EUROCONTROL

Operational Safety Study

Impact on ATC from a loss of aircraft transponder function - safety considerations

Edition 1.0
Edition date: 08/03/2019

FOUNDING MEMBER SESAR JOINT UNDERTAKING

NETWORK MANAGER

DOCUMENT APPROVAL

The following table identifies all management authorities who have successively approved the present issue of this documents.

Authority	Name and signature	Date
Surveillance Expert, NMD/NS/SCC	 Mr. Gilbert Caligaris	12/02/2019
Operational Safety Coordinator, NMD/NOM/SAF	 Mr. Tzvetomir Blajev	18/02/2019
Head of Safety Unit, NMD/NOM	 Mr. Antonio Licu	11/02/2019
Head of Network Operations Management Division	 Mr. Kenneth Thomas	01/03/2019
Director NM	 Mr. Joe Sultana	08/03/2019

HISTORY OF DOCUMENT

Edition	Date	Reason for change	Affected Sections
V0.1	06/12/2016	Initial Draft	
V0.2	20/06/2017	Processing comments received (NMD/NS/SCC and NMD/NOM/SAF)	All
V1.0	11/02/2019	Processing comments received from stakeholders	All

EXECUTIVE SUMMARY

This paper aims at providing input material into the "NM Top 5 Safety Priorities" for the topic of *"Operation without a transponder or with a dysfunctional one".*

The paper proposes an approach for the safety assessment of the impact on ATC from the loss of the aircraft transponder function, i.e. an Aircraft Surveillance Function (ASF) continuity failure. It addresses the case of an aircraft subject to Area Control Service and Approach Control Service. The paper proposes a set of generic operational elements for both the Aircraft and the Ground Domains, as well as recommendations for future work by appropriate stakeholder bodies.

Regarding the generic operational environments, the presence of both Independent Non-Cooperative Surveillance (INCS) and Cooperative Surveillance (CS) has been assumed in high density TMA whereas only CS has been assumed in the other airspace types (namely, low to high density En-route and low/medium TMA). This paper addresses ASF continuity failure in Area Control Service and Approach Control Service, but excludes Aerodrome Control Service.

Moreover, in this paper, the notion of a "Continuity" failure is applied only to an aircraft that is receiving an ATC Surveillance Service at the time the failure occurs. Therefore, ASF continuity failure prior to entering a sector or infringement cases are out of scope of this paper.

This paper covers both cases where the failure is either "detected" or "not detected" by the ATCo, and this for various situations of system "notification" (or not) on the ATCo surveillance interface (display). For this purpose, a display logic for system notifications to support ATCo detection has been assumed (including coasting mechanism and symbology).

The analysis is summarized as follows:

In airspace types where INCS is available:

- The failure should in general be detected by the ATCo through system notification and/or the display of an INCS-only track symbol. An INCS which is sufficiently good to support the (local) operational procedures with maintained nominal horizontal separation minima will reduce the severity of the event. In this case, the additional ATCo workload induced is therefore assumed to be marginal.

In airspace types with CS only:

- The ASF Function continuity failure (loss of the aircraft transponder function) should in general be notified by the ground system to the ATCo through an appropriate symbology. In this paper, this is assumed to be performed through a sequence of coasting symbols before the track is removed from the display (track drop).

- When the loss is detected by the ATCo, the additional workload induced by managing this situation through non-nominal procedures (e.g. applying alternate procedure in the form of procedural-based ATC) is considered to lead to a slight workload increase, typically expected to be severity 4 in safety terms.

- There is also the possible scenario where the ASF function fails and at the same time the notification is not effective enough to ensure ATCo detection. In this scenario the loss may remain undetected by the ATCo. This scenario leads to two mitigation objectives: The first is to ensure that the notification function is an effective functional barrier. The second objective is to limit the frequency of occurrence of the failure.

- Finally, the analysis indicates that the scenario where both the ASF function and the ground system notification function fail (therefore resulting in the loss not being detected by the ATCo) will drive the ground system function integrity requirements.

As a result, for the generic environment proposed by this paper, the following key elements have been identified to contribute to the reduction of the safety risk related to undetected loss of surveillance for single aircraft:

- The continuity performance of the ASF (typically through its overall Mean Time Between Failure - MTBF) for which quantified requirements should be agreed with the relevant stakeholders,

- Ground domain functionalities for the effective detection by the ATCo of the ASF loss reported through system notification in order to be able to perform the adequate operational procedure,

- The use of INCS (Independent Non-Cooperative Surveillance) where available or necessary.

The presence of INCS and/or notification to ensure the effective detection by the ATCo of the ASF loss appear to be major Ground domain functional barriers once an ASF continuity failure has occurred. In particular, this paper proposes as a priority action the implementation of the following requirement:

REQ-1: Effective mechanisms (e.g. through procedure and man-machine interface) shall be available at ATCo Controller Working Position to ensure that system notification of an Aircraft Surveillance Function continuity failure is effectively and without any delay detected by the ATCo.

For example, in addition to coasting notification some ATC systems may retain the last position as 'frozen' or other notifications until the ATCo has confirmed the detection of the notification, to ensure that the ATCo is aware that the track is terminated and is not updated anymore by measurements.

Future work aiming at the derivation of a quantified ASF continuity requirement will have to address the following topics:

- The selection of an appropriate safety methodology, addressing in particular the choice of Safety Targets agreed by the stakeholders,

- The sensitivity to a number of elements such as the Safety Targets, the probabilities of effect (therefore impacting the Safety Objectives), etc.

- The modelling of dynamic behaviours (such as probability of collision or important reduction of separation minima when loss of track remains undetected by the ATCo),

- The HMI implementation and related human behaviour aspects.

The generic operational elements and recommendations presented in this paper would need to be further reviewed and validated by appropriate stakeholder bodies.

TABLE OF CONTENTS

1 INTRODUCTION 8

1.1 **Objective of this working paper** 8
1.2 **Scope of this working paper** 8
1.3 **Reference Documents** 8
1.4 **Acronyms List** 9

2 LOGICAL SURVEILLANCE ARCHITECTURE AND TYPICAL ASF FAILURES 10

3 OPERATIONAL CONSIDERATIONS 12

3.1 **Operational Environment** 12
3.2 **Use of Independent Non-Cooperative Surveillance** 13
3.3 **Air Traffic Service Descriptions** 14
3.4 **Operational considerations related to the nominal mode of operation** 14
3.4.1 Nominal Surveillance Information and Notifications Displayed to ATC 14
3.4.2 Associated Nominal Operational Procedures 15
3.5 **Operational considerations related to the non-nominal mode of operation** 15
3.5.1 Non-Nominal Surveillance Information and Notifications Displayed to ATC 15
3.5.1.1 Coasting Function for horizontal position loss in CS only environment 16
3.5.1.2 Notification Function for horizontal position loss in combined CS and INCS environment 17
3.5.2 Associated Non-Nominal Operational Procedures 18
3.5.2.1 Non-Nominal procedures in CS environment only 18
3.5.2.2 Non-Nominal procedures in combined CS and INCS environment 18

4 SAFETY CONSIDERATIONS FOR THE "DETECTED TRACK LOSS" HAZARD 19

4.1 **Detected track loss in a CS only environment** 20
4.1.1 Hazard description 20
4.1.2 Hazard Effects 20
4.1.3 Pe determination 20
4.1.4 Resulting Safety Objectives 20
4.1.5 Safety Objective Allocation and Safety Requirements Definition 21
4.2. **Detected CS track loss in a combined CS and INCS environment** 22
4.2.1 Hazard description 22
4.2.2 Hazard Effects 22
4.2.3 Resulting Safety Objectives 22

5 SAFETY CONSIDERATIONS FOR THE "UNDETECTED TRACK LOSS" HAZARD 22

5.1 **Hazard description** 23
5.2 **Hazard Effects** 23
5.3 **Pe determination** 23
5.4 **Resulting Safety Objectives** 24
5.5 **Safety Objectives allocation and Safety Requirements** 24
5.5.1 Detection by the controller 25
5.5.2 Technical causes 25

6 CONCLUSION 26

ANNEX A - SEVERITY CLASS MATRIX AND SAFETY TARGETS 28

A.1 **Severity class matrix in SESAR** 28
A.2 **ATM Safety Targets in SESAR** 29
A.3 **Discussion on controller workload effects and related severity** 30

TABLE OF TABLES

Table 1: Selected Operational Environments 12
Table 2: Selected Operational Environments in CS only environments 16
Table 3: Selected Operational Environments in High Density TMA 17
Table 4: Severity class matrix defined in SESAR 28
Table 5: ATM Safety Targets defined in SESAR 29

TABLE OF FIGURES

Figure 1: Aircraft Surveillance Function failure 10
Figure 2: Aircraft SUR Function Failure continuity Requirements Scenarios 11
Figure 3: Air Traffic Services in ICAO context 14
Figure 4: Assumed Position Symbol HMI in the nominal mode of operations 15
Figure 5: ATCo SUR Interface Coasting Logic as a Function of Loss Duration in CS only environments 16
Figure 6: ATCo SUR Interface Coasting Logic as a Function of Loss Duration in combined CS and INCS TMA High Density environment 17
Figure 7: Detected ASF Continuity failure 19
Figure 8: Example of Safety Targets apportionment for OH1 21
Figure 9: Undetected Track Loss Hazard 23
Figure 10: OH1u Fault Tree 24
Figure 11: Variation of ATC Workload effect after an ASF continuity failure 30
Figure 12: Illustration of change in estimated separation after an ASF continuity failure (at T2) 31

1. INTRODUCTION

1.1 Objective of this working paper

This paper aims at providing input material into the "NM Top 5 Safety Priorities" for the topic of *"Operation without a transponder or with a dysfunctional one".*

The paper proposes an approach for the safety assessment of the impact on ATC from the loss of the transponder function, in other terms the impact of an Aircraft Surveillance Function (ASF) continuity failure. It includes a proposed set of generic operational considerations for both Aircraft and Ground Domains, as well as recommendations for future work by appropriate stakeholder bodies.

1.2 Scope of this working paper

This paper considers the impact of an ASF continuity failure on a single aircraft that is subject to Area Control Service and Approach Control Service. It analyses the "Continuity" failure when the aircraft is receiving an ATC Surveillance Service at the time the failure occurs and for which radio contact is maintained between ATC and flight crew.

Aircraft departing from an aerodrome without a functioning aircraft surveillance function, sector infringement and security aspects (e.g. deliberate turning off of the avionics) are out of scope of this paper.

1.3 Reference Documents

This document considers material from ICAO and SESAR as listed below.

[1] ICAO Doc 4444 – PANS-ATM Air Traffic Management, Procedures for Air Navigation Services, Fifteenth edition-2007

[2] Guidance to Apply the SESAR Safety Reference Material, Project ID: 03.00.00 Edition number: 1 03.00.00

1.4 Acronyms List

ADS-B	Automatic Dependent Surveillance – Broadcast
ASF	Aircraft Surveillance Function
ATC	Air Traffic Control
ATCo	Air Traffic Controller
ATM	Air Traffic Management
ATS	Air Traffic Service
CS	Cooperative Surveillance
CWP	Controller Working Position
DRC	Display Refresh Cycle
FIS	Flight Information Service
HMI	Human Machine Interface
ICAO	International Civil Aviation Organization
INCS[1]	Independent Non-Cooperative Surveillance.
MTBF	Mean Time Between Failure
OH	Operational Hazard
PANS-ATM	Procedures for Air Navigation Services – Air Traffic Management
Pe	Probability of Effects
PSR	Primary Surveillance Radar
SESAR	Single European Sky ATM Research
SO	Safety Objective
SPI/IDENT	Special Position Indication / Identification
ST	Safety Targets
TMA	Terminal Airspace
VHF	Very High Frequency

1 Reference to the term used in ICAO Aeronautical Surveillance Manual section 2.2.1.

2. LOGICAL SURVEILLANCE ARCHITECTURE AND TYPICAL ASF FAILURES

The Surveillance system considered in this paper is described by the logical model presented in the following *Figure 1*. This logical architecture includes the main functions of the Aircraft Domain, of the Spatial Domain and of the Ground Domain and their interactions that are necessary to support the ATC services in a given sector. Figure 1 also shows the location of the aircraft surveillance Continuity failure and its impact on ATC.

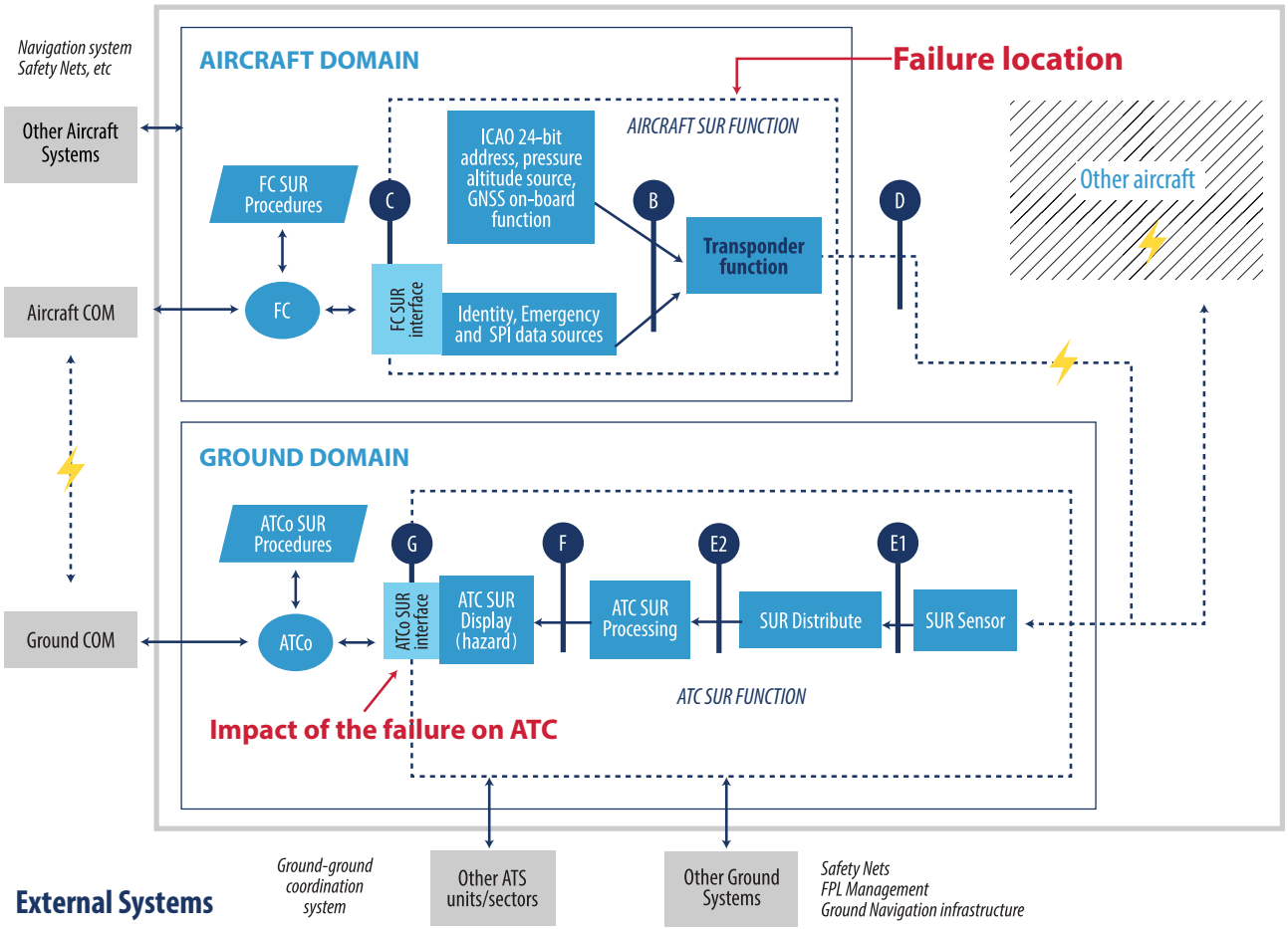

Figure 1: *Aircraft Surveillance Function failure*

The following *Figure 2* illustrates the propagation of Aircraft SUR Function failure, up to its impact at the ATCo interface level (e.g. track loss, which is notified[2] - or not – by the system to the ATCo, and then detected – or not – by the ATCo) and including its possible effects on operations.

[2] In this document, notification relates to the system whereas detection relates to the ATCo.

The left blue arrow depicts the case of an Aircraft SUR Function failure combined with a ground system notification of the ASF failure (e.g. resulting track coast and drop) which is assumed to be detected by the ATCo. The right blue arrow shows the case of an ASF failure combined with a simultaneous ground system display notification failure, resulting in that the ASF failure (and resulting track drop) is assumed to be not detected by the ATCo. In addition, the purple arrow depicts the case of an ASF failure that, although notified by the system, is not detected by the ATCo.

The case represented by the grey arrow on the right hand side of the Figure corresponds to a display failure and not an Aircraft SUR Function failure. Although the focus of this paper is on the ASF continuity failure, some considerations are provided in this paper to this case as this is the main source for ATC SUR Display function requirement derivation.

These cases are developed in the subsequent sections of the paper.

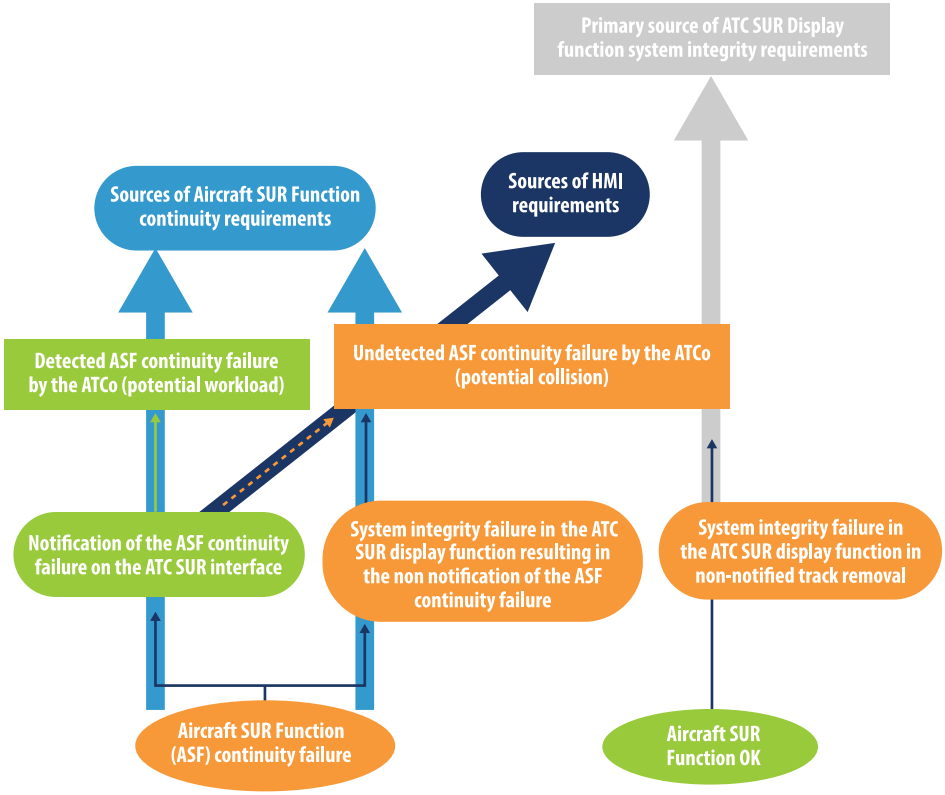

Figure 2: *Aircraft SUR Function Failure continuity Requirements Scenarios*

3. OPERATIONAL CONSIDERATIONS

3.1 Operational Environment

The operational environments analysed in this document have been selected based on those estimated as providing the most typical environmental characteristics (in terms of traffic characteristics, separation minima, density etc.) and supporting the most demanding Air Traffic Services (i.e. Air Traffic Control Services) regarding surveillance requirements. These environments correspond to the largest part of the surveillance deployment in Europe.

The result was to focus on two main ATC services applied for 6 key environments as follows:

- Surveillance supporting AREA Control Service in an En-Route sector.
- Surveillance supporting APPROACH Control Service in a TMA sector.

Complexity	Airspace	
	En-Route sector	TMA sector
Low	ER_5NM Low-Density	TMA_3NM Low-Density
Medium	ER_5NM Medium-Density	TMA_3NM Medium-Density
High	ER_5NM High-Density	TMA High-Density a) 3NM minima b) 2.5NM approach minima c) 2.0NM approach minima d) Independent Parallel Operations

Table 1: *Selected Operational Environments*

In assessing the operational effects of a hazard, such as one discussed in this paper, the characteristics of these environments (such as separation minima, class of airspace, complexity, density etc.) are taken into account.

The environmental characteristics also cover such aspects as flight plans, communications (where VHF is assumed), and navigation (where certain minimum capabilities are also assumed). The following characteristics are important both in assessing hazard effects and in the mitigation procedures used by the ATCo in responding to detected failures:

> **ASSUMP.001.** Direct controller pilot communication (VHF) is assumed available for the provision of ATC services in the environments considered.

3.2 Use of Independent Non-Cooperative Surveillance

ICAO does not prescribe the presence of INCS to support Air Traffic Services. In this document, the use of INCS in addition to CS is assumed in one airspace type.

Indeed INCS, such as Primary Surveillance Radar (PSR), is often derived as a local requirement to assist in managing e.g. unintentional sector infringements. It is also seen as a useful mitigation in the event of transponder failures, and for reduction of the severity of the ASF Continuity failure effects.

However, INCS as a sole means of surveillance would not meet typical surveillance requirements as it is not capable to provide the minimum required data items (i.e. identification and pressure altitude data). In this document, it is assumed that when the INCS is used with Cooperative sensors and in the event of the CS failure, ground system functions exist to maintain the Identification.

The following assumptions are therefore made:

> **ASSUMP.002.** (SUR SENSOR) It is assumed that in TMA High Density (CS) airspace, Independent Non-Cooperative Surveillance (INCS) is present in addition to cooperative surveillance, whereas in the other airspace types only cooperative surveillance is assumed.
>
> **ASSUMP.003.** (ATC SUR Function) it is assumed that in TMA High Density and in the event of cooperative surveillance sensors failure, the ATC SUR Function includes a function to maintain the Identification (and potentially continues to present ground speed).
>
> *Note: the focus of this document is on ASF continuity failure, however it also provides considerations regarding INCS, which is used as a mitigation against this failure.*

For the INCS to be effective in reducing severity, the performance of the INCS sensor is relevant specifically with respect to the horizontal position (including Accuracy, Display Refresh Cycle, and Probability of Detection). Indeed, to reduce the severity, it is essential that the use of INCS as mitigation during the CS failure can support the operational procedures.

> *Note: INCS cannot provide pressure altitude, SPI/IDENT, Emergency data. See section 3.4.1.related to presentation of surveillance data and section 3.5.2.2 related to the non-nominal procedures in High Density TMA.*
>
> *Note: see Section 5.5 for technical considerations, including INCS*
>
> **ASSUMP.004.** (SUR Sensor) It is assumed that the performance related to the horizontal position of the INCS track is sufficiently good to support the (local) operational procedures.

3.3 Air Traffic Service Descriptions

The ICAO Procedures related to the application of the ATC services considered in this document are described in PANS-ATM [1]. The following *Figure 3* shows how the two services considered (Area and Approach Control Services) and the ATS surveillance service fit within the overall ICAO structure and the scope of this paper.

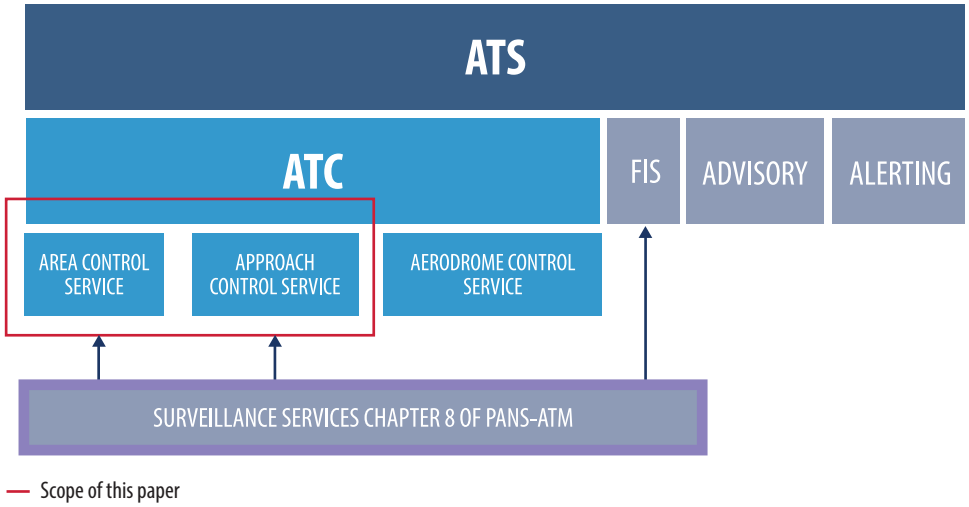

Figure 3: *Air Traffic Services in ICAO context*

Under ICAO PANS-ATM requirements [1], to enable the provision of Surveillance Services, ATC requires relevant information and notifications. The next sections summarise the key elements which are considered in this paper.

3.4 Operational considerations related to the nominal mode of operation

This section summarises the surveillance information presented on the ATCo SUR Interface and the related surveillance procedures.

3.4.1 Nominal Surveillance Information and Notifications Displayed to ATC

Horizontal position, pressure altitude, and identity are assumed as minimum data item requirements whereas other items (such as ground speed and track history) are recommended as best practice.

This paper assumes that all of the environments, except the High Density TMA, contain only CS sources and that surveillance horizontal position data is presented as a single nominal symbol (therefore assuming a fusion tracking system in the case of multiple CS sources). The other symbology related to the non-nominal mode is presented in section 3.5.

However for TMA High Density, both CS and INCS sources are assumed to exist in this analysis and as such the following text presents the assumptions made on the combined symbology.

In terms of surveillance horizontal position data symbols, although individual horizontal position symbols for different (CS and INCS) surveillance sources may be presented to the controller, combined symbols are recommended (PANS - ATM [1] §8.2.3). In TMA High Density the nominal presentation of individual non-correlated symbols on the ATCOs SUR Interface for the same aircraft may create a safety issue in that ATCOs may not know which one to use for separation and which one to ignore. This option is therefore not addressed in this paper and the following assumption is made:

> **ASSUMP.005.** It is assumed that a fusion[3] tracking system is used in order to present a single symbol for the display of horizontal position data in all environments.

In TMA High Density, a combined symbology provides the indication to ATC that the aircraft is being detected by both CS and INCS sources.

The following figure presents an example of the way to present combined CS and INCS symbols.

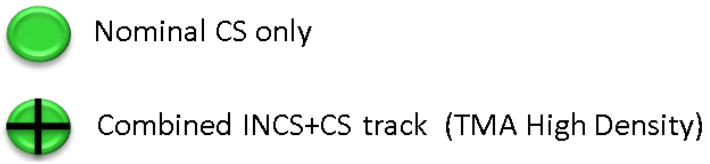

Figure 4: *Assumed Position Symbol HMI in the nominal mode of operations*

3.4.2 Associated Nominal Operational Procedures

In addition to the provision of information and notifications on the ATC SUR Display, ICAO PANS-ATM [1] chapter 8 and other ancillary chapters discuss in detail the surveillance procedures used by ATC.

The next section focuses on the non-nominal mode of operation where very little is provided in ICAO PANS-ATM in terms of response action to a complete loss of Aircraft SUR Function.

3.5 Operational considerations related to the non-nominal mode of operation

The focus of the non-nominal mode of operation is on aircraft transiting through the airspace with an Aircraft SUR Function failure (whereby the function was operational during the first part of the flight). This situation is considered as a source of a hazard for which the effects may impact safety, not only in the critical case when the failure remains undetected by the ATCo, but also in the detected case, due to its possible implication in terms of ATCo and Flight Crew workload.

3.5.1 Non-Nominal Surveillance Information and Notifications Displayed to ATC

In terms of surveillance related 'notifications' it is required that the ATCo surveillance interface provides information to the controller when the horizontal position information is no longer suitable for the application of nominal ATS. This notification is assumed to be provided through a coasting function (Cooperative Surveillance only environments) or through coasting/symbols indicating loss of CS where INCS remains (High Density TMA environments) as described in the next sections.

These are key assumptions for this paper as the performance of these functions determines a) if an Aircraft SUR Function failure will result in detection by ATC or not and b) the possible workload implication when detected.

[3] Or mosaic tracking presenting one simple symbol (where the source may be selectable at the CWP), provided it complies with assumptions made in this document for tthe fusion system, in particular *Figure 5*.

3.5.1.1 Coasting Function for horizontal position loss in CS only environment

This section relates to the following environments:

Complexity	Airspace	
	En-Route sector	TMA sector
Low	ER_5NM Low-Density	TMA_3NM Low-Density
Medium	ER_5NM Medium-Density	TMA_3NM Medium-Density
High	ER_5NM High-Density	n.a.

Table 2: *Selected Operational Environments in CS only environments*

The failure is assumed to disable all forms[4] of CS transmissions from one aircraft, leading to the coasting and then the loss (or freeze) of the CS track on the ATCo SUR interface as described below.

The principle of coasting presented in the figure below is assumed to be representative of the coasting logics currently implemented in Europe. It is recognized that local systems may present this notification differently.

Figure 5 presents a timeline of track presentation in case of a lack of update of the horizontal position. This timeline is function of the Display Refresh Cycle. (See also Annex A.3)

ASSUMP.006. It is assumed that the coast notification illustrated in *Figure 5* is applied for CS only environments (as typical ATC SUR Display function logic).

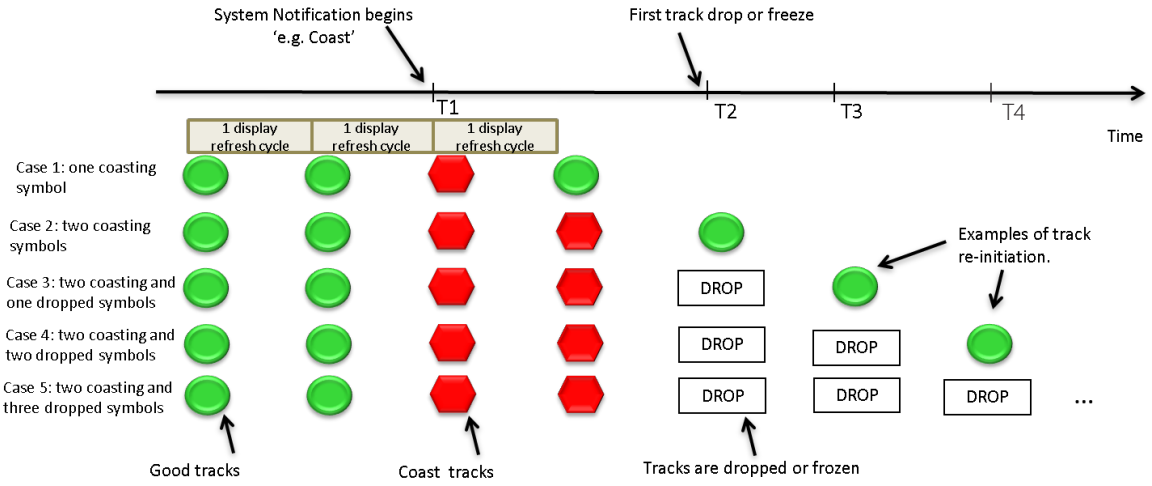

Figure 5: *ATCo SUR Interface Coasting Logic as a Function of Loss Duration in CS only environments*

[4] The Partial loss of CS transmission e.g loss of ADS-B or Mode S only is not addressed at generic level as it depends on the surveillance techniques available on the ground.

3.5.1.2 Notification Function for horizontal position loss in combined CS and INCS environment

As indicated in section 3.2, in High Density TMA the presence of INCS is assumed in addition to CS, and the following environments of section 3.1 are addressed:

Complexity	Airspace	
	En-Route sector	TMA sector
Low	n.a.	n.a.
Medium	n.a.	n.a.
High	n.a.	TMA High-Density a) 3NM minima b) 2.5NM approach minima c) 2.0NM approach minima d) Independent Parallel Operations

Table 3: *Selected Operational Environments in High Density TMA*

In the event of the loss of CS, various notifications to the Air Traffic Controllers on the display and associated operational procedures may exist.

ASSUMP.007. It is assumed that the coast notification illustrated in Figure 6 is applied for combined CS and INCS environments (as typical ATC SUR Display function logic).

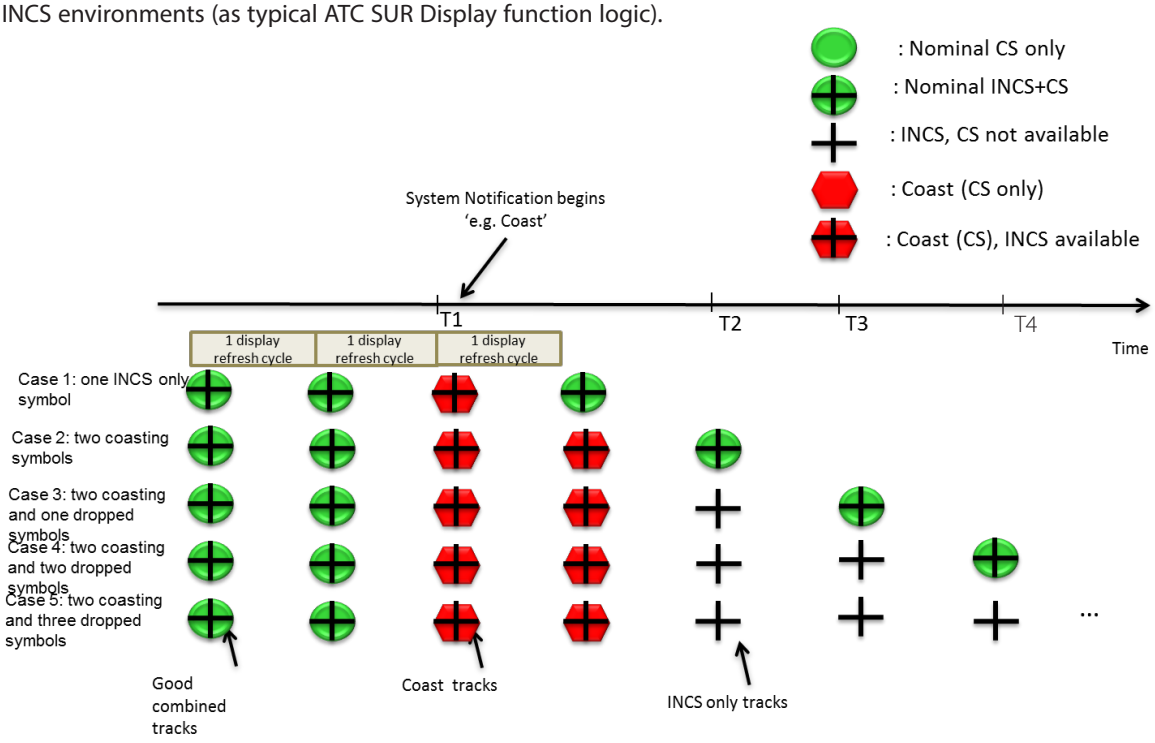

Figure 6: *ATCo SUR Interface Coasting Logic as a Function of Loss Duration in combined CS and INCS TMA High Density*

Note: the case of simultaneous failure of both CS and INCS is not presented in this section but is part of the hazard assessment in section 5.

3.5.2 Associated Non-Nominal Operational Procedures

ICAO procedures linked to surveillance failures are primarily focussed on such areas as identification, altitude verification and navigation monitoring. However, there is very little provided in terms of response action to a complete loss of Aircraft SUR Function and in this document assumptions [5] are made as to the reaction by ATC to detected Aircraft SUR Function failures, coupled with assumptions on the ATCo interface notification of such failures as introduced above.

The notification function is critical as an indication to ATC that surveillance data has either been lost or is no longer suitable for the application of nominal ATC procedures.

3.5.2.1 Non-Nominal procedures in CS environment only

In case of an Aircraft SUR Function failure, the notification presented in section 3.5.1.1 applies with coasting first and then track drop as illustrated in *Figure 5*. The coasting does not in itself imply a change or limitation of the ATC service (in this logic that represents short term horizontal position failures only), however for degradations that last for longer periods, for example where horizontal position data has not been updated for a number of Display Refresh Cycles, the ground system drops the track.

In addition to the coasting notification some ATC systems retain the last position as 'frozen' or other notifications to ensure ATC are aware that the track has been removed. If the loss has been detected, ATC will work with the flight crew and the engineering support to try to resolve the issue. However in the meantime they will stop applying nominal surveillance separation procedures and apply alternate procedures in the form of procedural based ATC and will aim at landing the aircraft at a suitable airport as soon as possible.

3.5.2.2 Non-Nominal procedures in combined CS and INCS environment

In case of an Aircraft SUR Function failure, the notification presented in *Figure 6* applies with first a coast of the CS track. This situation does not in itself imply a change or limitation of the ATC service (in this logic that represents CS short term horizontal position loss). However, for CS degradations that last for longer periods (see "T2" on *Figure 6*) where CS horizontal position data has not been updated, the ground system removes the CS horizontal position and pressure altitude of the track.

As described above in 3.5.1.1, in addition to this CS coasting notification, local systems may provide additional notifications for the CS track drop itself however this is not assumed in *Figure 6*. At this point in time, if the track loss has been detected, ATCo will work with the flight crew and the engineering support to try to resolve the issue. The difference with CS only environments is that in the meantime ATC may, subject to local regulatory approval, continue to apply a surveillance service based on the INCS track (as illustrated in Figure 6) and retained identification data (as per the assumption **ASSUMP.003**).

Given that this paper assumes the INCS only exists in support of the Approach control service within the TMA High Density, the affected aircraft will be located close to an aerodrome where it would be required to land. In this circumstance, depending on local safety case (e.g. accounting for the short duration of the exposure and the presence of direct pilot-controller communications), the regulatory approval may allow the nominal ATS surveillance minima to be applied (also accounting for the INCS performance assumption **ASSUMP.004** as detailed in section 3.2). ATCo would be aware that during this time certain CS only features would not exist such as pressure altitude, emergency codes/modes and enhanced Mode S data if implemented locally.

> **ASSUMP.008.** It is assumed that in TMA High Density the nominal horizontal separation minima can be maintained for a track where the CS component is not available (and therefore being displayed as INCS track only).

This assumption is based on the combination of the following considerations:

a) In TMA, the exposure to the failure is relatively short as the affected aircraft is close to an aerodrome where it will land

b) A single aircraft is affected by the ASF continuity failure (and therefore detected by INCS only) whereas all the surrounding aircraft are still detected by combined CS and INCS surveillance

[5] These assumptions are not procedures per se but present high level course of action considered to be taken in the event of failure detection.

c) The ICAO (PANS-ATM [1] § 8.7.3) allows for the use of "Non-Cooperative Surveillance" (referred as PSR or simply radar) in the application of nominal separation minima, provided that "the system capabilities at a given location so permit" and therefore that a local safety case exists to support this assumption

d) The **ASSUMP.004** in relation to the performance of the INCS track

However, the following assumption prevails for departing aircraft (despite the presence of INCS):

ASSUMP.009. It is assumed that departing aircraft without a properly functioning Aircraft SUR Function are instructed to return to the aerodrome for maintenance.

4. SAFETY CONSIDERATIONS FOR THE "DETECTED TRACK LOSS" HAZARD

This chapter provides some proposed considerations for the safety analysis of the "Detected Track Loss on the ATCo SUR Interface" hazard. It does not intend to provide quantitative results, but rather a discussion on the key elements such as effects, severities, causes, and functional mitigations.

The "Detected Track Loss on the ATCo SUR Interface" hazard corresponds to the case of ASF continuity failure, which is notified to the controller and assumed to be detected (represented in the red framed area in the following *Figure 7:* The analysis of this hazard is split into two sub-cases depending on the environment (due to the presence or not of INCS).

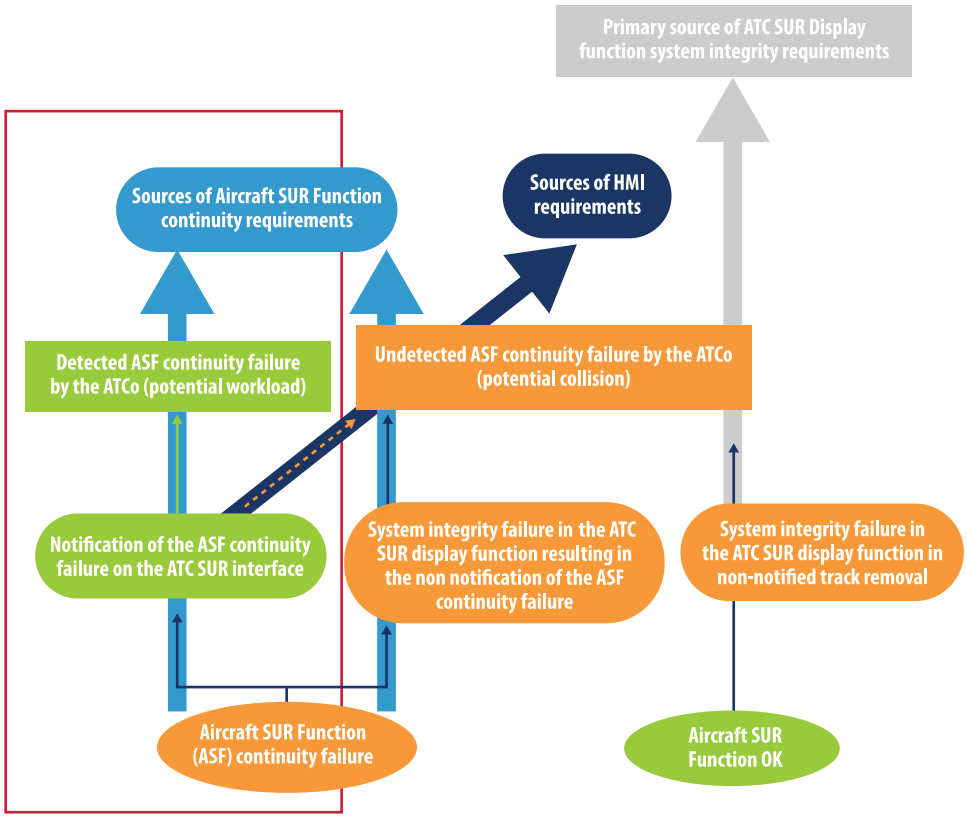

Figure 7: *Detected ASF Continuity failure*

4.1 Detected track loss in a CS only environment

4.1.1 Hazard description

This hazard corresponds to the loss of one cooperative surveillance track, which is notified to the controller and assumed to be detected[6] (OH1d). This notification is based on the display logic presented in *Figure 5*.

It is assumed that the track will be lost for a long duration (i.e. will not reappear after track drop).

4.1.2 Hazard Effects

Hazard effect: as INCS is not available in these airspace types, all tracks appear as CS only and the track for which CS is lost (Aircraft SUR Function continuity failure) is dropped after coasting (as indicated in 3.5.2.1). ATCo will stop applying nominal surveillance separation procedures for this aircraft, will apply alternate separation procedure and will expedite the aircraft to an aerodrome for landing. The expected effects are a slight increase in ATCo and pilot workload to implement alternate ATC procedure and minima, leading typically in safety terms to severity 4 or 5, depending on the environment characteristics (e.g. airspace density, peak traffic or not). The details related to the ATCo additional workload in that case are presented in ANNEX A.3).

The following assumption is made:

ASSUMP.010. It is assumed that ATCo are sufficiently trained to apply an alternate procedure in the event of failure of the surveillance information.

4.1.3 Pe determination

In safety terms, Pe represents the probability that a safety hazard leads to the feared effects as described in the previous section. When the loss occurs, there could be varying workload intensities that the ATC faces depending on traffic complexity. The failure may occur during quiet periods during which the effects will be less than when occurring at demanding periods. Pe leading to severity 4 or severity 5 effects need to be determined. For example, as always applying a severity 4 effects may not be realistic, a larger Pe (e.g. 0.8) may be considered when OH1d leads to severity 4 during peak hours and a lower Pe (e.g. 0.2) when OH1d leads to severity 5 effects during non-peak hours.

Note: Pe values may vary from one environment to another.

4.1.4 Resulting Safety Objectives

In safety terms, the Safety Objective (SO) represents the maximum allowable frequency of occurrences of the hazard.

Safety Objectives are derived from the consideration of Safety Targets (ST) and Pe.

The Surveillance Safety Targets (equipment part) correspond to a portion of the ATM Safety Targets. Various ATM Safety Targets may be considered (see for example the SESAR ATM Safety Targets ANNEX A.2).

Then, the Surveillance Safety Targets shall be apportioned between the various hazards.

The overall apportionment of the ATM Safety Targets to the hazards is depicted in the following figure.

6 Case of track loss notification not detected by the ATCo is dealt with section 5 in the undetected case.

Severity	ATM ST (flight.hour)
Severity 1	1.0e-08
Severity 2	. . .
Severity 3	. . .
Severity 4	. . .

Severity	SUR ST (flight.hour)
Severity 1	
Severity 2	
Severity 3	
Severity 4	

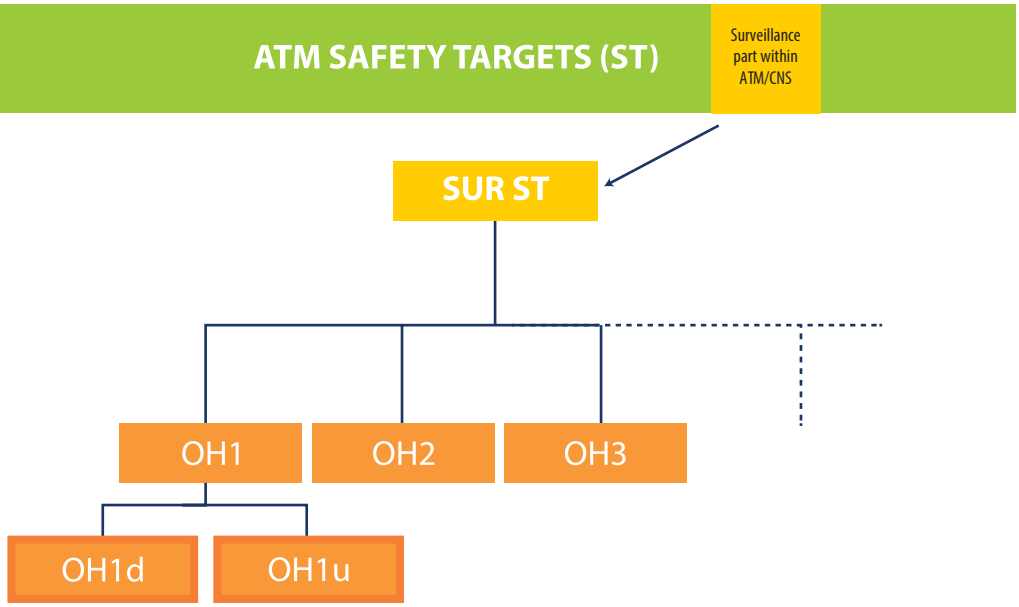

Figure 8: *Example of Safety Targets apportionment for OH1*

4.1.5 Safety Objective Allocation and Safety Requirements Definition

Two kinds of groups of causes may lead to OH1d:

- Aircraft Surveillance Function (ASF) continuity failure,
- Failure in the ground SUR domain.

Note: this paper focuses primarily on the ASF continuity failure, however it highlights that other causes such as failures in the ground SUR domain lead to the same hazards, and that an apportionment between the aircraft and ground causes has to be performed.

The likelihood that a failure in the ground SUR domain affects an individual aircraft instead of multiple aircraft is assessed to be smaller in comparison to the likelihood of a cause coming from the airborne side. Therefore a larger ratio (e.g. of 0.9) may be selected for the SO allocation to the ASF continuity failure and a lower ration (e.g. of 0.1) to the ground SUR domain failure.

In the absence of safety barriers between each of the causes and the occurrence of the hazard, the Safety Objective determined in the previous section could then directly be used to derive safety requirements on the ASF continuity failure (in terms of per flight.hour or MTBF).

4.2 Detected CS track loss in a combined CS and INCS environment

4.2.1 Hazard description

This hazard corresponds to the loss of the cooperative surveillance component of a combined INCS and CS track, which is notified to the controller and assumed to be detected [7] (OH1d). This notification is based on the display logic presented in section 3.5.1.2.

It is assumed that the cooperative surveillance component of the combined INCS and CS track will be lost for a long duration (i.e. will not reappear after track drop).

4.2.2 Hazard Effects

The INCS horizontal position information only is displayed (as indicated in §3.5.1.2), with identification data (and possibly ground speed data) and nominal horizontal separation minima maybe applied by ATCo, subject to assumptions **ASSUMP.004** and **ASSUMP.008** in relation with INCS performance supporting this procedure. In that case there is in principle no real ATCO workload impact for a single aircraft and therefore typically a severity 5[8] may be assigned to this hazard.

Note: the loss of ground CS affecting multiple / all tracks is out of the scope of this document.

4.2.3 Resulting Safety Objectives

Usually, no safety objective is derived from severity 5.

5. SAFETY CONSIDERATIONS FOR THE "UNDETECTED TRACK LOSS" HAZARD

This chapter provides some proposed considerations for the safety analysis of the "Undetected Track Loss on the ATCo SUR Interface" hazard (OH1u). As for the previous chapter 4, it does not intend to provide quantitative results, but rather includes a discussion on the key elements such as effects, severities, and causes.

This "Undetected Track Loss on the ATCo SUR Interface" hazard considers the situation where one track in a sector that was previously displayed and had been identified by the controller unexpectedly disappears from the ATCo SUR interface for a long duration.

The most demanding scenario is assumed to apply when the surveillance track loss is not detected by the controller.

In the figure below three flows in the red framed area are depicted for the "undetected track loss" hazard.

7 Case of track loss notification not detected by the ATCo is dealt with section 5 in the undetected case

8 The severity of this hazard in a CS only environment was evaluated to 4 or 5, depending on the traffic conditions (peak or non-peak hours), therefore it seems reasonable in comparaison to have a severity 5 for this hazard in the CS+INCS case. This is however to be assessed at local level depending on local procedures.

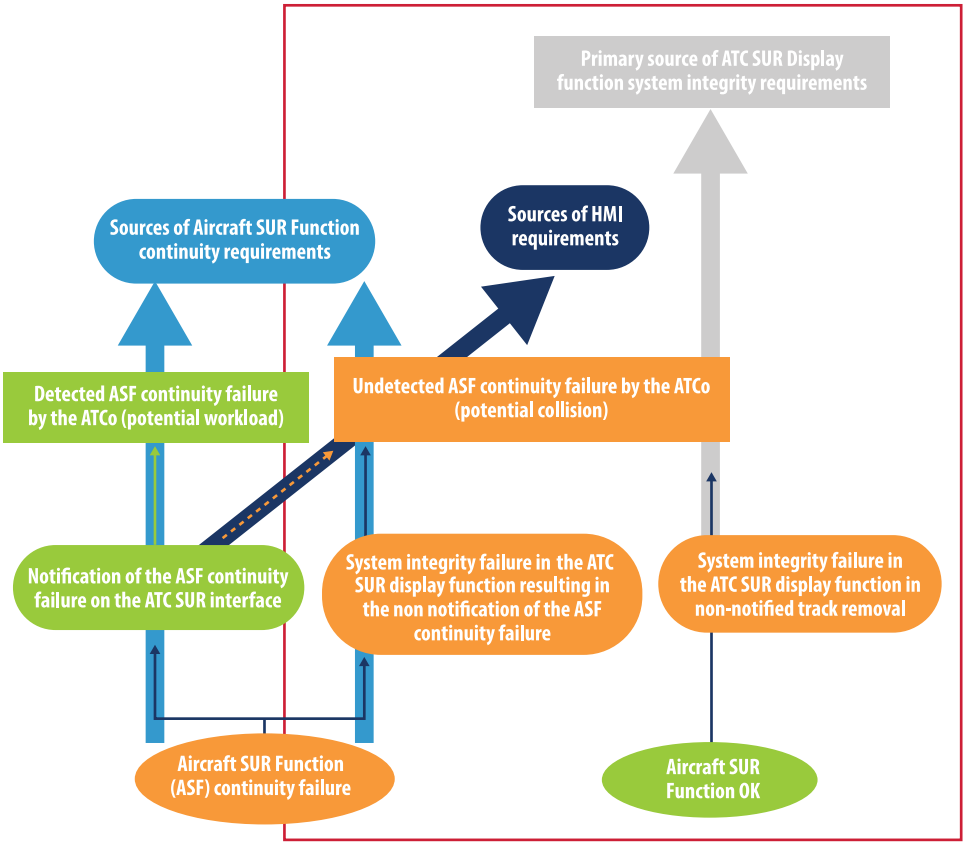

Figure 9: *Undetected Track Loss Hazard*

Three cases lead to the "undetected track loss": each time, independently from the occurrence of an ASF failure, a ground system failure or human failure has to occur for the track loss to pass unnoticed to the controller.

5.1 Hazard description

This hazard corresponds to the undetected loss of a track on the ATCo SUR Interface. The track was previously displayed and had been identified by the controller, but then unexpectedly disappears from the ATCo SUR interface for a long duration, and the loss remains undetected, regardless of the notification by the system or not.

5.2 Hazard Effects

An important element is the consideration of whether the concerned aircraft is potentially in a close proximity (or not) with another/other aircraft. Once the track has been removed from the display and if undetected by the ATCo, there is a risk that only providence can prevent a breakdown of separation. In this undetected case, a breakdown of separation could equate to severity 1 or severity 2 effects.

5.3 Pe determination

In safety terms, Pe represents the probability that a safety hazard leads to the feared effects as described in the previous section. When the undetected loss occurs there could be varying effects as described in previous section, depending particularly on:

- the probability that the affected aircraft will be in a close proximity with another/other aircraft during the continuity failure,
- the safety methodology (probability that the separation breakdown leads to the various severities (e.g. 1, 2)

The various resulting Pe may differ depending on the various airspace classes considered.

5.4 Resulting Safety Objectives

The same principles for apportionment from ATM Safety Targets to OH1 Safety Targets as those described in Section 4.1.4 apply (see *Figure 8*).

Then the Safety Objectives for OH1u can be derived from these Safety Targets and the Pe defined in the previous section.

5.5 Safety Objectives allocation and Safety Requirements

This step relates to linking the hazards to its potential causes, including in particular the ASF continuity failure. This is usually done through Fault Tree approach. An example of Fault Tree is provided below, for both CS only and CS/INCS environments.

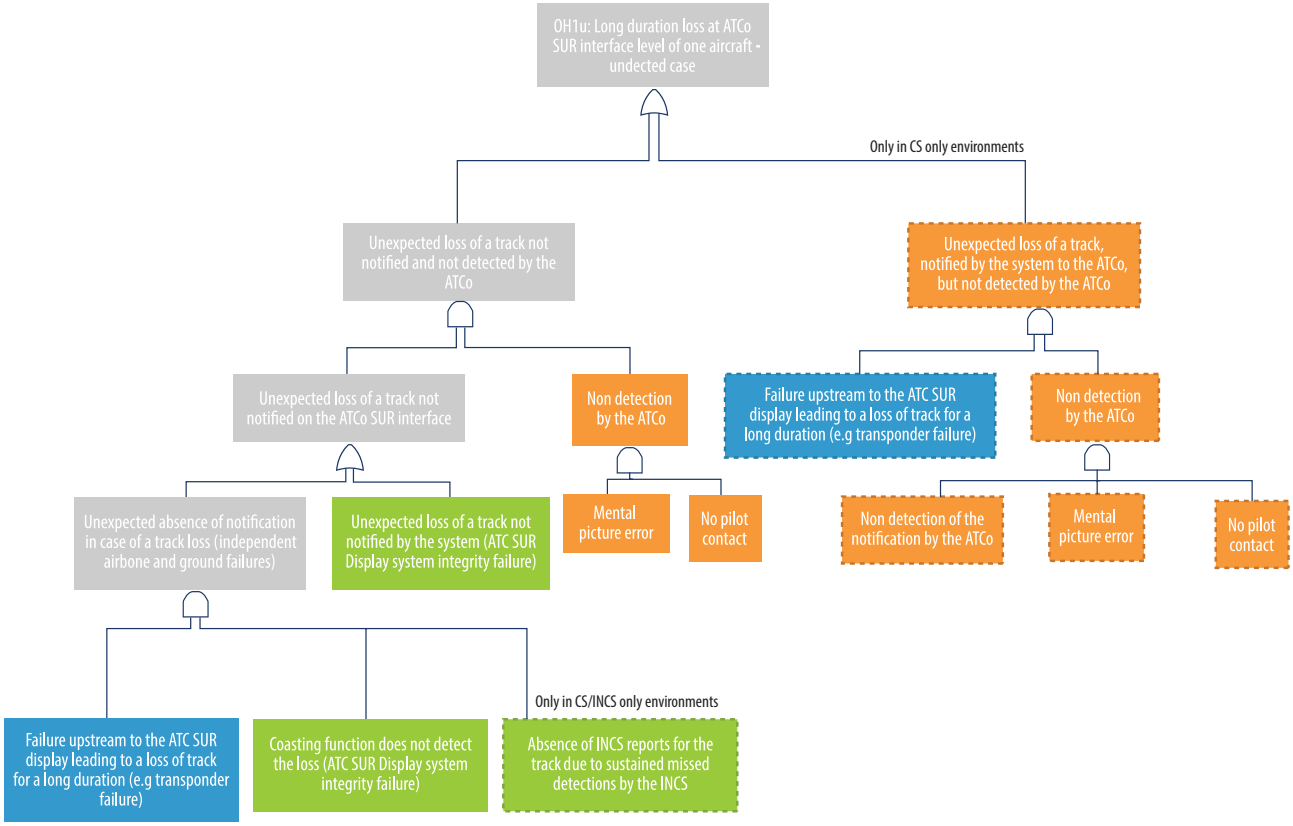

Figure 10: *OH1u Fault Tree*

Note 1: this fault tree is applicable to both CS-only and CS/INCS environments. However, some differences should be noted:

- *The right side branch is only applicable to the CS only environments, and in this case notification is as described in Figure 5. In the CS/INCS environments, the track is still displayed using INCS only symbol and therefore this branch is not applicable.*
- *The box with the dotted line at the bottom on the left hand side of branch of the fault tree is only applicable in CS/INCS environments, as it reflects the possible case of combined ASF continuity failure and sustained loss of detection by INCS that can potentially lead to the worst-case scenario of the undetected case of the failure by the ATCo.*

Note 2: this fault tree reflects the combination of events which could lead to the hazard. This is a logical model. Indeed, a number of common events (e.g. ASF failure), can be found in different parts of this fault tree. This means that their contributions to the occurrence of the hazard are taken into account at multiple times on this figure, when they should be considered only once in the calculation as typically done by a Fault-Tree software tool.

Note 3: Non-detection by the ATCo in the right side branch includes mental picture error. Other barriers (e.g. strips) may be considered in order to ensure completeness of the fault-tree.

5.5.1 Detection by the controller

As indicated in the Fault Tree, two cases are considered regarding the (non-)detection of the loss by the controller:

a) The case of non-detection by the ATCo when the system has provided a notification (right side of the Fault Tree)

b) The case of non-detection by the ATCo in the absence of notification by the system (left side of the Fault Tree)

Related assumptions may be considered, dealing with the probabilities of:

- ATCo failing at detecting a notification by the system
- ATCo failing at detecting the loss through his mental picture of the traffic
- ATCo failing at detecting the loss through pilot contact

The key element to ensure detection of the loss by the controller (case a)) is the definition of the following functional requirement:

REQ-1 Effective mechanisms (e.g. through procedure and man-machine interface) shall be available at ATCo Controller Working Position to ensure that system notification of an Aircraft Surveillance Function continuity failure is effectively and without any delay detected by the ATCo.

Note: The delay referred to in the requirement above should however allow for "confirmation" to happen first after some coasting to avoid false alarm for single plot misses.

5.5.2 Technical causes

Then, as indicated in the Fault tree, the Safety Objective can be apportioned between the following technical causes:

- ASF Continuity Failure
- Coasting function failure
- ATC SUR Display system integrity
- Missed detection by the INCS (for the CS/INCS environments only)

Such Fault tree could therefore be used to derive quantitative safety requirements on the ASF continuity failure (in terms of per flight-hour or MTBF) and on the ATC SUR Display system integrity, which proved to be important technical elements for meeting the Safety Objective.

The ASF continuity failure obtained from this undetected case would need to be reconciled with the results from the detected case in order to retain the most stringent requirement.

6. CONCLUSION

This paper has analysed the Aircraft Surveillance Function (ASF) continuity failure for an aircraft in Area Control Service and Approach Control Service.

For this analysis, the presence of both Independent Non-Cooperative Surveillance (INCS) and Cooperative Surveillance (CS) has been assumed in high density TMA whereas only CS has been assumed in all other airspace types (namely, low to high density En-route and low/medium TMA). In each of these environments, a Controller Working Position display logic for system notifications of track loss to support ATCo detection has been assumed (including coasting mechanism, symbology and corresponding operational procedures).

The analysis covers ASF continuity failure for both the detected case and the undetected case, independently from system notification or not (as a notification may remain undetected by the ATCo).

Regarding the need for effective system notification to the controller the requirement has been identified that effective mechanisms (e.g. through procedure and man-machine interface) shall be available at ATCo Controller Working Position to ensure that system notification of an Aircraft Surveillance Function continuity failure is effectively and without delay detected by the ATCo.

Moreover, the presence of INCS is considered an important ingredient in risk reduction.

The paper provides also a number of considerations for the derivation of technical requirements for ASF continuity failure. These considerations therefore include key elements such as effects (from controller workload for the detected case up to aircraft in close proximity/collision for the undetected case), severities and causes of the related hazards.

The generic operational elements and recommendations presented in this paper would need to be further reviewed and validated by appropriate stakeholder bodies.

ANNEX A - SEVERITY CLASS MATRIX AND SAFETY TARGETS

A.1 Severity class matrix in SESAR

Next table describes the operational effects per severity class.

SESAR		
Severity	Hazardous situation (a) Operational Effect of failure (b)	
Severity 1	(a) A situation where an aircraft comes into physical contact with another aircraft in the air (b) Accident	
Severity 2	Sev. 2a	(a) A situation where an imminent collision was not mitigated by an airborne collision avoidance but for which geometry has prevented physical contact (b) Near collision
	Sev. 2b	(a) A situation where airborne collision avoidance prevents near collision (b) Imminent collision
Severity 3	(a) A situation where an imminent collision was prevented by ATC Collision prevention: STCA, expedite, etc *Note: this should encompass an ATC induced tactical conflict that nearly always lead to imminent infringement* (b) Imminent infringement	
Severity 4	Sev. 4a	(a) A situation where an imminent infringement coming from a crew/aircraft induced conflict was prevented by tactical conflict management (b)Tactical Conflict (crew/aircraft induced)
	Sev. 4b	(a) A situation where an imminent infringement coming from a planned conflict was prevented by tactical conflict management (b) Tactical Conflict (planned)
Severity 5	(a) A situation where, on the day of operations, a tactical conflict (planned) was prevented by Traffic Planning and Synchronization (b) Pre tactical conflict	

Table 4: *Severity class matrix defined in SESAR*

A.2 ATM Safety Targets in SESAR

Severity	ATM ST in SESAR [flight.hour]	
Severity 1	1,0E-09	
Severity 2	Sev. 2a	1,0E-06
	Sev. 2b	1,0E-05
Severity 3	1,0E-04	
Severity 4	Sev. 4a	1,0E-03
	Sev. 4b	1,0E-02

Table 5: *ATM Safety Targets defined in SESAR*

Next section discusses the safety targets for the severity class 4 in relation to the specific OH1d assessment in this paper.

A.3 Discussion on controller workload effects and related severity

The following illustration shows in the event of a failure of the ASF leading to a notified dropped track on ATC SUR display, how workload effects increase over time and vary between environments with an INCS (TMA High Density) and those without.

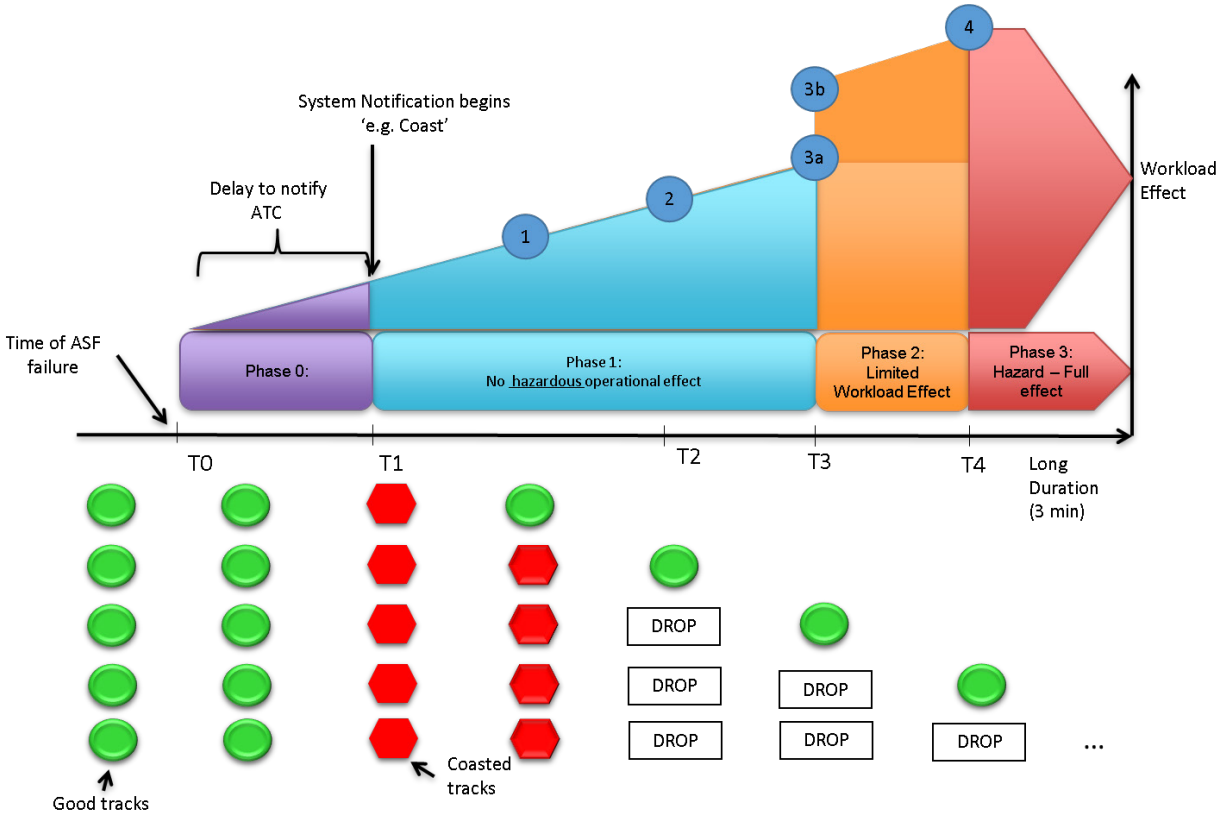

Figure 11: *Variation of ATC Workload effect after an ASF continuity failure*

The following 4 points are linked to the numbers shown in the circles in the figure above.

This figure is an example only and intends to illustrate that over time workload will increase. However in environments where INCS exists, the peak workload effects are mitigated. It is recognized that in real time operations the actual interaction between ATCo and flight crew will vary depending on flight crew and ATCo reaction time.

1. At the second coast, the ATCo is assumed to react to the notification and will request the flight crew to check their transponder setting. As this analysis is based on a failure of the ASF the flight crew should, in most cases, respond by advising ATCo that there has been a failure on board and most likely they will need some more time to see if they can resolve the issue. There is no safety effect at this stage as ATCo are trained to deal with these occurrences, even in busy airspace.

2. At T2 the flight crew may have advised ATCo that they are unable to resolve the ASF issue. At the same time the CS track is dropped from the display. For environments that contain an INCS, a surveillance track remains and as per the assumptions in this document, the Aircraft identification is maintained.

3. Approximately around the second drop it would be expected that ATCo have considered the CS track may not be reacquired. In this phase workload effects depend on the presence or not of the INCS and on the level of ATCo training:

a. In environments with INCS (TMA High Density in this paper) ATCo will rely on that data to apply surveillance based minima and in most cases will request the flight crew to return to the aerodrome to have the issue resolved (as described in §3.5.2.2). For this environment workload effect does not increase any further (leading to severity 5).

b. However, in environments where INCS does not exist, ATCo will now have to apply an alternate minimum with surrounding traffic. This situation is problematic as prior to the failure, ATCo were applying surveillance based minima which are significantly smaller than procedural minima (see *Figure 12* below). Changing flight level is sometimes considered an easy solution however in some sectors there may be aircraft already occupying many of the available levels. Assuming ATCo have been trained to apply an alternate procedure (see **ASSUMP.0010** defined in §4.1.2), they will apply lateral minima allowing the affected aircraft to descend through other occupied levels and reach a terminal airspace where INCS exists and the aircraft can land at the relevant aerodrome. Then ATCo workload effects would not increase any further.

4. In environments where INCS does not exist and if ATCo have not been trained to apply appropriate procedural minima in the event of a lost track, then the workload effect continues to rise. This could result in a separation infringement with surrounding traffic. However this case is out of scope of this paper as per **ASSUMP.0010.**

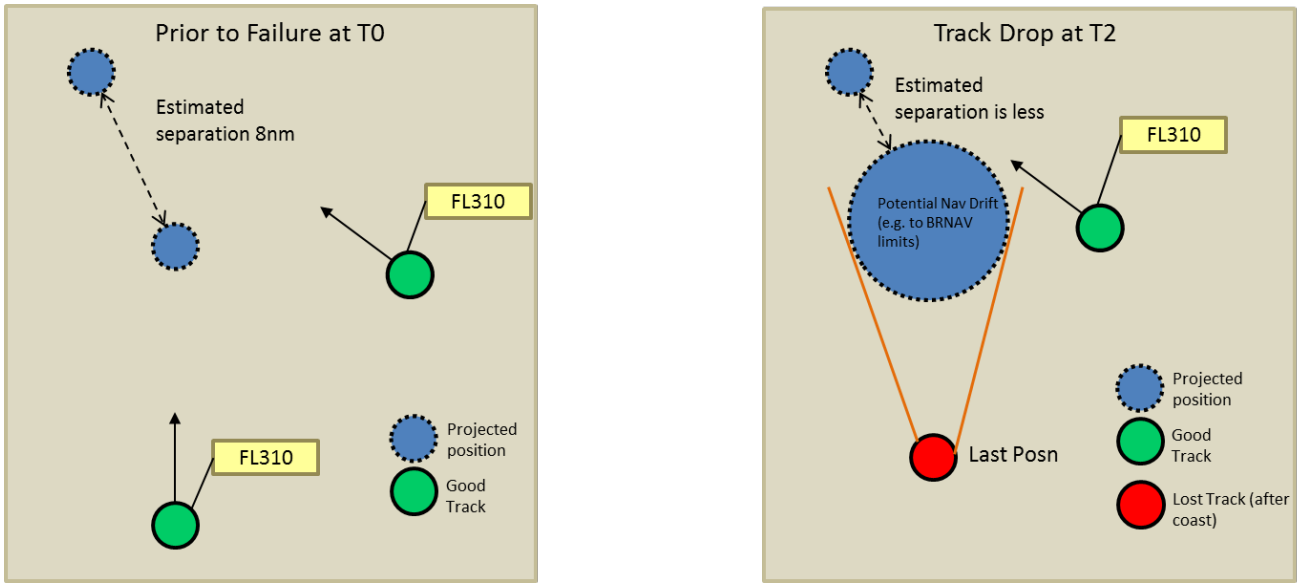

Figure 12: *Illustration of change in estimated separation after an ASF continuity failure (at T2)*

In SESAR (see A.1 *Table 4*) the effects for severity class 4 have been divided into two types of "conflicts" (which is determined as an imminent infringement): "planned" conflict (4.b) or "crew/aircraft induced" conflict (4.a) as indicated in *Table 4* extracted from [2].

When considering the specific ASF continuity failure leading to detected track loss (OH1d severity 4) in this paper, it is important to ensure that the appropriate ST are selected for this specific severity class 4, as the operational effects cannot be directly mapped on the type of SESAR conflict cases.

Indeed in the event of a track loss that is detected by the controller, the induced workload is rather linked to the provision of alternate separation minima (procedural) that could be compared to a planned conflict rather than to a "crew/aircraft induced" conflict. The analysis assumes that the aircraft was separated at the time of the failure.

> *Note: the crew/aircraft induced" conflict (4.a) category is understood to correspond to flight crew deviations from ATC clearances (e.g. level busts, lateral or vertical speed deviation …), whereas the planned" conflict (4.b) category rather includes Ineffective Tactical Conflict Management.*

www.eurocontrol.int