of Effects / [SO xx]
ABN-06	Aircraft in emergency	In case of emergency situation (such as loss of pressurization or loss of engine), the flight crew will apply the appropriate emergency procedure.	No specific safety objective for this abnormal condition
ABN-07	Severe aircraft technical system failure - Radio communication failure	In the absence of ground instruction, flight crew will follow the flight plan until the IAF. The ATCO will be in charge of providing separation via appropriate clearances relayed to surrounding aircraft. If the aircraft is being radar vectored: the standard procedure that might depend on the ICAO regional regulation has to be applied.	No specific safety objective for this abnormal condition
ABN-08	Severe aircraft technical system failure - Loss RVSM capability	In case of a loss of RVSM capability for a given aircraft, the following actions have to be performed: - Pilot announce the loss of RVSM capability to the ATCO - RVSM flight level cannot be used anymore	No specific safety objective for this abnormal condition
ABN-09	Severe aircraft technical system failure - Transponder failure	Impact on ground: Loss of the flight track on the CWP (En Route CWP are only based on secondary radar). If possible allocate a specific FL to this aircraft, with a fine update of longitudinal evolution via regular radio reports, and provide non-radar separation between this aircraft and the other ones.	Ask for regular frequency reports on this aircraft and ensure non-radar separation minima

Table 9: List of Safety Objectives (success approach) for Abnormal Conditions

3.9 Mitigation of System-generated Risks (failure approach)

The SESAR Safety Reference Material (SRM, see §3.3 in [1]) recommends to identify hazards at the level of the operational services:

	<p>To avoid System-generated hazards to be inconsistently defined across the SESAR work programme, they <u>have to be</u> identified at the level of the Operational services, <i>i.e.</i> a level that is independent of the actual design of the System and is related to the failure of an operational service.</p>
---	--

Basically, for the ATC tools of PJ10.02a, there are two failure modes:

- a) The tool does not operate whereas it ought to (a conflict is not detected, a trajectory deviation is not detected, a conflicting aircraft is not taken into account by the What If/What Else) ;

b) The tool “over operates”: it launches an unnecessary alarm (for instance).

If we consider the first failure mode a) and apply it to our five operational services, we identify the five following hazards:

1. The Planner Controller fails to detect a pre tactical conflict (failure a) of the “Conflict Detection aid for the PC”);
2. The Planner Controller improperly solves a pre tactical conflict (failure of the “Conflict Resolution aid for the PC”);
3. The Tactical Controller fails to detect a tactical conflict (failure of the “Conflict Detection aid for the TC”);
4. The Tactical Controller improperly solves a tactical conflict (failure of the “Conflict Resolution aid for the TC” operational service);
5. A trajectory deviation is not detected by the two air traffic controllers.

We recall that the assessment of the severity of hazards is based upon the last barrier which is infringed by the hazard (see Figure 1), so hazards 1 and 2 have a similar severity (Traffic Planning Barrier infringed), and the same operational impact: for these two hazards there is a pending unidentified pre tactical conflict which is to be solved at the tactical level. Similarly, hazards 3 and 4 have the same infringed barrier (Tactical Conflict Management) and the same operational impact: for these two hazards there is a pending tactical conflict which was failed to solve by the tactical controller and will be addressed by the STAC.

Similarly, if we consider the second failure mode b) and apply it to our five operational services, we identify the five following hazards:

1. The “Conflict Detection aid for the PC” signals to the Planner Controller a false pre tactical conflict;
2. The “Conflict Resolution aid for the PC” is polluted by a false conflict and suggests a less optimal trajectory for an incoming aircraft.
3. The “Conflict Detection for the TC” signals to the Tactical Controller a false tactical conflict;
4. The “Conflict Resolution aid for the TC” is polluted by a false conflict and suggests a less optimal trajectory for an aircraft in the sector.
5. The “Trajectory deviation aid” improperly signals a deviation.
6. A trajectory deviation is not detected by the two air traffic controllers.

For hazards 1 and 2, we assume that the Planner controller detects the dysfunction of the tool and corrects it, so the operational impact is a workload increase due to a wrong information. We make a similar assumption for hazards 3 and 4, that the Tactical controller detects the dysfunction and corrects it, also resulting in a workload increase. Finally, the hazard 5 is a nuisance alarm which also results in an increased workload.

As a conclusion, we end up with the same hazards identified by the SAR V2 (see [8]), that we reproduce below.

3.9.1 Identification and Analysis of System-generated Hazards

3.9.1.1 CD/R aid to PC

ID	Description	Related SO (success approach)	Operational Effects	Mitigations of Effects	Severity (most probable effect)
Hz 001	CD/R aid to PC misleads the controller which fails to take action	SO#021 SO#022 SO#023 SO#0210	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.	MAC-SC4b
Hz 002	CD/R aid to PC misleads the controller and increases workload	SO#021 SO#022 SO#023 SO#0210	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.	MAC-SC4b
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 up encounter.	MAC-SC4b
Hz 005	CD/R aid to PC misunderstood	SO#021 SO#022 SO#023	The tools are working correctly,	Training.	MAC-SC4b

	by the controller	SO#0210	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.	<p>Tactical may question planner's decision and solve the possible safety related incident.</p> <p>Situational awareness of Planner – controller will be able to detect and assess the possible error by different means (e.g. radar).</p> <p>Some kind of deviation monitoring may pick up the possible error.</p> <p>TC Aid will eventually pick up encounter.</p>	
--	-------------------	---------	---	--	--

Table 10: System-Generated Hazards and Analysis for CD/R aid to PC

3.9.1.2 CD/R aid to TC

ID	Description	Related SO <i>(success approach)</i>	Operational Effects	Mitigations of Effects	Severity <i>(most probable effect)</i>
Hz 006	CD/R aid to TC misleads the controller	SO#011 SO#012 SO#014	The tool misleads the controller into missing a tactical conflict.	Executive controller picks up encounter from radar scan. Other tools (STCA etc.) can help.	MAC-SC3
Hz 007	CD/R aid to TC presents nuisance alerts	SO#011 SO#012 SO#014	The tool presents nuisance alerts to the controller which increase workload, potentially leading to a missed tactical conflict.	The controller can delete/suppress nuisance alerts. In order to avoid nuisance alerts parameters for situations when the TC aid should trigger alerts have to be defined.	MAC-SC3
Hz 008	CD/R aid to TC presents	SO#011 SO#012	The tool presents nuisance	The controller can use other tools to double check the proposal (e.g. radar).	MAC-SC3

	nuisance resolution	SO#014	resolution proposals leading to a missed tactical conflict.	If an unsafe clearance was made by the ATCO then the conflict detection would alert controller to the conflict. Ground based and airborne safety nets e.g. STCA.	
Hz 009	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.	MAC-SC3
Hz 010	C D/R aid to TC misunderstood by the controller	SO#011 SO#012 SO#014	The tools are working correctly, however the controller may misunderstand / misinterpret the data shown and make a bad tactical decision. This therefore increases workload 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.	MAC-SC4b

Table 11: System-Generated Hazards and Analysis for CD/R aid to TC

3.9.1.3 Trajectory deviation Aid

ID	Description	Related SO <i>(success approach)</i>	Operational Effects	Mitigations of Effects	Severity <i>(most probable effect)</i>
Hz 011	Failure of the “improved part” Trajectory deviation aid	SO#021 SO#022 SO#023 SO#0210	The “improved” trajectory deviation aid allows to detect earlier a trajectory deviation (before it actually starts), by using data from the avionics. The deviation is still detected but once it happens.	The worst credible effect would be that, due to this delay, the Tactical Controller has to solve some new conflict with a limited anticipation. This effect is captured by the MAC-SC4A	MAC-SC4A
Hz 012	The trajectory deviation aid causes a nuisance alarm	SO#021 SO#022 SO#023 SO#0210	The tool issues an alarm whereas there is no actual trajectory deviation, issuing a workload increase, but also a “loss of trust” towards the tool	The “loss of trust” towards the tool would at worst, lead to trajectory deviation which would be neglected by the Tactical controller, and a possible conflict solved with limited anticipation. The effect is conservatively assessed as MAC-SC4A.	MAC-SC4A

Table 12: System-Generated Hazards and Analysis for the Trajectory deviation Aid

3.9.2 Derivation of Safety Objectives (integrity/reliability)

As explained in Guidance E of Reference [2], Safety Objectives for each Hazard are derived according to the following equation:

$$SO_{Hz} = \frac{\text{Maximum_Tolerable_Freq._of_occurrence}_{\text{relevant_severity_class}}}{N \times IM}$$

where:

- $MTFoO_{\text{relevant_severity_class}}$ stands for the Maximum Tolerable Frequency of Occurrence being the maximum probability of the hazard’s effect as defined in Table 13;
- N is the overall number of operational hazards for a given severity class at a given barrier as obtained from Table 14;
- IM is the Impact Modification factor to take account of additional information regarding the operational effect of the hazard, in particular related to the number of aircraft exposed to the operational hazard.

Severity Class	Hazardous situation	Operational Effect	MTFoO [per fh]
MAC-SC1	A situation where an aircraft comes into physical contact with another aircraft in the air.	Accident - Mid air collision (MF3)	1e-9
MAC-SC2a	A situation where an imminent collision was not mitigated by an airborne collision avoidance but for which geometry has prevented physical contact.	Near Mid Air Collision (MF3a)	1e-6
MAC-SC2b	A situation where airborne collision avoidance prevents near collision	Imminent Collision (MF4)	1e-5
MAC-SC3	A situation where an imminent collision was prevented by ATC Collision prevention	Imminent Infringement (MF5-9)	1e-4
MAC-SC4a	A situation where an imminent infringement coming from a crew/aircraft induced conflict was prevented by tactical conflict management	Tactical Conflict (crew/aircraft induced) (MF6.1)	1e-3
MAC-SC4b	A situation where an imminent infringement coming from a planned conflict was prevented by tactical conflict management	Tactical Conflict (planned) (MF5.1)	1e-2
MAC-SC5	A situation where, on the day of operations, a tactical conflict (planned) was prevented by Traffic Planning and Synchronization.	Pre tactical conflict (MF5.2)	1e-1

Table 13: Risk Classification Scheme for MAC in En-Route & TMA.

Severity Class	Number of hazards per Severity Class per Accident Type			
	MAC (ER&TMA)	RWY Coll.	CFIT	TWY Coll.
SC1	1	1	5	1
SC2	n/a	n/a	10	n/a
SC2a	5	5	n/a	5
SC2b	10	10	n/a	10
SC3	25	20	n/a	20
SC4a	30	n/a	n/a	n/a
SC4b	30	n/a	n/a	n/a
SC5	100	100	n/a	100

Table 14: Maximum Hazard Numbers per Severity Class per Accident Type

Using the information presented above, the frequency of occurrence is calculated for each of the Safety Objectives:

$$SO_Hz_4B = \frac{\text{Maximum_Tolerable_Freq._of_occurrence}_{\text{relevant_severity_class}}}{N \times IM} = \frac{10^{-2}}{30 \times 2} = 1,67 \times 10^{-4}$$

$$SO_Hz_4A = \frac{\text{Maximum_Tolerable_Freq._of_occurrence}_{\text{relevant_severity_class}}}{N \times IM} = \frac{10^{-3}}{30 \times 2} = 1,67 \times 10^{-5}$$

$$SO_Hz_3 = \frac{\text{Maximum_Tolerable_Freq._of_occurrence}_{\text{relevant_severity_class}}}{N \times IM} = \frac{10^{-4}}{25 \times 2} = 2 \times 10^{-6}$$

3.9.2.1 Safety objectives for the CD/R aid for the PC

ID	Safety Objectives
HZ001	1.67*10 ⁻⁴
HZ002	1.67*10 ⁻⁴

Hz003	$1.67 \cdot 10^{-4}$
Hz004	$1.67 \cdot 10^{-4}$
Hz005	$1.67 \cdot 10^{-4}$

Table 15: Safety Objectives (integrity/reliability)

3.9.2.2 Safety objectives for the CD/R aid for the TC

ID	Safety Objectives
Hz006	$2 \cdot 10^{-6}$
Hz007	$2 \cdot 10^{-6}$
Hz008	$2 \cdot 10^{-6}$
Hz009	$2 \cdot 10^{-6}$
Hz010	$1,67 \cdot 10^{-4}$

Table 16: Safety Objectives (integrity/reliability)

3.9.2.3 Safety objectives for the Trajectory Deviation Aid

ID	Safety Objectives
Hz011	$1,67 \cdot 10^{-5}$
Hz012	$1,67 \cdot 10^{-5}$

Table 17: Safety Objectives (integrity/reliability)

4 Safe Design at SPR Level

4.1 Scope

This section addresses the following activities:

- Description of the SPR-level model (see **Guidance G.2** of **Reference [2]**) of the end-to-end Solution ATM System - section 4.2
- Derivation, from the Safety Objectives (Functionality and Performance) of section 3, of Safety Requirements for the SPR-level design - section 4.3
- Analysis of the operation of the SPR-level design under normal operational conditions – section 4.4
- Analysis of the operation of the SPR-level design under abnormal conditions of the Operational Environment - section 4.5
- Assessment of the adequacy of the SPR-level design in the case of internal failures and mitigation of the System-generated hazards - section 4.6”

4.2 The PJ10.02a Solution SPR-level Model

4.2.1 Scope and notations of the SPR level Models

The introduction of Conflict Detection/Resolution aids for the planner and the tactical has been addressed by SESAR1 WP 4.7.2 and WP 5.7.2, so there is no need to replicate this work here. In other words, we have not addressed in this document the Safety requirements linked to the baseline ATC tools, we have limited ourselves to the scope of PJ10.02a. The scope of PJ 10.02a is (for all but two exercises, EXE001 and EXE002) an improvement of these ATC Tools, through a provision of additional data (ADS-C EPP and Mode S). In addition to that, for two Exercises (EXE004 and EXE005), the CPDLC has also been implemented. For exercise EXE001, the improvement was in the algorithm of the CD aid for the TC. EXE002 addresses the implementation of TCT in Stockholm TMA, and is not addressed in this document (since its scope falls within the SESAR1).

The purpose of SPR level Models is to allow the design of SPR Requirements as a mean to satisfy the Safety Objectives found in Section 3, so the SPR level Models will focus on the data flows associated to five Operational Services listed in §3.6.2, in order to allow the design of SPR Requirements aimed at guaranteeing the performance of these operational services. These SPR Requirements will be established by considering possible failures on the data flows, together with their impacts on the corresponding operational services. We have distinguished **technical** data flows (where the failure is technical, for instance data corruption) from operational data flows, where a human actor insert data into the system, and the error is **operational** (insertion error, for instance).

When designing the different SPR level Models, we found two ways of synthesizing: firstly, we found that the Conflict Detection and Conflict Resolution had similar data flows, whether it was for the Planner or for the Tactical, so in the Models these will be represented without mentioning Planner or Executive. Secondly, we found that some exercises shares similarities, so that it was possible to synthesize different exercises with the same SPR level model.

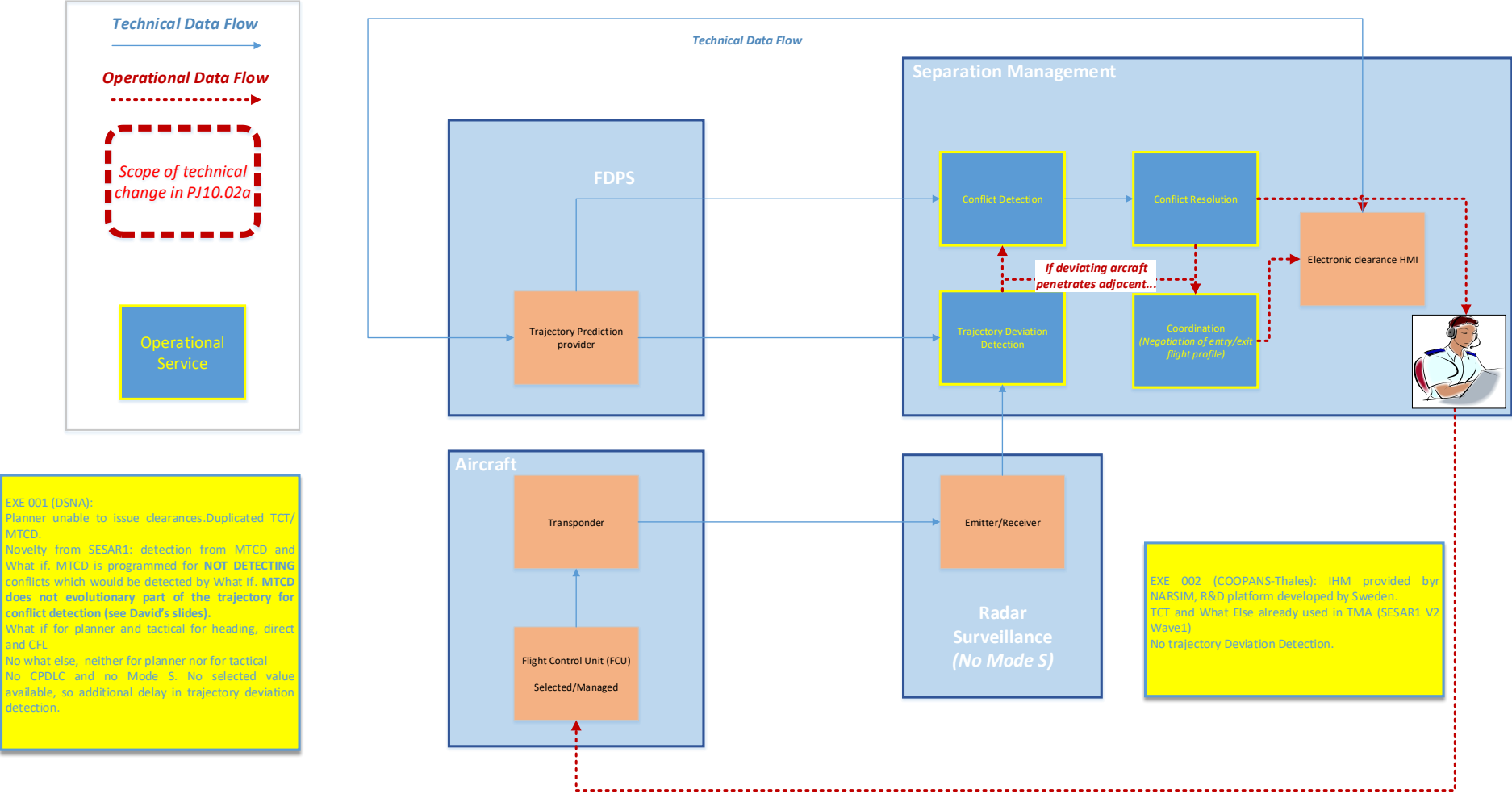
Namely, EXE 001 (DSNA) and EXE002 (COOPANS) were merged due to the following similarities:

- No ADS-C EPP and no Mode S;
- No CPDLC.

Similarly, EXE 004 (ANS-CR and Eurocontrol) and EXE005 (Skyguide) were merged due to the following similarities:

- No ADS-C EPP but Mode S;
- CPDLC.

4.2.2 SPR-level Model for EXE001 and EXE002



EXE 001 (DSNA):
 Planner unable to issue clearances. Duplicated TCT/MTCD.
 Novelty from SESAR1: detection from MTCD and What if. MTCD is programmed for **NOT DETECTING** conflicts which would be detected by What if. MTCD does not evolutionary part of the trajectory for conflict detection (see David's slides).
 What if for planner and tactical for heading, direct and CFL.
 No what else, neither for planner nor for tactical.
 No CPDLC and no Mode S. No selected value available, so additional delay in trajectory deviation detection.

EXE 002 (COOPANS-Thales): IHM provided by NARSIM, R&D platform developed by Sweden.
 TCT and What Else already used in TMA (SESAR1 V2 Wave1)
 No trajectory Deviation Detection.

Figure 2: SPR level Model for EXE001 and EXE002

4.2.3 SPR-level Model for EXE003

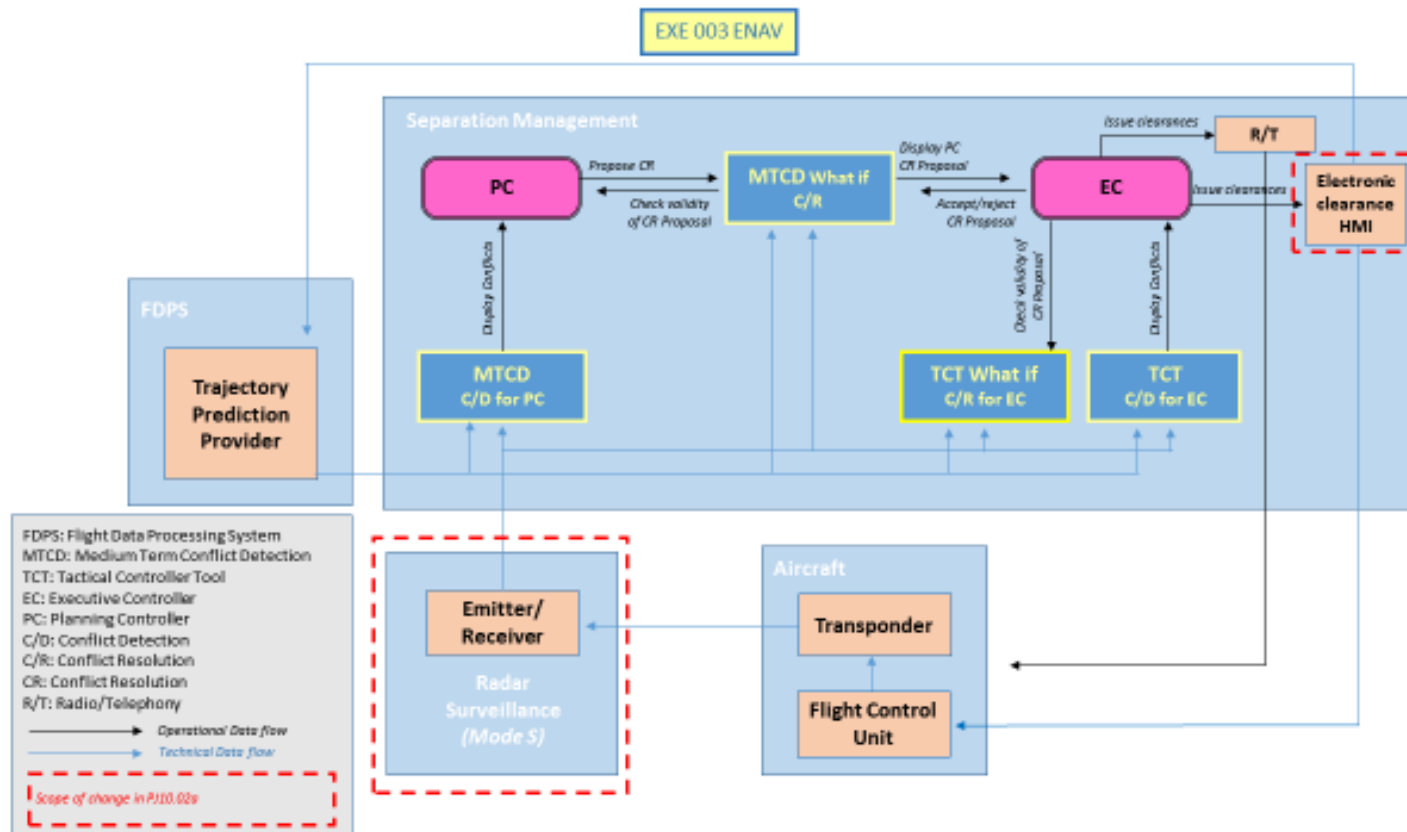


Figure 3: SPR level Model for EXE003

4.2.4 SPR-level Model for EXE004 and EXE005

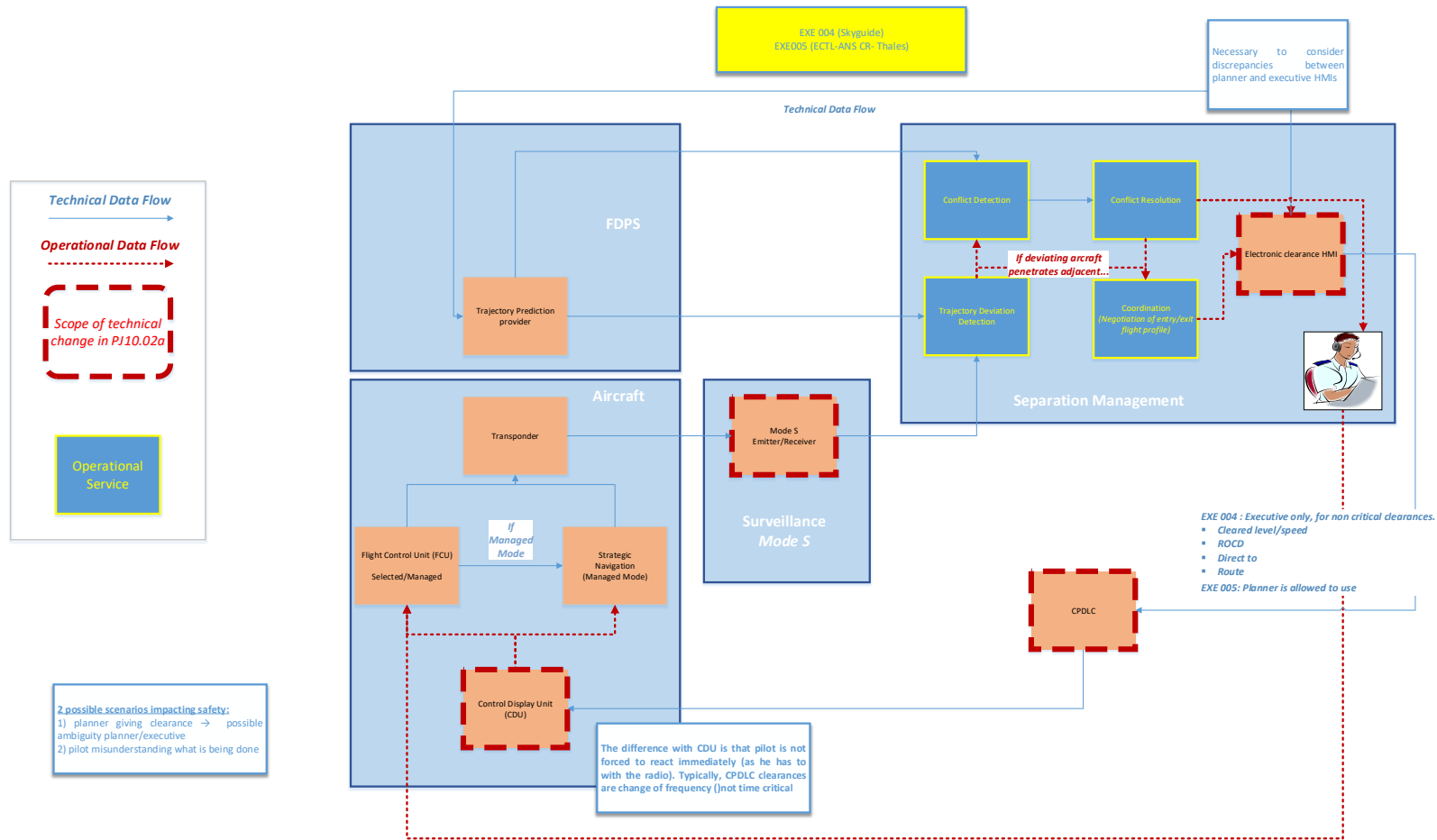


Figure 4: SPR level Model for EXE004 and EXE005

4.2.5 SPR-level Model for EXE006

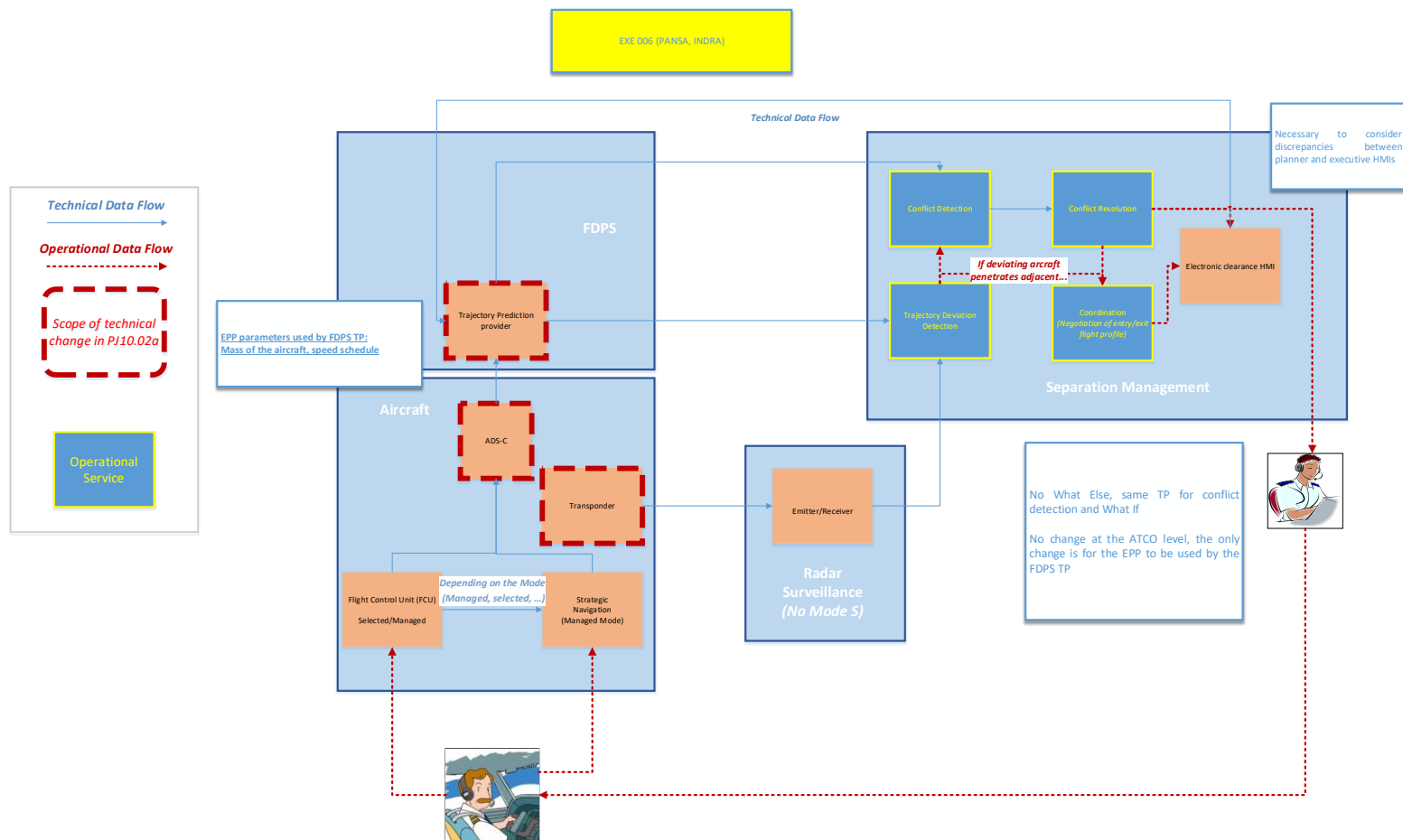


Figure 5: SPR level Model for EXE006

4.2.6 SPR-level Model for EXE007

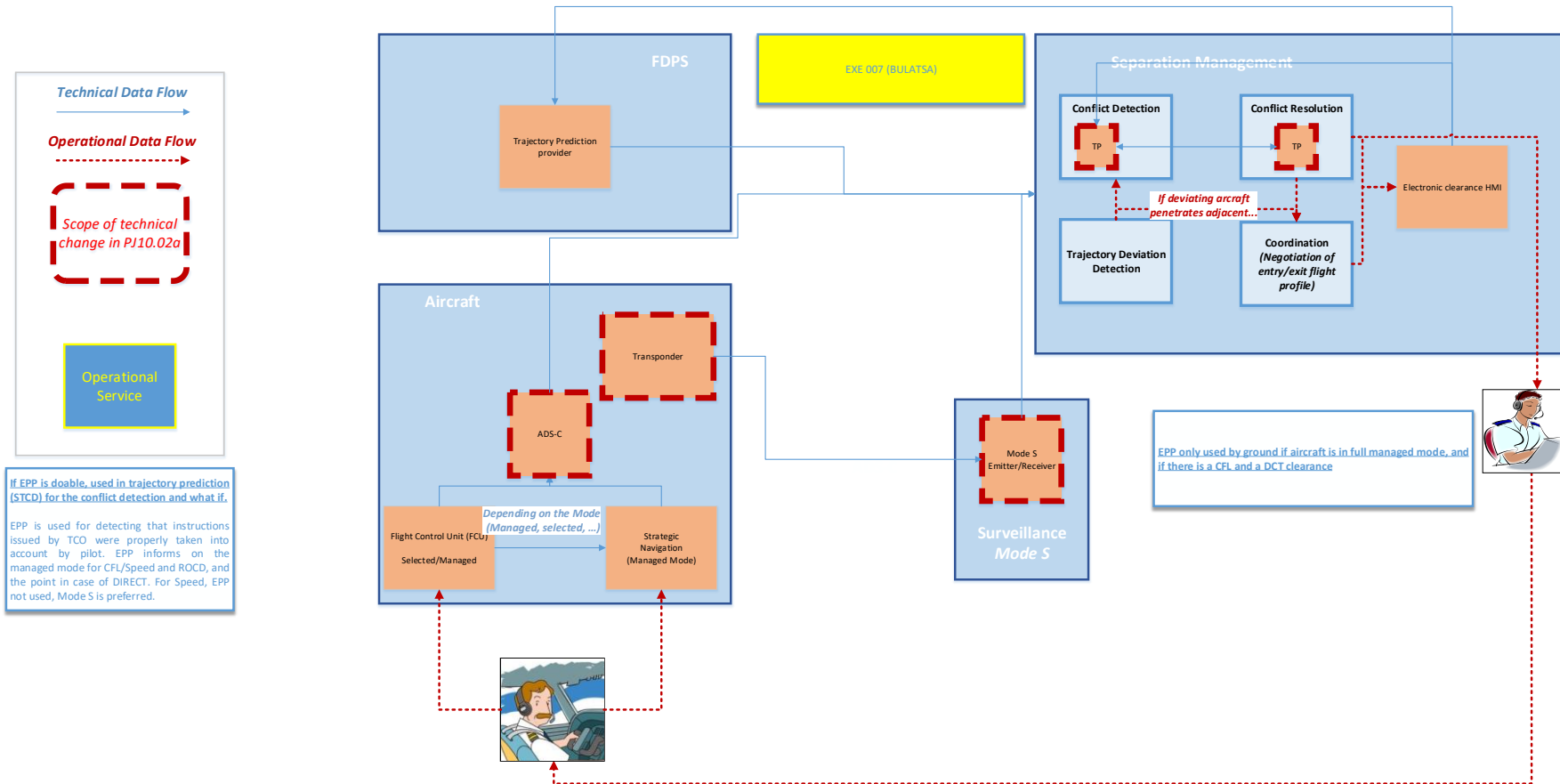


Figure 6: SPR level Model for EXE007

1000 **4.3 Derivation of Safety Requirements (Functionality and**
 1001 **Performance – success approach)**

1002 The safety requirements which are presented here are limited to the scope of the PJ10.02A, which is
 1003 represented in dashed red for all SPR models illustrated from Figure 2 to Figure 6. We have not
 1004 reproduced here the safety requirements which were derived for the ATC tools in SESAR1 WP 04.07.2
 1005 and WP05.07.2, and we have limited ourselves to the technical scope of PJ10.02A, which is the
 1006 additional data provided to the ATC tools, together with the use of CPDLC for some exercises.

1007 **4.3.1 Safety Requirements derived from EXE001 (DSNA) and EXE002**
 1008 **(COOPANS)**

1009 The SPR-level model of Figure 2 does not show any “innovative” data flow entering the ATC tools,
 1010 neither any innovative Sub System interacting with the ATC tools (such as, for instance, the CPDLC) so
 1011 there are no safety requirements being derived from the success approach safety objectives.

1012 In other words, the EXE001 and EXE002 fall into the scope of the previous SESAR1 solutions WP 4.7.1
 1013 and WP 5.7.1, so they should comply with the sole safety requirements of these two WPs.

1014 **4.3.2 Safety Requirements derived from EXE003 (ENAV)**

1015 The SPR-level model of Figure 3 shows two data flows entering the ATC tools, both starting from the
 1016 Mode S:

- 1017 – Mode S data sent to the Trajectory Deviation Detection aid
- 1018 – Mode S data sent to the Trajectory Prediction of the Conflict Detection aid

1019 As seen in Figure 3, the technical architecture of EXE003 makes use of a combined Trajectory Predictor,
 1020 which combines the Trajectory Prediction (TP) from the FDPS together with the Mode S data (Ground
 1021 Speed, ROCD, TOD) in order to determine an improved TP. This improved TP is then sent to all ATC
 1022 tools.

1023

Safety Objectives (Functionality and Performance from success approach)	Requirement (forward reference)	Maps on to
Possibly all SO#(depending on the use of Mode S data)	SR_SO 01	Combined Trajectory Prediction
SO#021	SR_SO 02	MTCD → PC
SO#201	SR_SO 03	MTCD What-if → PC
SO#022	SR_SO 04	EC → MTCD What-if

		EC → TCT What-if
SO#011 SO#014	SR_SO 05	TCT > EC
SO#013 SO#014 SO#015	SR_SO 06	TCT What-if > EC

1024 **Table 18: Mapping of Safety Objectives to SPR-level Model Elements**

1025 In order to make a valid use of the Mode S data, the Combined Trajectory Predictor should verify that
 1026 the Mode S fields used by the algorithmic device are available and valid (as explained, for instance, in
 1027 Appendix A2 of Reference [10]). In addition, some requirements specific to the HMI have been added,
 1028 in order to ease the interpretation of the alarms by the Air Traffic Controllers.

Safety Requirement (functionality & performance) [SPR-level Element]	Requirement & Model	Derived from Table 4 to Table 8
SR_SO 01	If the ATC Tools make use of a “combined Trajectory Prediction” (which integrates the FDPS TP together with Mode S data from the avionics), the combined TP shall check that the avionics Mode S data are available and valid.	Possibly all SOs
SR_SO 02	Only MTCD alerts (CD for the PC) corresponding to a predicted loss of both vertical and horizontal separation minima shall be displayed on the track label of the flight tracks involved in the conflict.	SO#021
SR_SO 03	When the PC uses the What-if function (C/R for the PL) to check if a given FL change or Route change is conflict free, the visualization of the outcome shall be provided as close as possible to the HMI area where the request was issued (e.g. in the track label), in order to minimize the risk that the PC will spend too much time to check the validity of the proposed change.	SO#201
SR_SO 04	When receiving a conflict resolution proposal (either FL change or Route change) via the What-if functionality (C/R for the EC), the EC shall be able to implement/reject the proposal using an HMI feature located as close as possible to the affected flight (e.g. in the track label), in order to minimize the risk of spending too much time before implementing/rejecting the conflict resolution.	SO#022

SR_SO 05	Only TCT alerts (C/D for the EC) corresponding to a predicted loss of both vertical and horizontal separation minima shall be displayed on the track label of the flight tracks involved in the conflict.	SO#011
SR_SO 06	When the EC uses the What-if function (C/R for the EC) to check if a given FL change or Route change is conflict free, the visualization of the outcome shall be provided as close as possible to the HMI area where the request was issued (e.g. in the track label), in order to minimize the risk that the EC will spend too much time to check the validity of the proposed change.	SO#013

1029 **Table 19: Derivation of Safety Requirements (functionality and performance) from Safety Objectives**

1030 **4.3.3 Safety Requirements derived from EXE004 (Skyguide) and EXE005 (ANS-**
1031 **CR/Eurocontrol)**

1032 As illustrated in Figure 4, EXE004 and EXE005 share the following similarities:

- 1033 – Use of Mode S;
- 1034 – Use of CPDLC (only for the Tactical in EXE004, for the Planner also in EXE005);
- 1035 – Enhanced HMI for the Controller Working Positions (CWPs) in order to allow each controller
1036 to “know” what the other does (necessary in case of CPDLC used by both controllers).

1037 The “innovative” dataflows are firstly the use of Mode S, and secondly the use of CPDLC, which requires
1038 to consider also the action of the pilot on his Controller Display Unit (CDU).

1039 The SPR-level model of Figure 3 shows two data flows entering the ATC tools, both starting from the
1040 Mode S:

- 1041 – Mode S data sent to the Trajectory Deviation Detection aid
- 1042 – Mode S data sent to the Trajectory Prediction of the Conflict Detection aid

Safety Objectives (Functionality and Performance from success approach)	Requirement (forward reference)	Maps on to
SO#011	SR_SO 07	HMI → ATCO PC/EC
SO#021		
SO#014	SR_SO 08	ATCO PC/EC → CPDLC
SO#022		

SO#012	SR_SO 09	Mode S → Trajectory Deviation Detection
--------	----------	---

1043 **Table 20: Mapping of Safety Objectives to SPR-level Model Elements**

1044 A consequence of CPDLC is a risk that the “other” controller (the one which did not send the CPDLC
 1045 message) is not aware of the CPDLC message sent by his colleague. Therefore, it is necessary to ensure
 1046 that both controllers are always aware of the clearances which are sent by any of them, otherwise the
 1047 conflict resolutions and detections functions might be impacted.

1048 When Using CPDLC, the pilot retrieves the CPDLC message from his Control Display Unit and he is not
 1049 compelled to execute the cleared instruction immediately (as it is the case if he receives an instruction
 1050 by radio), so CPDLC messages should not be used for time critical conflict resolutions.

1051 Similarly to EXE003, the use of Mode S for trajectory deviation requires to use valid Mode S.

1052

Safety Requirement (functionality & performance) [SPR-level Element]	Requirement & Model	Derived from Table 4 to Table 8
SR_SO 07	When CPDLC is used by controllers, the Human Machine Interface should display the CPDLC clearance to the “other” controller so that he keeps informed of the CPDLC message sent by his colleague	SO#011 SO#021
SR_SO 08	When CPDLC is used, controllers should limit it to conflict resolutions which are not time critical	SO#014 SO#022
SR_SO 09	When Mode S is used for trajectory deviation detection, The Monitoring Aid should ensure that the Mode S fields are available and valid	SO#012

1053 **Table 21: Derivation of Safety Requirements (functionality and performance) from Safety Objectives**

1054

1055 **4.3.4 Safety Requirements for ADS-C EPP data (success approach)**

1056 EXE 006 & EXE 007 target V2 maturity and the upcoming sections highlight the safety requirements
 1057 derived from V2 exercises and prepare for V3 studies. EXE006 and EXE007 both use ADS-C EPP data.
 1058 In the following subsections, we will derive safety requirements from the global architecture for both
 1059 exercises. In this subsection, we limit ourselves to the ADS-C EPP data itself, and we detail safety

1060 requirements related to the success approach, that is aiming at ensuring that the ATC tools will be
1061 improved optimally.

1062 ADS-C EPP data comprise three different sets of information:

- 1063 1) A 4D trajectory prediction consisting in a sequence of Waypoints, with corresponding time of
1064 arrival and FL;
- 1065 2) Speeds provided for EPP waypoints;
- 1066 3) A subset of integrity parameters (such as checksums), which describe the integrity of the ADS-
1067 C EPP data

1068 We detail below how the pro and cons of using such or such data from the ADS-C EPP, for the purpose
1069 of improving the trajectory prediction

1070 **4.3.4.1 ADS-C EPP trajectory prediction for the simplest case**

1071 We start by the simplest case of a steady aircraft flying towards a Waypoint, where the ADS-C EPP data
1072 contains an expected time of arrival for this Waypoint, together with a value of the CAS. There are two
1073 ways to predict the aircraft trajectory towards the waypoint:

- 1074 1) From the ADS-C EPP distance and the time of arrival to the waypoint, derive a Ground Speed
1075 (GS), and extrapolate the aircraft trajectory with this Ground Speed.
- 1076 2) Convert the ADS-C EPP CAS into a True Air Speed (TAS), then add an estimate of the wind speed
1077 to this TAS in order to estimate a Ground Speed.

1078 The method 1) gives a more accurate result than the method 2), because the aircraft can estimate the
1079 TAS (thanks to the pitot) and the Ground Speed (thanks to its GPS) with a good accuracy, and therefore
1080 the wind speed which is the difference of these two speeds. Therefore, the times of arrival from the
1081 ADS-C EPP data are of a good quality. On the other hand, the wind speed used by the FDPS in method
1082 2) comes for global meteorological data files, which are less accurate than the estimation made by the
1083 avionics.

1084 As a consequence, if it is possible to use method 1), this method should be preferred. However, the
1085 con of method 1) is that it requires to modify the traditional algorithm used by FDPS, which usually
1086 process both a True Air Speed and a Wind speed in order to estimate a Ground Speed (which is the
1087 sum of these two speeds). In other words, using the method 2) can be done by adding to the FDPS a
1088 simple plugin (which extract the CAS from the ADS-C EPP data), whereas the method 1) requires more
1089 complex changes on the FDPS. These changes represent an additional financial cost, which is not
1090 minor.

1091 We derive the first Safety Requirement for this case.

1092

Safety Requirement	Requirement	Derived from
(functionality & performance)		Table 4 to Table 8
[SPR-level Model Element]		

SR_EPP_1	For a steady aircraft flying towards a waypoint, the improvement of trajectory prediction by using ADS-C EPP will be made preferably using method 1) above rather than method 2), provided that both methods are possible.	
----------	--	--

1093 **4.3.4.2 ADS-C EPP trajectory prediction for the “less simple” case of an**
1094 **evolutionary aircraft**

1095 We now consider a less simple case than the previous one, where the aircraft still flies towards a
1096 waypoint, but instead of being steady it is in vertical evolution during a portion of its flight. In order to
1097 simplify, this case, we will assume that the aircraft is currently in vertical evolution (climb or descent),
1098 and the question is how to predict its trajectory given ADS-C EPP data. Here, we shall use both the
1099 speeds in the ADS-C EPP and the 4D trajectory prediction provided by the ADS-C EPP, in order to
1100 provide an optimal estimate.

1101 Firstly, an assumption used in EUROCONTROL BADA ([13]) is that the aircraft keeps a constant CAS
1102 along the vertical sections defined by a speed schedule, and a constant Mach above a cross over
1103 altitude (denoted as "transition altitude" in [13]). When this assumption holds, it can be established that
1104 the horizontal acceleration and the vertical speed have a fixed ratio, and that this ratio is a function of
1105 the current altitude and of the value of the CAS. In mathematical terms,

1106
$$\frac{ACC}{V_Z} = Constant(FL, CAS)$$

1107 In Eurocontrol BADA methodology this Constant is similar to the Energy Share Factor (ESF), in the sense
1108 that it describes the share of Energy between the horizontal and the vertical.

1109 We have one equation for two unknown (acceleration and vertical speed), so we need another
1110 equation. If we use the Total Energy Model, the second equation is given by

1111
$$mgV_Z + m V_{TAS} ACC = (THRUST - DRAG) V_{TAS}$$

1112 Where V_{TAS} stands for the True Air Speed. BADA provides an estimate for the Thrust and the Drag, so
1113 in this last equation everything is known except the vertical speed and the acceleration.

1114 These two equations allow to extrapolate a trajectory prediction, starting from the acceleration and
1115 the vertical speed, and integrating in order to determine the altitude, the horizontal speed and the
1116 horizontal position.

1117 However, the value of the Thrust may depend on the choice of the pilot, so it is possible to extrapolate
1118 a “possible range” of trajectories, by choosing (for instance) an initial fixed vertical speed. From this
1119 initial vertical speed, the steps are as follows:

- 1120 1) Determine the corresponding acceleration using the first Equation;
1121 2) Determine a corresponding value for the Thrust using the second Equation;
1122 3) With this value of the thrust, extrapolate the whole trajectory.

1123 Then, once arrived at the final FL, we keep on extrapolating the aircraft trajectory until it arrives to the
1124 first Waypoint, with the same speed as the speed that the aircraft had at the end of its vertical
1125 evolution. Figure 7 illustrates our algorithm. By proceeding through trial and error, we iterate until we

1126 find a satisfactory choice for the initial V_z , which results in arriving at the Waypoint at the proper time
 1127 (the time provided by the ADS-C EPP report).

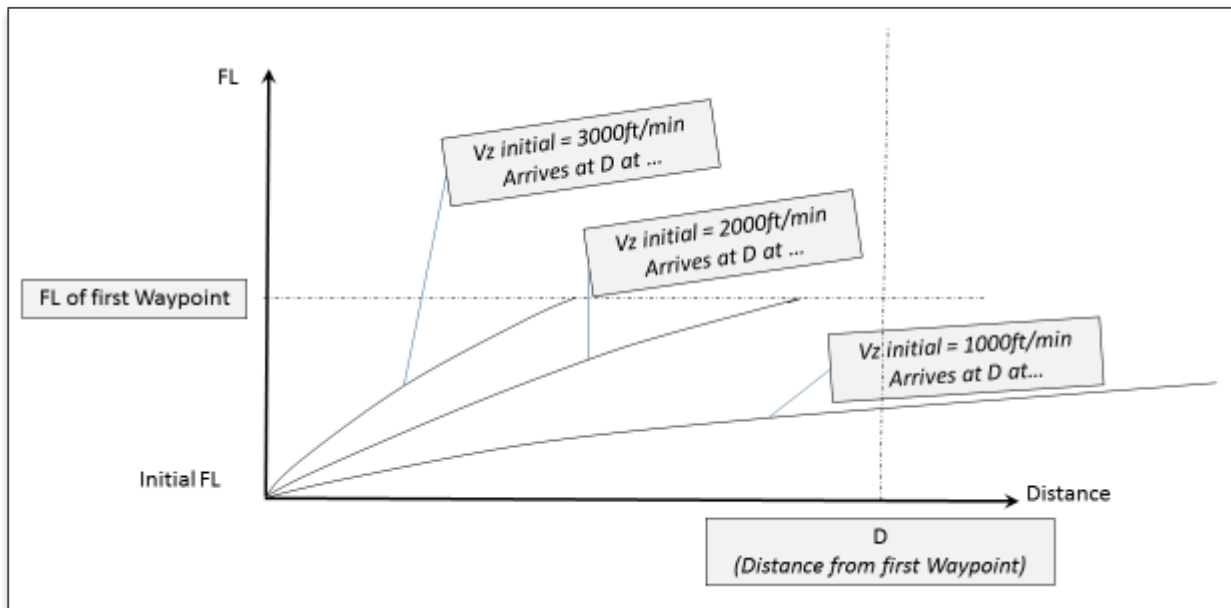


Figure 7

1128
 1129
 1130 Then this algorithm can be reproduced for all subsequent Waypoints. Here we considered the case of
 1131 an aircraft initially in climb, the case of the descent is equivalent.

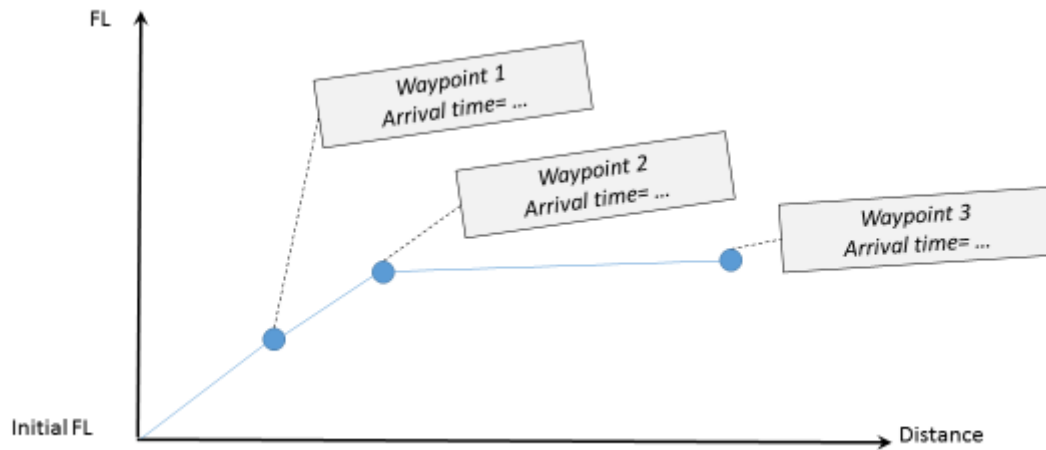
1132 In Summary, the algorithm detailed above makes the best use of the ADS-C EPP report, in the sense
 1133 that it is compliant with the “Constant CAS” assumption, and that the aircraft flies with the CAS
 1134 provided by the ADS-C EPP report, and arrives at the different Waypoints as indicated in the ADS-C EPP
 1135 report.

1136 We derive the following safety requirement:

Safety Requirement (functionality & performance) [SPR-level Model Element]	Requirement	Derived from Table 4 to Table 8
SR_EPP_2	For an evolutionary aircraft flying towards a waypoint, the improvement of trajectory prediction by using ADS-C EPP can be achieved by considering algorithmic means, such as the one explained above (provided that its implementation is made possible by the FDPS architecture.).	

1137 **4.3.4.3 ADS-C EPP trajectory prediction when the aircraft does not fly towards a**
 1138 **waypoint**

1139 The previous algorithm only considered the distances from the consecutive Waypoints in order to
 1140 extrapolate a trajectory prediction. So this algorithm still applies for an evolutionary aircraft which
 1141 does not fly towards a Waypoint. In other words, the principle is to use the ADS-C EPP 4D trajectory
 1142 in order to extrapolate a “final distance” (the distance to the Waypoint), and having this distance we
 1143 can proceed exactly as in the two previous subcases.



1144
 1145 **Figure 8**

1146 Figure 8 illustrates the ADS-C EPP profile which is used together with the previous algorithm. The
 1147 accuracy of the trajectory prediction is strongly dependent on the accuracy of the ADS-C EPP profile
 1148 illustrated in Figure 8. The algorithm presented so far is mostly applicable to ATC tools devoted to the
 1149 executive controller, which relies upon passed clearances. This algorithm could also meet operational
 1150 needs more oriented towards planning services (such as, for instance, conflict detection at the planner
 1151 level). The challenge, here, is to insert operational constraints into such an algorithm which will apply
 1152 to the flight in the future (such as the Letters of Agreement), but which have not been issued so far in
 1153 terms of clearances; this thread of activity is part of the V3 scope, so it is not addressed in this
 1154 document. This operational need is traced through a specific requirement, expressed hereafter.

1155

1156

Safety Requirement (functionality & performance) [SPR-level Model Element]	Requirement	Derived from Table 4 to Table 8
SR_EPP_3	For an aircraft which does not fly toward a waypoint, the improvement of trajectory prediction by using ADS-C EPP can be achieved by considering algorithmic means, such as the	

one explained above, after determining that the accuracy requirements are met by the ADS-C EPP data (To be considered during Future V3 Validation phase).

If such an algorithm was to be used at the operational level for a planning purpose, caution should be taken to properly ensure that the computation of the predicted trajectory takes into account operational constraints impacting the future of the flight profile (such as the Letters Of Agreement). This is to be considered during future V3 validation phase

1157

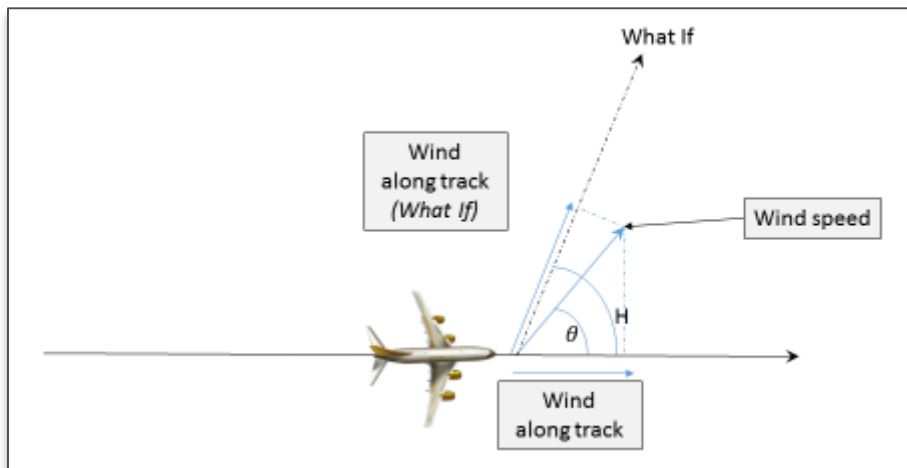
1158

1159 **4.3.4.4 Use of ADS-C EPP data for What If**

1160 In case of a What If for CFL we will use the set of coefficients computed from the last ADS-C EPP report
 1161 (all if in full manage mode or the valid portion (i.e. for CLF the portion up to cleared level)). This set of
 1162 coefficients will be applied on our internal algorithms used for the computation of Vertical Speed and
 1163 Ground Speed.

1164

1165 In the case of a What If for a horizontal clearance (such as a heading), the previous algorithm will have
 1166 to be modified in order to consider the impact of the wind on the aircraft trajectory.



1167

1168

Figure 9

1169 As illustrated in Figure 9, in the case of a What If trajectory, the along track component of the Wind
 1170 will be modified for the aircraft. This is the component to be considered when extrapolating a
 1171 trajectory prediction, since the aircraft will fly so as to eliminate its cross track wind component.

1172 Therefore, the previous algorithm should be completed as follows: once a trajectory prediction has
1173 been established as explained in the previous subsection, this trajectory prediction should be modified
1174 by subtracting the “Wind Along Track” and adding the “Wind along track (What If)”, as illustrated in
1175 Figure 9.

1176 In summary, the ADS-C EPP trajectory prediction for What If requires to have the wind information.
1177 This information is usually available for meteorological files.

1178 In the sequel of this subsection, we investigate the magnitude of the error when the wind component
1179 is not taken into account.

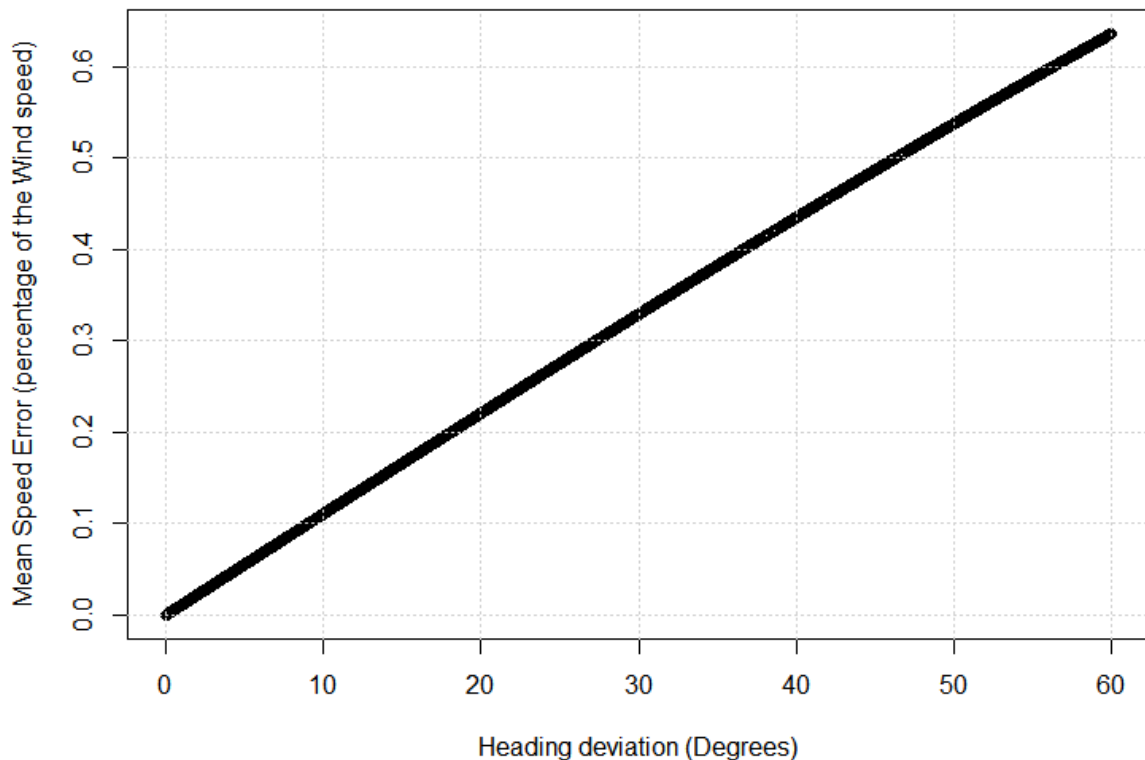
1180 As can be seen on Figure 9, the change of horizontal trajectory corresponding to the What If horizontal
1181 clearance will impact of the True Air Speed of the aircraft, due to the modification of the along track
1182 component of the wind speed. The Wind Speed modifies the True Air Speed of the aircraft by the factor

1183
$$V_{Wind}|\cos \theta - \cos(\theta - H)|$$

1184 Where H is the difference of heading between the course of the aircraft and the What If course, and θ
1185 is the wind speed angle from the course of the aircraft. This wind speed angle may take any value
1186 between 0 and 360 degrees, so the mean value of this “TAS error” (in terms of percentage of the Wind
1187 Speed) is given by

1188
$$\frac{1}{360} \int_0^{360} |\cos \theta - \cos(\theta - H)| d\theta$$

1189 And the computation of this equation for different values of H (we recall that H represents the angle
1190 between the What If trajectory and the nominal trajectory) is illustrated in Figure 10.



1191

1192

Figure 10

1193 We now explain how to use the diagram of Figure 10, for practical purpose. For a deviation of (say) 25
1194 degrees between the nominal aircraft trajectory and the What If trajectory, the speed error is around
1195 0.28 of the Wind Speed. For a “reasonable” value of the wind speed (say 30 kts), this error amounts to
1196 $0.28 \times 30 = 8.4$ kt. For a 10 minutes extrapolation, the error will be $8.4/6 = 1.4$ Nm. So, the value of
1197 1.4Nm is an “extra buffer” which has to be added when estimating the separation between aircraft
1198 using the What If.

1199 The above computations are only illustrative of a way to proceed in order to take into account the
1200 wind error. A more conservative approach would be to consider not the Mean but the 0.9 Quantile of
1201 the error, so that we would be assured that the Wind error is always below our buffer value, with 90%
1202 chances. Figure 11 shows the new value if we take the 90% Quantile. If we recompute our previous
1203 illustrative example with the values of Figure 11, we find, for an angle of 25 degrees, a 0.9 quantile of
1204 0.43, so that, for a wind speed of 30 kt, the wind error amounts to $30 \times 0.43 = 12.9$ kt. For an
1205 extrapolation of 10 minutes, the error would be $12.9/6 = 2.15$ Nm.

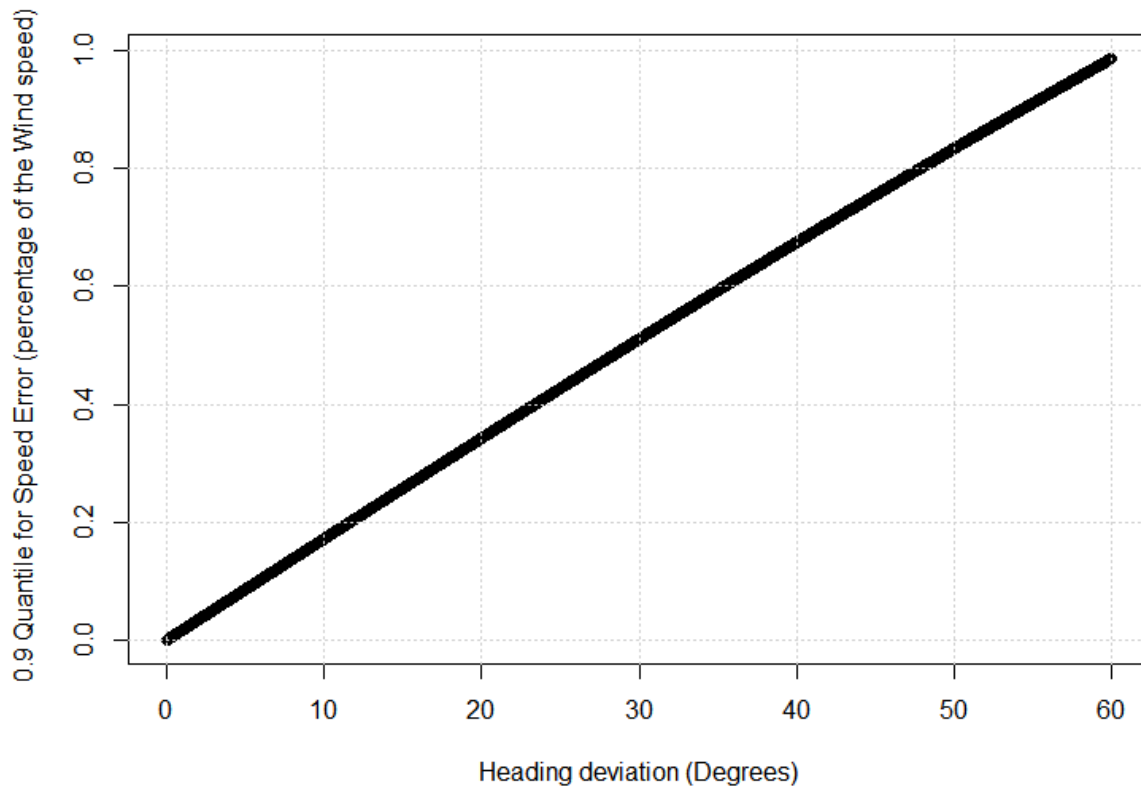


Figure 11

1206

1207

1208 We derive the following safety requirement:

Safety Requirement (functionality & performance) [SPR-level Model Element]	Requirement	Derived from Table 4 to Table 8
SR_EPP_4	When extrapolating a trajectory prediction using the ADS-C EPP report for a What If, the algorithm should consider the wind, as explained previously. If this enhancement is not possible, an additional buffer should be added when estimating separation using a What If. This buffer accounts for the wind speed change between the “4D ADS-C EPP report” and the What If horizontal trajectory. The method illustrated in Figure 10 and Figure 11 could be applied for estimating this extra buffer	

1209

1210

1211 **4.3.5 Safety Requirements derived from EXE006 (PANSAs, INDRA)**

1212 In EXE006 ADS-C EPP data is used in order to improve the Trajectory Prediction of the FDPS.

1213 The ADS-C EPP data comes from the FMS part of the avionics. When the Flight is in “Full Managed
 1214 Mode” (Lateral, Vertical, Speed managed modes are ON), the FMS controls the flight profile completely
 1215 and optimally (in terms of Flight efficiency). But during the flight, ATCOs provide Radar vectoring and
 1216 issue clearances for various operational constraints requiring the aircraft to fly in less optimal flight
 1217 profile. To comply with ATCO instructions, pilots feed the instructions either into the FCU by selecting
 1218 the necessary flight parameters on his cockpit console resulting in “Selected Mode” (i.e combination
 1219 of single/multiple/all the modes of Lateral, Vertical & Speed managed as OFF) which is less optimal (in
 1220 terms of Flight efficiency) than that of “Full managed mode”, or directly in the FMS depending on the
 1221 clearance. When the flight is In “Selected Mode” (Partial/Full), the flight profile will comply with this
 1222 selection until the pilot deselects the already selected flight parameters on his cockpit console.

1223 In General, the trajectory of the Flight is computed by the FMS periodically along with the planned
 1224 trajectory (FMS predictions of overall future trajectory) and is downlinked through ADS-C Periodic
 1225 reports irrespective of whether the Aircraft is flying in Managed/Selected modes. If any considerable
 1226 change in trajectory takes place due to Pilot’s intervention while complying ATCO’s instructions, this
 1227 can result in ADS-C Event reports downlinked (it’s up to ground to set up conditions On-Event ADS-C
 1228 contract) which give all the information about the changed trajectory and its associated Flight
 1229 parameters (EPP included in some events). In addition, the status of the On-board individual Managed
 1230 modes (Lateral, Vertical & Speed) is always present in downlinked EPP.

1231 From the above description, it can be understood that the complete trajectory of a flight can be a
 1232 combination of Managed and selected modes during various phases of the flight. Considering this, it
 1233 becomes significant to guarantee the *validity* of the predictions provided in ADS-C EPP data in both
 1234 Managed and Selected modes. The word “validity” refers to the consistency of the predicted trajectory
 1235 with regards to the clearances provided by the ATCO. This validity is expressed both in terms of delay
 1236 and accuracy, since in compliance to the new ATCO open-loop clearance and its planning to reach final
 1237 destination, some delay may result in calculating the new predictions by the FMS, together with some
 1238 inaccuracy in the new predictions for the given time horizon of the ATCO unit.

1239 This analysis voluntarily remains at the operational level (since this work is in V2, and future safety
 1240 work will be done in V3), and does not claim any technical accuracy at that level.

1241 This safety aspect encompasses both the conflict Detection&Resolution and the Monitoring.

1242

Safety Objectives	Requirement	Maps on to
(Functionality and Performance from success approach)	and (forward reference)	

All SO depending on the context of use of the ADS-C EPP	SR_SO 05	ADS-C EPP Transmission
SO#012	SR_SO 06	ADS-C EPP Transmission

1243 **Table 22: Mapping of Safety Objectives to SPR-level Model Elements**

1244

Safety Requirement (functionality & performance) [SPR-level Element]	Requirement & Model	Derived from Table 4 to Table 8
SR_SO 10	The validity (in the sense of : consistency with regards to the cleared profile) of ADS-C EPP data when the flight is in Selected Mode should be guaranteed for using in ATCO Ground system tools. (To be considered for future V3 maturity validation phase)	All SO depending on the context of use of the ADS-C EPP
SR_SO 11	Controllers should be trained in order to keep in mind that aircraft may deviate without the “improved trajectory deviation Aid” being able to inform them	SO#012

1245 **Table 23: Derivation of Safety Requirements (functionality and performance) from Safety Objectives**

1246

1247 [...]

ID	Assumptions
	The Planning conflict detection aid tool shall be active at all CWPs at all times (SO#211).
	The Planning conflict resolution 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 (SO#212).
	The Tactical conflict detection aid tool shall be active at all CWPs at all times (SO#016).

1248 **Table 24: Assumptions made in deriving the above Safety Requirements**

1249 **4.3.6 Safety Requirements derived from EXE007 (BULATSA)**

1250 EXE007 uses both Mode S and ADS-C EPP data, so the Safety Requirements for EXE007 include both
 1251 the corresponding safety requirements already identified in the previous exercises.

1252 .

1253

Safety Objectives (Functionality and Performance from success approach)	Requirement (forward reference)	Maps on to
SO#012	SR_SO 04	Mode S
All SO depending on the context of use of the ADS-C EPP	SR_SO 05	ADS-C EPP data transmission
SO#012	SR_SO 6	ADS-C EPP data transmission

1254 **Table 25: Mapping of Safety Objectives to SPR-level Model Elements**

1255 In order to make a valid use of the Mode S data, the Combined Trajectory Predictor should verify that
 1256 the Mode S fields used by the algorithmic are available and valid (as explained, for instance, in
 1257 Appendix A2 of Reference [10]).

Safety Requirement (functionality & performance) [SPR-level Model Element]	Requirement	Derived from Table 4 to Table 8
SR_SO 12	When Mode S is used for trajectory deviation detection, The Monitoring Aid should ensure that the Mode S fields are available and valid	SO#012
SR_SO 13	The validity (in the sense of : consistency with regards to the cleared profile) of ADS-C EPP data when the flight is in Selected Mode should be guaranteed for using in ATCO Ground system tools. (To be considered for future V3 maturity validation phase)	All SO depending on the context of use of the ADS-C EPP

SR_SO 14	Controllers should be trained in order to keep in mind that aircraft may deviate without the “improved trajectory deviation Aid” being able to inform them	SO#012

1258 **Table 26: Derivation of Safety Requirements (functionality and performance) from Safety Objectives**

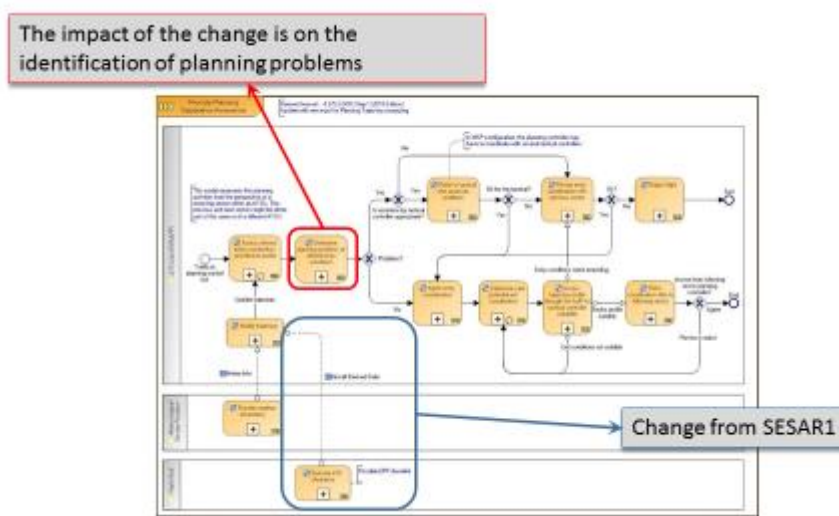
1259

1260 **4.4 Analysis of the SPR-level Model – Normal Operational**
 1261 **Conditions**

1262 **4.4.1 Context of the Analysis**

1263 This subsection complements the functional and logic descriptions, which were more focused on the
 1264 exchange of data between the different actors. Here, the focus is not so much on the exchange of data,
 1265 but rather on the sequence of events occurring in the different scenarios. The scenarios are those
 1266 described in the Use Cases of the OSED.

1267 If we consider the description of the Operational Service “Provide Planning Separation Assurance”
 1268 from the OSED, we have for the Planner Controller:



1269

1270 **Figure 12**

1271 The only change from SESAR1 is the Aircraft Derived Data which will possibly modify the trajectory
 1272 prediction, and impact the determination of planning problems. So the change from SESAR1 is not on
 1273 the working methods or on the features of the ATC Tools. In other words, if we follow the OSED
 1274 diagram illustrated in Figure 12, the change from SESAR1 is “transparent” from the ATCO, which will
 1275 keep on using the same tools with the same functionalities and the same working methods, so there
 1276 is no need to analyse any further the scenarios. We have the same conclusion for the Tactical

1277 Controller, where the change from SESAR1 is also on the provision of Aircraft Derived Data which will
 1278 possibly impact on the determination of problems (see Figure 13).

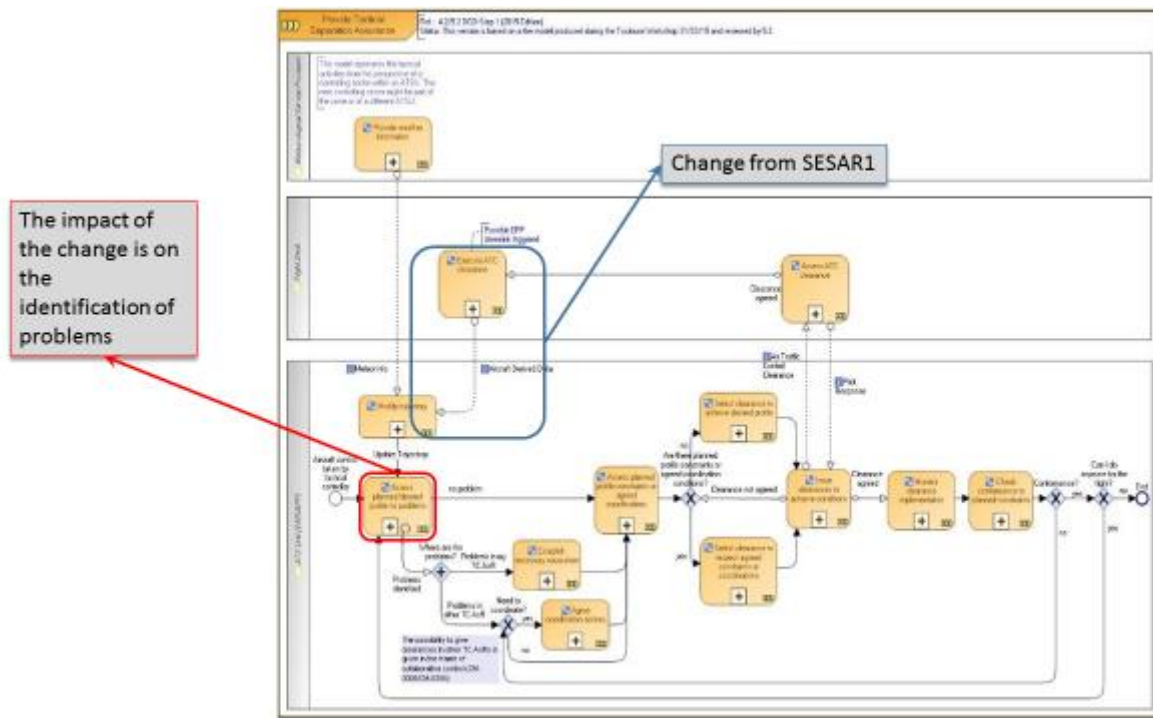


Figure 13

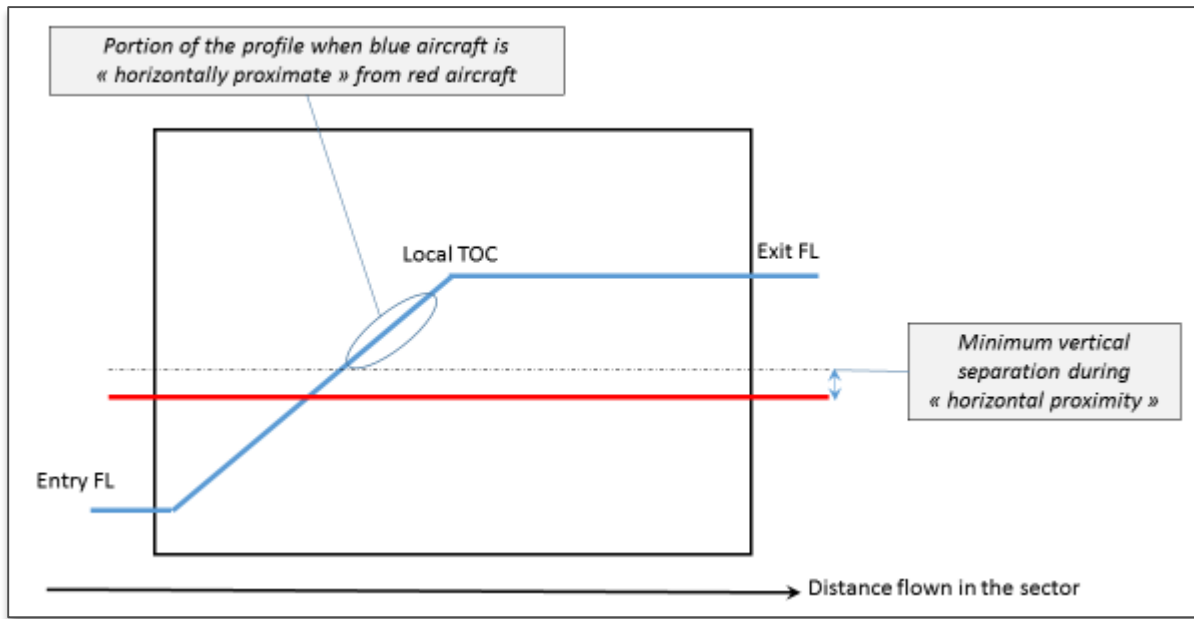
1279
 1280
 1281 So, in the case of Exercises using ADS-C EPP data, there is no rationale for detailing the scenarios, since
 1282 they are similar to those already studied in SESAR1.

1283 There is, however, an opportunity of use for the thread analysis, when the ATCO working methods
 1284 have been modified accordingly with the ATC tools. This is the case for the EXE001.

1285 4.4.2 Analysis for EXE001

1286 4.4.2.1 Description of the MTCD algorithm modification

1287 In EXE001, it was decided to modify the MTCD algorithm in order to reduce the identification of “false
 1288 positive” planning problems. The baseline MTCD uses a classical trajectory prediction, where the
 1289 aircraft is expected to climb as soon as possible and to descend as late as possible. Figure 14 illustrates
 1290 the determination of a planning problem between an entering flight (in blue) expected to climb (exit
 1291 FL greater than entry FL) and a steady flight (in red). The MTCD algorithm determines for both flight
 1292 profiles the “portions of horizontal proximity”, together with the minimal vertical separation during
 1293 the horizontal proximity, and if this minimal vertical separation is below a threshold then the algorithm
 1294 identifies a planning conflict.



1295

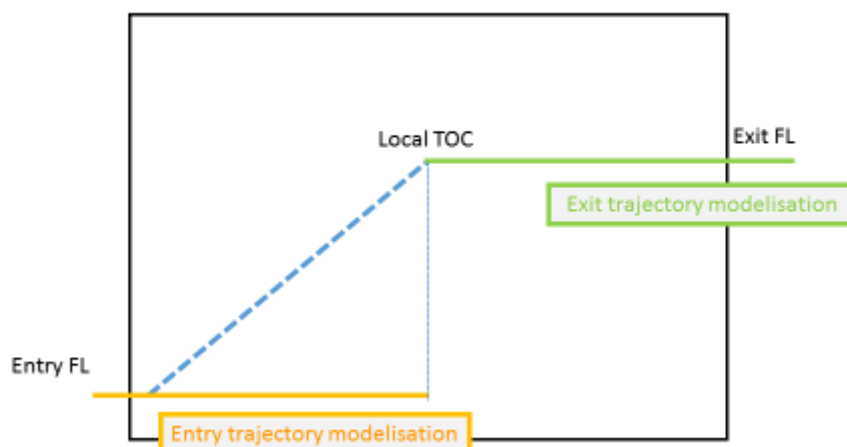
1296

Figure 14

1297 The solution MTCD tested in EXE001 uses a different modelisation for the trajectory of the entering
 1298 flight. Instead of “assuming” that the flight will start climbing as soon as it enters the sector (as
 1299 represented in Figure 14 for the baseline MTCD), the solution MTCD computes its own calculation
 1300 according to two steady modelisations:

- 1301 – One entry modelisation, steady at the Entry FL;
- 1302 – One exit modelisation, steady at the Exit FL.

1303 The end of the entry modelisation and the beginning of the exit modelisation correspond to the point
 1304 of Top Of Climb, as illustrated in Figure 15.



1305

1306

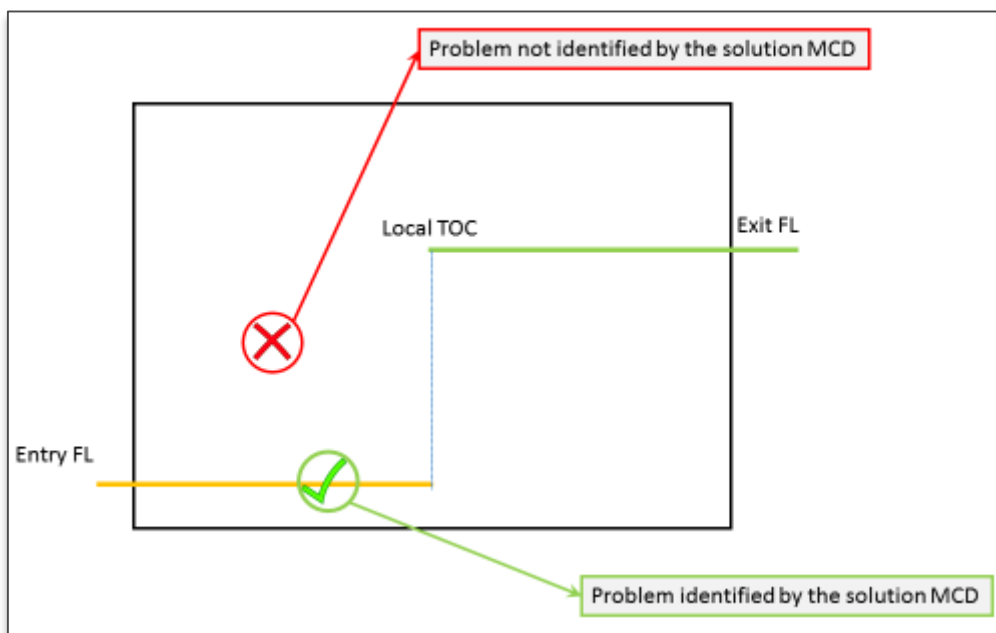
Figure 15

1307

1308 In summary, the solution MTCD doesn't take into consideration climbing (resp descending) portions of
1309 the trajectory, and replaces them by steady portions, at the Entry FL (resp Exit FL).

1310 The consequences of this modelling are illustrated in Figure 16. When identifying planning problems
1311 with the entering aircraft, the solution MTCD identifies problems with aircraft which are steady at the
1312 Entry FL, but does not identify problems with all aircraft which could be interfering during the climbing
1313 phase between the Entry FL and the exit FL. The rationale for that choice is that the problems which
1314 are not identified by the solution MTCD on Figure 16 (the red ones) are not real problems, since the
1315 aircraft has not been yet cleared to climb. If the ATCO keeps the entering aircraft steady at the Entry
1316 FL, these problems are "false positive detections" by the MTCD. However, if the aircraft is not cleared
1317 to climb and remains at the Entry FL, then the problems which are identified by the solution MTCD on
1318 Figure 16 (the green ones) are real problems, in the sense that the entering aircraft will actually have
1319 conflict with the corresponding aircraft if it keeps at the Entry FL.

1320 In summary, the choice of modelling for the solution MTCD is to limit the identification of MTCD
1321 problems to a scenario where the aircraft is not cleared to climb as soon as possible. It was expected
1322 that this choice of modelling would lead to a reduction of the number of false identification by the
1323 MTCD.



1324

1325

Figure 16

1326 The length of the Entry trajectory modelisation corresponds, as we saw in Figure 15, to the duration
1327 required for the aircraft to climb towards its Exit FL. This length corresponds to an "anticipation
1328 threshold" for identifying problems with other aircraft which would be steady at the Entry FL. As the
1329 entering aircraft proceeds without being cleared to climb, this "anticipation threshold" remains
1330 unchanged, in the sense that the solution MTCD updates the Entry trajectory modelisation accordingly,
1331 as illustrated on Figure 17.

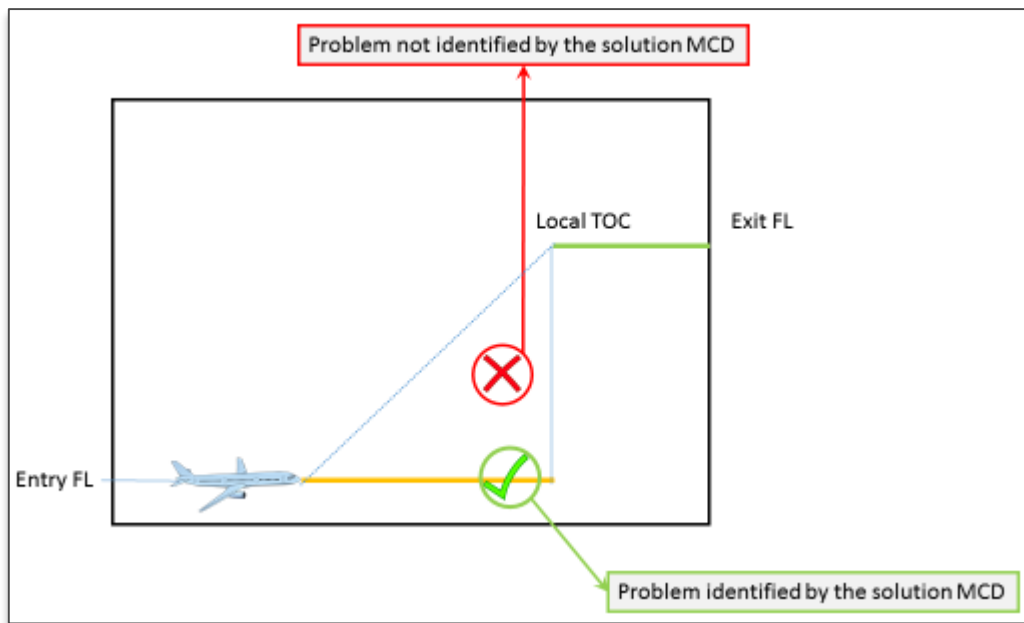


Figure 17

1332

1333

1334 4.4.2.2 Consequence on the ACTO working method

1335 The consequences are mostly for the Tactical Controller. The MTCD alarms are displayed on his HMI
 1336 and do not include problems which could occur on the vertically evolutive part of its trajectory, for
 1337 entering aircraft expected to climb (resp descend). The consequence is that, when the Tactical
 1338 controller clears an aircraft to climb so as it joins its Exit Flight Level, he should use the What If, since
 1339 he has not been warned by the MTCD of any possible problem associated by the climbing clearance.
 1340 Of course the Tactical Controller is expected to perform his own detection task prior to the clearance
 1341 delivery, with support of analysis services (like the ERATO filtering tool for instance). But in order to be
 1342 fully “protected by the system”, each CFL should be checked manually with the what-if service just
 1343 before relaying the CFL clearance to the aircraft. Normally the ATCO mental image and the what-if
 1344 result should be consistent. If it is not the case, it means that the mental image of the ATCO is
 1345 erroneous, and that an additional analysis is required.

1346 4.4.2.3 Scenarios for EXE001 for Normal Operations

1347 *Extract the Normal Operational Scenarios from the OSED and capture them in Table 17.*

1348 4.4.2.4

ID	Scenario	Rationale for the Choice
1	Tactical Controller which clears aircraft to climb to Exit Flight Level	For this scenario, MTCD alarms associated to the climb were not played beforehand

1349 **Table 27: Operational Scenarios for EXE001 – Normal Conditions**

1350 **4.4.2.5 Additional Safety Requirements for EXE001**

1351

Safety Requirement derived from Scenarios for Normal Operations of EXE001	Requirement	Scenario ID
SR_001_1	When a Tactical Controller issues a clearance of climb/descent to (or toward) the Exit FL, he should beforehand check with the What If that this clearance does not create any tactical problem.	EXE001 Scenario 1

1352 **Table 28: Additional Safety Requirement from Scenarios for Normal Operations for EXE001**

1353 **4.5 Analysis of the SPR-level Model – Abnormal Operational**
 1354 **Conditions**

1355 Abnormal Operational Conditions have been listed in Section 3.8, and mitigations have been set for all
 1356 cases, without requiring any specific requirement.

1357 **4.6 Design Analysis – Case of Internal System Failures**

1358 **4.6.1 Causal Analysis**

1359 **4.6.1.1 Causal Analysis for EXE001 and EXE002**

1360 Similarly to what we wrote in §4.2.2, there is no causal analysis to perform for these two EXE since
 1361 there is no external cause to the failure of the ATC tools.

1362 **4.6.1.2 Causal Analysis for EXE003**

1363 The use of Mode S data for both the trajectory prediction and the trajectory deviation detection
 1364 creates new causes for occurrence of hazards associated to these functions.

1365 **4.6.1.3 Causal Analysis for EXE004 and EXE005**

1366 The use of Mode S data for trajectory deviation detection creates new causes for occurrence of hazards
 1367 associated to these functions, but only for nuisance alarms.

1368 A CPDLC message issued by the Planner Controller not displayed on the Tactical HMI might cause the
 1369 Tactical controller to miss a conflict detection, but this would be detected by the TCT. Similarly, a CPDLC
 1370 message issued by the Tactical Controller not displayed on the Planner HMI might cause the Planner
 1371 controller to issue an induced pre-tactical conflict, which will result in an extra workload for the Tactical
 1372 Controller.

1373 **4.6.1.4 Causal Analysis for EXE006**

1374 The use of Mode S data for both the trajectory prediction and the trajectory deviation detection
 1375 creates new causes for occurrence of hazards associated to these functions.

1376 **4.6.1.5 Causal Analysis for EXE007**

1377 The use of Mode S data for both the trajectory prediction and the trajectory deviation detection
1378 creates new causes for occurrence of hazards associated to these functions.

1379 The use of ADS-C EPP data for both the trajectory prediction and the trajectory deviation detection
1380 creates new causes for occurrence of hazards associated to these functions.

1381 **4.6.2 Common Cause Analysis**

1382 **4.6.2.1 Common Cause analysis for EXE003**

1383 As can be seen on Figure 3, the Mode S data are used both for Conflict Detection (TCT, MTC) and for
1384 Conflict Resolution (What If), so it is necessary here to get detailed information on the Mode S data
1385 parameters used, in order to identify possible scenarios of common cause error involving both the
1386 Planner and the Executive.

1387 **4.6.2.2 Common Cause analysis for EXE004 and EXE005**

1388 The level of refinement of the SPR model did not allow identification of common causes.

1389 **4.6.2.3 Common Cause analysis for EXE006**

1390 The level of refinement of the SPR model did not allow identification of common causes.

1391 **4.6.2.4 Common Cause analysis for EXE007**

1392 The level of refinement of the SPR model did not allow identification of common causes.

1393 **4.6.3 Safety Requirements (integrity/reliability)**

1394 **4.6.3.1 Safety Requirements for EXE003**

1395 In the table below, the hazard described in the description column should not occur more often than
1396 the probability identified in the Severity column. The operational effects and mitigation effects column
1397 explain at which barrier this hazard is mitigated.

1398

ID	Description	Related Hazards	Operational Effects	Mitigations of Effects	Severity (most probable effect)
	CPDLC message issued by TC not displayed on PC HMI	H2002	The Planner Controller may create an induced pre-tactical conflict, causing an extra workload for the Tactical Controller	TC Aid will eventually pick up encounter.	MAC-SC4b
	CPDLC message issued by PC	H2001 mitigated	The Tactical controller is not aware of a change of profile for an incoming	CD/R Aid for TC will detect the TC error, and allow	MAC-SC4b

	not displayed on TC HMI		flight, so he may create induced conflicts, or miss actual tactical conflicts	him to solve it, causing only an extra workload	
	Undetected corrupted Mode S data	Hz006 Hz007	There are two possible effects. Firstly, a nuisance alarm may occur. Secondly, in the case of a real trajectory deviation with corrupted Mode S data which would not allow to detect it in advance, the MONA would still work but with some delay, so that the overall effect would be a loss of the “early detection” (before even the start of the deviation).		

1399

1400

ID	Description
	Corruption of Mode S data MAC-SC3
	MTCD Loss is less frequent than the probability described by MAC-SC4b
	TCT Loss is less frequent than the probability described by MAC-SC3

1401

4.6.3.2 Safety Requirements for EXE004 and EXE005

ID	Description	Related Hazards	Operational Effects	Mitigations of Effects	Severity (most probable effect)
	CPDLC message issued by TC not displayed on PC HMI	Hz002	The Planner Controller may create an induced pre-tactical conflict, causing an extra workload for the Tactical Controller	TC Aid will eventually pick up encounter.	MAC-SC4b
	CPDLC message issued by PC	Hz001 mitigated	The Tactical controller is not aware of a change of profile for an incoming	CD/R Aid for TC will detect the TC error, and allow	MAC-SC4b

	not displayed on TC HMI		flight, so he may create induced conflicts, or miss actual tactical conflicts	him to solve it, causing only an extra workload	
	Undetected corrupted Mode S data	Hz006 Hz007	There are two possible effects. Firstly, a nuisance alarm may occur. Secondly, in the case of a real trajectory deviation with corrupted Mode S data which would not allow to detect it in advance, the MONA would still work but with some delay, so that the overall effect would be a loss of the “early detection” (before even the start of the deviation).		

1402

ID	Description
	CPDLC message issued by TC not displayed on PC HMI is less frequent than the probability described by MAC-SC4b
SR_INT_5	CPDLC message issued by PC not displayed on TC HMI is less frequent than the probability described by MAC-SC4b
	Mode S data does not become corrupted

1403

4.6.3.3 Safety Requirements for ADS-C EPP (integrity/reliability)

1404

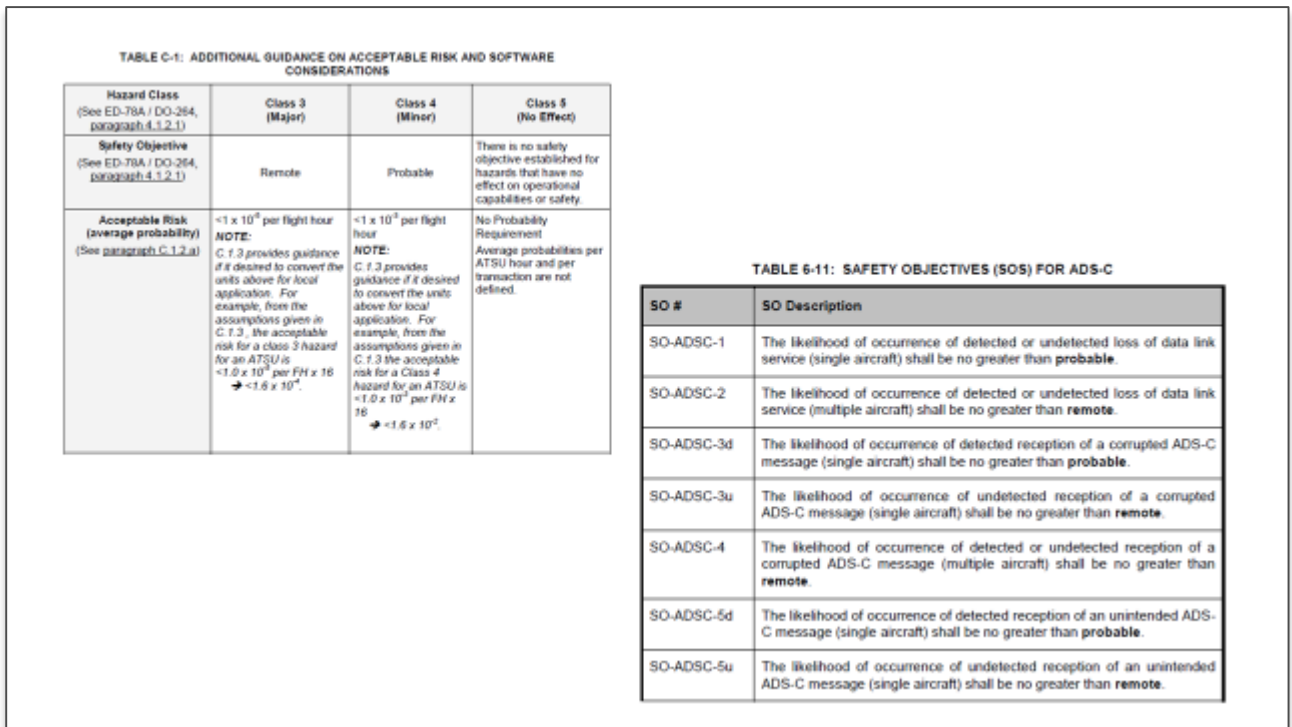
The EUROCAE ED-228A (Ref [12]) is the standard of reference related to ADS-C and ADS-C EPP (We recall that EPP is provided by ADS-C). Appendix B of [12] provides a detail set of requirements for the definition of the ADS-C EPP data. Section 6.3 of this document provides all safety and performance requirements related to ADS-C. We reproduce in Figure 18 the integrity requirement for an undetected corruption of the ADS-C EPP data, as defined in ED-228A.

1405

1406

1407

1408

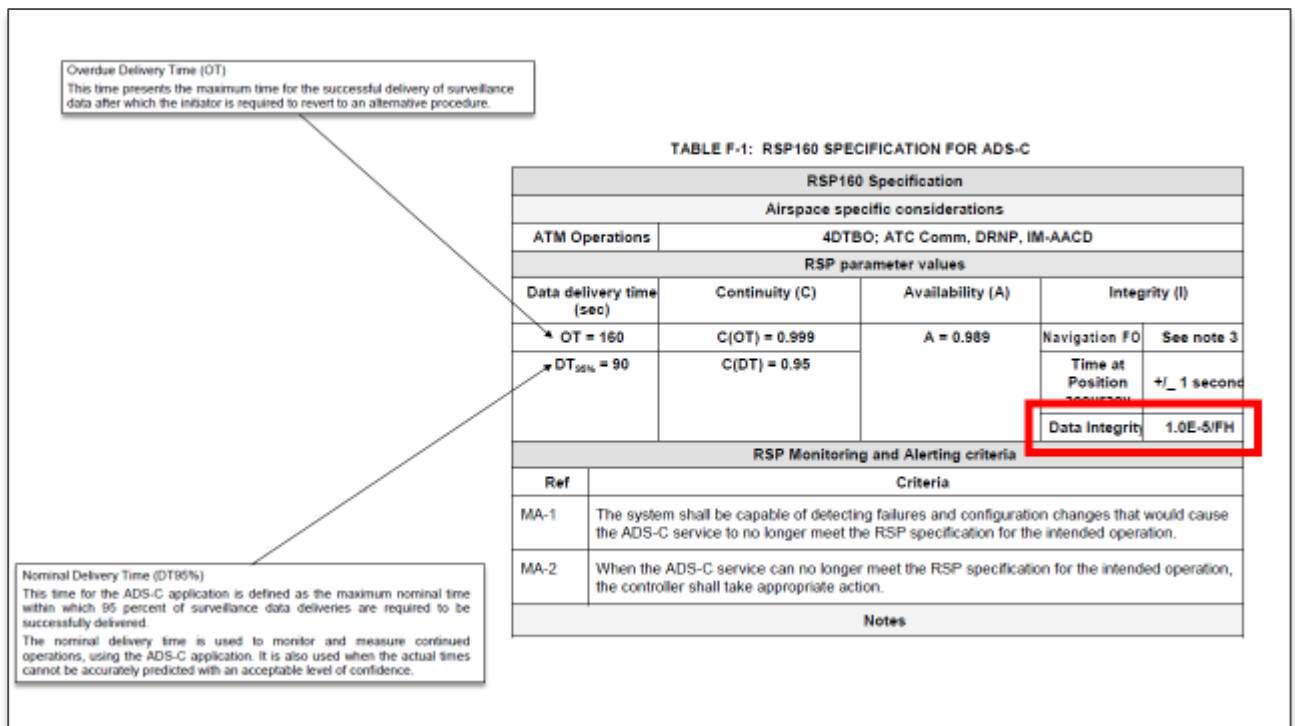


1409

1410

Figure 18

1411 It is also interesting to note the D-228A requirements based on the delivery time for an ADS-C message,
 1412 which is detailed in Figure 19



1413

1414

Figure 19

1415 We notice that the only requirement for the delivery time is for its 95% quantile, DT_{95%}, which is 90
 1416 seconds. In order to approximate a “best average” delivery time, we consider a distribution of positive
 1417 quantities which over weights the tail of the distribution, typically an exponential distribution (known
 1418 to have the heaviest tail). For such a distribution, the 95% quantile suffices to know the mean delivery
 1419 time, by using:

1420

$$e^{-\frac{90}{D}} = 0.05$$

1421

So that $D = \frac{-90}{\ln(0.05)} \cong 30$ seconds. So, an “optimistic” average delivery time is of 30 seconds. As an
 1422 illustration of that, we display in different distributions verifying the criterion DT_{95%}=90 seconds, from
 1423 the Gamma family. Gamma(1) corresponds to the exponential distribution, and Gamma(n) may be
 1424 seen as the sum of n independent exponential distributions. Gamma(n) for integer n is also called an
 1425 Erlang distribution and is widely using in queuing theory, for modelling waiting times.

Candidate distributions verifying DT95% = 90 seconds

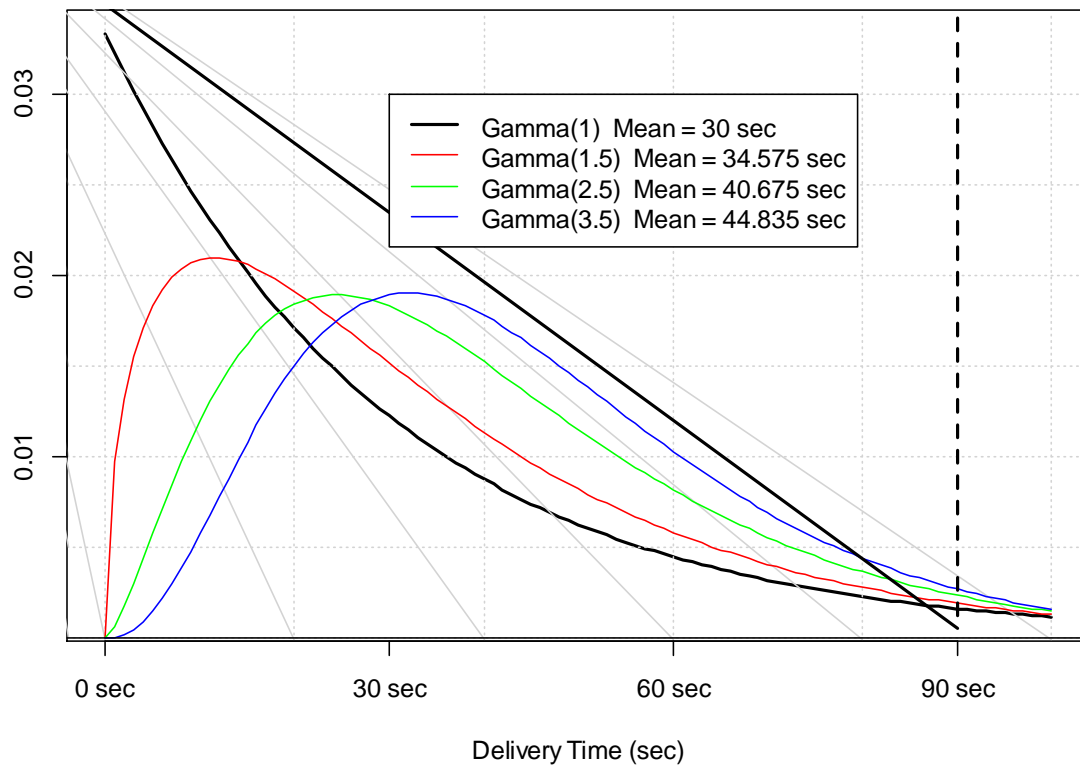


Figure 20

1426

1427

1428

1429 The delivery time has not been tested during the PJ10.02A since all exercises using ADS-C EPP used
 1430 simulated data (without considering ADS-C transmission time). As a consequence, we have not
 1431 expressed any requirement on this subject. Nevertheless, the mean delivery times illustrated in Figure
 1432 20 should be noted, and more particularly the fact that the mean transmission time is always expected
 1433 to exceed 30 seconds.

1434 **4.6.3.4 Safety Requirements for EXE006**

ID	Description	Related Hazards	Operational Effects	Mitigations of Effects	Severity <i>(most probable effect)</i>
	Corruption of ADS-C EPP data	Possibly all hazards Hz001 to	The tool misleads the controller into missing a tactical conflict, or a nuisance alarm	Executive controller picks up encounter from radar scan. Other tools (STCA etc.) can help.	MAC-SC3

		Hz005			
--	--	-------	--	--	--

1435

ID	Description
	Corruption of ADS-C EPP data MAC-SC3

1436

1437 It should be noted that severity of the hazard above is MAC-SC3, which is more stringent than the value
 1438 provided by EUROCAE ED-228A (see Figure 18 and the value of MAC-SC3 in section 3.9.2).

1439 **4.6.3.5 Safety Requirements for EXE007**

ID	Description	Related Hazards	Operational Effects	Mitigations of Effects	Severity (most probable effect)
	Corruption of ADS-C EPP data	Possibly all hazards Hz001 to Hz005	The tool misleads the controller into missing a tactical conflict, or a nuisance alarm	Executive controller picks up encounter from radar scan. Other tools (STCA etc.) can help.	MAC-SC3
	Corruption of Mode S data	Possibly all hazards Hz001 to Hz005	The tool misleads the controller into missing a tactical conflict, or a nuisance alarm	Executive controller picks up encounter from radar scan. Other tools (STCA etc.) can help.	MAC-SC3

1440

ID	Description
	Corruption of ADS-C EPP data MAC-SC3
	Corruption of Mode S data is less frequent than the probability described by MAC-SC3

1441



1442 It should be noted that severity of the hazard above is MAC-SC3, which is more stringent than the value
1443 provided by EUROCAE ED-228A (see Figure 18 and the value of MAC-SC3 in section 3.9.2).

1444

1445

1446

5 Detailed Safe Design at Physical Level

1447

No safety activity has been done at that level within PJ10.02A, since we have not been granted the level of technical detail which would have been required for that purpose.

1448

1449

1450

6 Acronyms and Terminology

1451

Term	Definition
2D, 3D, 4D	Two Dimensional, Three Dimensional, Four Dimensional
A/C	<i>Aircraft</i>
ACARS	<i>Aircraft Communications Addressing and Reporting System</i>
ACAS	<i>Airborne Collision Avoidance System</i>
ACC	Area Control Centre
ADS-B	<i>Automatic Dependent Surveillance-Broadcast</i>
ADS-C	<i>Automatic Dependent Surveillance-Contract</i>
AIM	<i>Accident Incident Model</i>
AN	Availability Note
ANSP	Air Navigation Service Provider
AOI	Area of Interest
AOR	Area of Responsibility
ATC	Air Traffic Control
ATCO	Air Traffic Controller
ATFCM	Air Traffic Flow and Capacity Management
ATM	Air Traffic Management
ATM MP	Air Traffic Management Master Plan
ATS	Air Traffic Service
ATSAW	Airborne Traffic Situation Awareness
ATSU	Air Traffic Service Unit
BADA	Base of Aircraft Data
CAS	Collision Avoidance System
CB	Cumulonimbus (Storm Cloud)

CD/R	Conflict Detection and Resolution
CDU	Controller Display Unit
CFIT	Controlled Flight Into Terrain
CFL	Cleared (Current) Flight Level
CM	Conflict Management
CNS	<i>Communications, Navigation and Surveillance</i>
CPDLC	<i>Controller-Pilot Data Link Communication</i>
CWP	Controller Working Position
DCB	Demand Capacity Balancing
DSS	Decision Support System
EATMA	European ATM Architecture
E-ATMS	European Air Traffic Management System
EC	European Commission
EC	Executive Controller
EFPL	Extended Flight Plan
E-OCVM	European Operational Concept Validation Methodology
EPP	Extended Projected Profile
ER	En-Route
ERATO	En-Route Air Traffic Organizer
ESF	Energy Share Factor
EUROCAE	European Organisation for Civil Aviation Equipment
EXE	Exercise
FCU	Flight Control Unit
FDPS	Flight Data Processing System
FL	Flight Level
FM	Flow Management
FMP	Flow Management Planning

FMS	Flight Management System
FTS	Fast Time Simulation
GA	General Aviation
GPS	Global Positioning System
GS	Ground Speed
HAZID	Hazard Identification
HMI	Human-Machine Interface
HPAP	Human Performance Assessment Plan
ICAO	International Civil Aviation Organisation
IFR	Instrument Flight Rules
INTEROP	Interoperability Requirements
LOA	Letter of Agreement
MAC	Mid Air Collision
Mode S	Transponder S mode
MONA	Monitoring Aids
MTCD	Medium Term Conflict Detection
MTFoO	Maximum Tolerable Frequency of Occurrence
NEXTGEN	Next Generation Transportation System
NM	Network Mangement
NoTT	No Valid Flight Plan Data Available
OE	Operational Environment
OFA	Operational Focus Area
OI	Operational Improvement
OPLINK	Operational Data Link
OSED	Operational Service and Environment Definition
PC	Planner Controller
RATE	Vertical Deviation Rate

ROCD	Rate of climb/descent
ROUTE	Route (deviation)
RTCA	Radio Technical Commission for Aeronautics
RTS	Real Time Simulation
RWY	Runway
SAC	Safety Criteria
SAP	Safety Assessment Plan
SAR	Safety Assessment Report
SC	Safety Criteria
SeAP	Security Assessment Plan
SESAR	Single European Sky ATM Research Programme
SHAPE	Solutions for Human Automation Partnerships in European ATM
SJU	SESAR Joint Undertaking (Agency of the European Commission)
SO	Safety Objective
SPD	Speed Deviation
SPR	Safety and Performance Requirements
SRM	Safety Reference Manual
STCA	Short Term Collision Avoidance
STCA	Short Term Conflict Alert
SUT	System Under Test
SWIM	System Wide Information Model
TAS	True Air Speed
TC	Tactical Controller
TCT	Tactical Controller Tool
TMA	Terminal Manoeuvring Area
ToC	Top of Climb
ToD	Top of Descent

TP	Trajectory Prediction or Tactical Planner
TS	Technical Specification
TTM	Tactical Trajectory Module
TWY	Taxiway
UC	Use Case
VALP	Validation Plan
VALR	Validation Report
VALS	Validation Strategy
VFR	Visual Flight Rules
WP	Work Package

1452 **Table 29: Acronyms and terminology**

1453

7 References

1454 [Safety](#)

- 1455 [1] SESAR, Safety Reference Material, Edition 4.0, April 2016
- 1456 [2] SESAR, Guidance to Apply the Safety Reference Material, Edition 3.0, April 2016
- 1457 [3] SESAR Safety Assessment Plan Template
- 1458 [4] SESAR Solution XX Safety Plan
- 1459 [5] SESAR, Final Guidance Material to Execute Proof of Concept, Ed00.04.00, August 2015
- 1460 [6] SESAR, Resilience Engineering Guidance, May 2016
- 1461 [7] SESAR Solution PJ10-02a : SPR-INTEROP/OSED for V2 - Part I, November 2018
- 1462 [8] SESAR Solution PJ10-02a : SPR-INTEROP/OSED for V2 - Part II - Safety Assessment Report (SAR),
1463 August 2018
- 1464 [9] Accident Incident Model Version 10-3, December 2015
- 1465 [10] ICAO Doc 9871, Technical Provisions for Mode S Services and Extended Squitter, First Edition,
1466 2008
- 1467 [11] SESAR Solution PJ.10-02a initial SPR-INTEROP/OSED for V3 - Part I
- 1468 [12] EUROCAE ED-228A (Safety And Performance Requirements Standard For Baseline 2 ATS Data
1469 Communications (Baseline 2 SPR Standard), March 2016
- 1470 [13] User Manual For The Base of Aircraft Data (BADA) Revision 3.15, EEC Technical/Scientific
1471 Report No. 19/03/18-45, May 2019

1472 **Appendix A Safety Objectives**

1473 **A.1 Safety Objectives (Functionality and Performance)**

ID	Safety Objective (Functionality and Performance)	Traceability (Operational Service)
SO#21	The Planning conflict detection aid shall indicate pairs of aircraft which have planning encounters at the entry or exit sector boundary.	OS 1
SO#201	Planning conflict detection aid calculations should permit to display an encounter even if one aircraft is outside the sector (AOI crossing).	OS1, OS2
SO#211	The Planning conflict detection aid tool shall be active at all CWPs at all times.	OS1, OS2
SO#22	The Planning conflict resolution aid shall identify planning encounters in proposed resolutions.	OS2,
SO#23	The Planning conflict resolution aid shall detect planning encounters which would involve the subject flight for all sector coordination entry and exit levels.	OS2
SO#29	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.	OS2
SO#212	The Planning conflict resolution 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.	OS2
SO#11	The Tactical conflict detection 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.	OS3
SO#14	TC Aid shall support the TC to correctly prioritise and resolve conflicts indicated to the ATCO by TC aid in a timely way.	OS3, OS4
SO#16	The Tactical conflict detection aid tool shall be active at all CWPs at all times.	OS4, OS5, OS6
SO#13	For the subject aircraft the Tactical conflict resolution aid shall identify conflicts for any probed clearances.	OS4
SO#15	The Tactical conflict resolution aid shall detect Tactical encounters which would involve the subject flight for all flight levels within the sector.	OS4
SO#12	The Conformance monitoring aid shall indicate the following deviations between an aircraft's known position and predicted trajectory:	OS5

ID	Safety Objective (Functionality and Performance)	Traceability (Operational Service)
	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)	
SO#24	The Conformance monitoring aid shall monitor aircraft's achievability to meet entry and exit coordination.	OS5
SO#27	The Conformance monitoring aid shall detect deviations from each flights entry and exit conditions.	OS5

1474

1475

1476

A.2 Safety Objectives (Integrity)

ID	Safety Objective (Integrity)	Traceability
Hz001SO00 x	The frequency of occurrence of Hz001 - CD/R aid to PC misleads the controller which fails to take action shall not be greater than $1.67 \cdot 10^{-4}$ (/flt hr).	Hz 001
Hz002SO00 x	The frequency of occurrence of Hz 002 CD/R aid to PC misleads the controller and increases workload shall not be greater than $1.67 \cdot 10^{-4}$ (/flt hr).	Hz 002
Hz004SO00 x	The frequency of occurrence of Hz 004 CD/R aid to PC suffers a detected failure shall not be greater than $1.67 \cdot 10^{-4}$ (/flt hr).	Hz 004
Hz005SO00 x	The frequency of occurrence of Hz 005 CD/R aid to PC misunderstood by the controller shall be no greater than $1.67 \cdot 10^{-4}$ (/fl hr).	Hz 005
Hz006SO00 x	The frequency of occurrence of Hz 006 CD/R aid to TC misleads the controller shall be no greater than $2 \cdot 10^{-6}$ (/fl hr).	Hz 006
Hz0071SO0 0x	The frequency of occurrence of Hz 007 CD/R aid to TC presents nuisance alerts shall be no greater than $2 \cdot 10^{-6}$ (/fl hr).	Hz 007
Hz008SO00 x	The frequency of occurrence of Hz 008 CD/R aid to TC presents nuisance resolution shall be no greater than $2 \cdot 10^{-6}$ (/fl hr).	Hz 008
Hz009SO00 x	The frequency of occurrence of Hz 009 CD/R aid to TC suffers a detected failure shall be no greater than $2 \cdot 10^{-6}$ (/fl hr).	Hz 009
Hz0010SO0 0x	The frequency of occurrence of Hz 010 CD/R aid to TC misunderstood by the controller shall be no greater than $1.67 \cdot 10^{-4}$ (/fl hr).	Hz 010

ID	Safety Objective (Integrity)	Traceability
Hz0011SOO 0x	The frequency of occurrence of Hz 011 Failure of the “improved part” Trajectory deviation aid shall be no greater than 1.67×10^{-5} (/fl hr).	Hz 011
Hz0012SOO 0x	The frequency of occurrence of Hz 012 The trajectory deviation aid causes a nuisance alarm shall be no greater than 1.67×10^{-5} (/fl hr).	Hz 012

1477

1478

1479 **Appendix B Consolidated List of Safety Requirements**

1480 Safety Requirements (Functionality and Performance)

SR REF	Safety Requirement (functionality & performance)
SR_SO 01	If the ATC Tools make use of a “combined Trajectory Prediction” (which integrates the FDPS TP together with Mode S data from the avionics), the combined TP shall check that the avionics Mode S data are available and valid.
SR_SO 02	Only MTCD alerts (CD for the PC) corresponding to a predicted loss of both vertical and horizontal separation minima shall be displayed on the track label of the flight tracks involved in the conflict.
SR_SO 03	When the PC uses the What-if function (C/R for the PL) to check if a given FL change or Route change is conflict free, the visualization of the outcome shall be provided as close as possible to the HMI area where the request was issued (e.g. in the track label), in order to minimize the risk that the PC will spend too much time to check the validity of the proposed change.
SR_SO 04	When receiving a conflict resolution proposal (either FL change or Route change) via the What-if functionality (C/R for the EC), the EC shall be able to implement/reject the proposal using an HMI feature located as close as possible to the affected flight (e.g. in the track label), in order to minimize the risk of spending too much time before implementing/rejecting the conflict resolution.
SR_SO 05	Only TCT alerts (C/D for the EC) corresponding to a predicted loss of both vertical and horizontal separation minima shall be displayed on the track label of the flight tracks involved in the conflict.
SR_SO 06	When the EC uses the What-if function (C/R for the EC) to check if a given FL change or Route change is conflict free, the visualization of the outcome shall be provided as close as possible to the HMI area where the request was issued (e.g. in the track label), in order to minimize the risk that the EC will spend too much time to check the validity of the proposed change.
SR_SO 07	When CPDLC is used by controllers, the Human Machine Interface should display the CPDLC clearance to the “other” controller so that he keeps informed of the CPDLC message sent by his colleague
SR_SO 08	When CPDLC is used, controllers should limit it to conflict resolutions which are not time critical
SR_SO 09	When Mode S is used for trajectory deviation detection, The Monitoring Aid should ensure that the Mode S fields are available and valid

SR REF	Safety Requirement (functionality & performance)
SR_EPP_1	For a steady aircraft flying towards a waypoint, the improvement of trajectory prediction by using ADS-C EPP will be made preferably using method 1) above rather than method 2), provided that both methods are possible.
SR_EPP_2	For an evolutionary aircraft flying towards a waypoint, the improvement of trajectory prediction by using ADS-C EPP can be achieved by considering algorithmic means, such as the one explained in §4.3.4.2 (provided that its implementation is made possible by the FDPS architecture.).
SR_EPP_3	<p>For an aircraft which does not fly toward a waypoint, the improvement of trajectory prediction by using ADS-C EPP can be achieved by considering algorithmic means, such as the one explained in §4.3.4.3, after determining that the accuracy requirements are met by the ADS-C EPP data (To be considered during Future V3 Validation phase).</p> <p>If such an algorithm was to be used at the operational level for a planning purpose, caution should be taken to properly ensure that the computation of the predicted trajectory takes into account operational constraints impacting the future of the flight profile (such as the Letters Of Agreement). This is to be considered during future V3 validation phase</p>
SR_EPP_4	When extrapolating a trajectory prediction using the ADS-C EPP report for a What If, the algorithm should consider the wind, as explained previously. If this enhancement is not possible, an additional buffer should be added when estimating separation using a What If. This buffer accounts for the wind speed change between the “4D ADS-C EPP report” and the What If horizontal trajectory. The method illustrated in Figure 10 and Figure 11 could be applied for estimating this extra buffer
SR_SO 10	The validity (in the sense of : consistency with regards to the cleared profile) of ADS-C EPP data when the flight is in Selected Mode should be guaranteed for using in ATCO Ground system tools. (To be considered for future V3 maturity validation phase)
SR_SO 11	Controllers should be trained in order to keep in mind that aircraft may deviate without the “improved trajectory deviation Aid” being able to inform them
SR_SO 12	<p>When Mode S is used for trajectory deviation detection,</p> <p>The Monitoring Aid should ensure that the Mode S fields are available and valid</p>
SR_SO 13	The validity (in the sense of : consistency with regards to the cleared profile) of ADS-C EPP data when the flight is in Selected Mode should be guaranteed for using in ATCO Ground system tools. (To be considered for future V3 maturity validation phase)
SR_SO 14	Controllers should be trained in order to keep in mind that aircraft may deviate without the “improved trajectory deviation Aid” being able to inform them

SR REF	Safety Requirement (functionality & performance)
SR_001_1	When a Tactical Controller issues a clearance of climb/descent to (or toward) the Exit FL, he should beforehand check with the What If that this clearance does not create any tactical problem.

1481

1482 **B.1 Safety Requirements (Integrity)**

1483 No Safety Requirements related to Integrity have been identified.

ID	Description
	Corruption of Mode S data MAC-SC3
	MTCD Loss is less frequent than the probability described by MAC-SC4b
	TCT Loss is less frequent than the probability described by MAC-SC3
	CPDLC message issued by TC not displayed on PC HMI is less frequent than the probability described by MAC-SC4b
SR_INT_5	CPDLC message issued by PC not displayed on TC HMI is less frequent than the probability described by MAC-SC4b
	Mode S data does not become corrupted
	Corruption of ADS-C EPP data MAC-SC3
	Corruption of ADS-C EPP data MAC-SC3
	Corruption of Mode S data is less frequent than the probability described by MAC-SC3

1484

1485 **Appendix C Assumptions, Safety Issues & Limitations**

1486 **C.1 Assumptions log**

1487 The following Assumptions were necessarily raised in deriving the above Functional and Performance
1488 Safety Requirements:

Ref	Assumption	Validation
	The Planning conflict detection aid tool shall be active at all CWP's at all times (SO#211).	needs to be validated
	The Planning conflict resolution 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 (SO#212).	needs to be validated
	The Tactical conflict detection aid tool shall be active at all CWP's at all times (SO#016).	needs to be validated
	The division of tasks between TC and PC will be the same as in current operations. (ASM-PJ10.02a-V3-VALP-001.0005)	needs to be validated
	All aircraft are equipped with Mode-S. (ASM-PJ.10-02a-V3-VALP.004)	needs to be validated
	A significant proportion of aircraft are equipped with Data-Link (ATN-B1). (ASM-PJ.10-02a-V3-VALP.005)	needs to be validated
	Air-Ground Data-Link data exchanges are assumed. However, voice is the primary ATC communications medium between pilots and ATCOs, and data link is used for non-time critical communications. (ASM-PJ.10-02a-V3-VALP.006)	needs to be validated
	Implemented automated support for conflict detection, conformance monitoring and electronic coordination (ASM-PJ.10-02a-V3-VALP.010)	needs to be validated
	ATC Procedures for Using Advanced System Assistance to Conflict Detection/Resolution and electronic coordination (ASM-PJ.10-02a-V3-VALP.011)	needs to be validated
	All aircraft will have same level of RNAV and MODE-S equipage	needs to be validated

	The ADS-C EPP equipage level will differ on both Ref. and Sol. Scenarios. (ASM-PJ10.02a-V3-VALP-007.0003)	
	The division of tasks between TC and PC will be the same as in current operations. (ASM-PJ10.02a-V3-VALP-007.0004)	See A004
	Mode S is not used for improving the trajectory prediction	Section 4.2.4
	Conflict detection for the TC also uses the "Improved TP"	Section 4.2.5
	Conflict resolution uses the same "improved TP" as conflict detection (for PC and TC).	Section 4.2.5
	Trajectory Deviation also uses the "Improved TP"	Section 4.2.5
	ADS-B in EXE007 is used by STCD TP instead of the ADS-C EPP.	Section 4.2.6
A	ANSP, Airspace Users and Network Manager need to have the same level of information in flight planning phase regarding flight profile and routing whatever the environment (Standard network or Free route environment)	
A018	Planning controller performs "manual" mid-term conflict detection in parallel to the management of the conflicts detected by the mid-term conflict detection tool	
A019	Tactical controller performs "manual" tactical conflict detection in parallel to the management of the conflict detected by the tactical conflict detection tool	

1489 **Table 30: Assumptions log**

1490 **C.2 Safety Issues log**

1491 The following Safety Issues were necessarily raised during the safety assessment:

Ref	Safety issue	Resolution

1492 **Table 31: Safety Issues log**

1493 **C.3 Operational Limitations log**

1494 The following Operational Limitations were necessarily raised during the safety assessment:

Ref	Operational Limitations	Resolution

1495 **Table 32: Operational Limitations log**



1496 **Appendix D Key Additional Information**

1497



1498
1499
1500

-END OF DOCUMENT-

1501

Insert beneficiary's logos below, if required and remove this sentence



AIRBUS



THALES



1502

Founding Members

