EUROPEAN ORGANISATION
FOR THE SAFETY OF AIR NAVIGATION

EUROCONTROL

Preliminary System Safety Analysis for the Controller Access Parameter service delivered by Mode S Enhanced Surveillance

Edition Number	**:**	**1.1**
Edition Date	**:**	**07.04.2004**
Status	**:**	**Released Issue**
Intended for	**:**	**General Public**

EUROPEAN AIR TRAFFIC MANAGEMENT PROGRAMME

DOCUMENT CHARACTERISTICS

TITLE		
Preliminary System Safety Analysis for the Controller Access Parameter service delivered by Mode S Enhanced Surveillance		
	EATMP Infocentre Reference:	04/04/07-02
Document Identifier	**Edition Number:**	1.1
MODES/SAF/002	**Edition Date:**	07.04.2004

Abstract

This documents contains a generic safety analysis of the introduction of Controller Access Parameter (Magnetic Heading, Indicated Airspeed, Vertical Rate, Selected Altitude) obtained using Mode S Enhanced Surveillance.

Keywords

Mode S	CAP	Safety	PSSA
Enhanced Surveillance	Selected Altitude		

Contact Person(s)	Tel	Unit
Pascal Dias	93369	
Eric Potier	93504	

STATUS, AUDIENCE AND ACCESSIBILITY

Status		Intended for		Accessible via	
Working Draft	☐	General Public	☑	Intranet	☐
Draft	☐	EATMP Stakeholders	☐	Extranet	☐
Proposed Issue	☐	Restricted Audience	☐	Internet (www.eurocontrol.int)	☑
Released Issue	☑	*Printed & electronic copies of the document can be obtained from the EATMP Infocentre (see page iii)*			

ELECTRONIC SOURCE

Path:	G:\Mode S\ST03 - System Design & Safety\Safety\Enhanced Sur PSSA	
Host System	Software	Size
Windows_NT	Microsoft Word 10.0	1271 Kb

EATMP Infocentre
EUROCONTROL Headquarters
96 Rue de la Fusée
B-1130 BRUSSELS

Tel: +32 (0)2 729 51 51
Fax: +32 (0)2 729 99 84
E-mail: eatmp.infocentre@eurocontrol.int

Open on 08:00 - 15:00 UTC from Monday to Thursday, incl.

Mode S Programme
E-mail: ModeS@eurocontrol.int
Web: http://www.eurocontrol.int/mode_s/

DOCUMENT APPROVAL

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

AUTHORITY	NAME AND SIGNATURE	DATE
Please make sure that the EATMP Infocentre Reference is present on page ii.		
Mode S Programme manager	Pascal Dias	07/04/2004
Mode S Programme Safety manager	Eric Potier	07/04/2004

DOCUMENT CHANGE RECORD

The following table records the complete history of the successive editions of the present document.

EDITION NUMBER	EDITION DATE	INFOCENTRE REFERENCE	REASON FOR CHANGE	PAGES AFFECTED
0.1			Initial draft	All
0.2			Incorporation of Mode S Safety Task force comments	All
0.3			Incorporation of Mode S Safety Task force comments	All
0.4			Incorporation of Mode S Safety Task force comments	All
0.5			Incorporation of Mode S Safety Task force comments	All
0.6	16.09. 2003		Avionics figures aligned with Elementary PSSA figures	
1.0	17.10. 2003		Proposed issue: EATMP template + highlighting of assumptions + discussion on detected corruption of SA (p24+p36)	All
1.1	07.04. 2004		Released issue EATMP infocentre number clarification (following JAA comment) on . Vertical rate dual source . Selected altitude and intermediate step . Barometric pressure setting mentionned	

CONTENTS

EXECUTIVE SUMMARY

This document has developed a Preliminary System Safety Analysis (PSSA) of four controller access parameters (CAP) which are delivered by Mode S Enhanced Surveillance. This document defines a generic operational and technical environment with a set of assumptions, which defines how the CAP will be used. The CAP considered in the safety analysis are:

- Magnetic Heading
- Indicated Airspeed
- Vertical Rate
- Selected Altitude

For each of the CAP, a set of safety objectives is defined based on the Operational Hazard Assessment results and the assumed environment.

The PSSA then assesses whether the future operational environment, with Mode S enhanced surveillance, can meet the safety objectives.

Based on the assumptions listed in this document, such as classifying these CAPs as minor for the avionics the analysis concludes that the listed CAP can be used by the controllers.

The PSSA demonstrates that the functionality provided by Selected Altitude (as an addition to the VHF read back facility) can potentially reduce the undetected corruption of cleared flight level. This will have a positive impact on the incident rates where cleared flight level is used operationally, for example in TMA environments. Nevertheless this information shall not be taken as a confirmation that any aircraft will reach and maintain the Cleared Flight Level. The monitoring of climb/descent shall continue as is the case today.

A discussion concerning the use of Vertical Rate, Magnetic Heading and Indicated Airspeed illustrates that the Mode S equipment contribution does not impact on the occurrence of corrupted information. Indeed the higher integrity of the Mode S link improves the likelihood of correct information being presented to the controller.

The analysis re-enforces the positive contribution of the controller in detecting failures and controllers should continue to monitor the movements of aircraft even if the value presented on the track label appears correct.

A word of caution

The analysis presented in the document relies on all the assumptions being true and valid. ANSPs and other readers should ensure that the assumptions made in this document are applicable to their airspace, using this document as a contributor to their local safety case.

1 INTRODUCTION

1.1 Context

1.1.1.1 This document presents a Preliminary System Safety Analysis (PSSA) of four data items required by the controller access parameters (CAP) service, which are delivered by Mode S Enhanced Surveillance. The document has been produced by the Eurocontrol Mode S Programme to support to the implementation of Mode S Enhanced Surveillance.

1.1.1.2 The CAP information considered in the safety analysis are (with the equivalent ARINC 429 references included within brackets):

- Magnetic Heading (equivalent to ARINC429 label 320);
- Indicated Airspeed (equivalent to ARINC429 label 205 or 206);
- Vertical Rate (equivalent to ARINC429 label 365 or 212);
- Selected Altitude (equivalent to ARINC429 label 102).

1.1.1.3 CAP may be delivered by a number of communications systems (including both voice and datalink). This analysis only considers the use of Mode S Enhanced Surveillance as a means of delivering CAP to the controller.

1.1.1.4 The document is not a safety case for the implementation of CAP or Mode S Enhanced Surveillance. It is presented as a 'typical example' of a safety assessment and as a contributor to the production of local safety cases

1.2 Scope of the Analysis

1.2.1.1 The PSSA process is an iterative process, which is typically initiated at the beginning of the design or modification phase of a system. The purpose of the PSSA is to determine if the tolerable risk of a failure of the system, specified in a set of safety objectives derived from the OHA [6], can be met by the proposed/modified architecture.

1.2.1.2 The Air Navigation System is defined as the aggregate of organisations, people, infrastructure, equipment, procedures, rules and information used to provide the Airspace Users Air Navigation Services in order to ensure the safety, regularity and efficiency of international air navigation. This definition is illustrated in Figure 1.

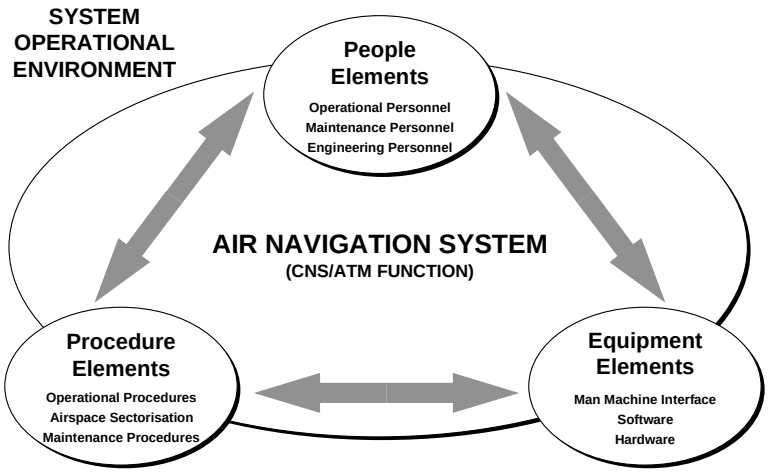


Figure 1 - Definition of the Air Navigation System

1.2.1.3 The approach adopted in this analysis is based on:

- A quantitative safety assessment of the equipment.
- A qualitative safety assessment of procedural and human contribution. However, where possible assumptions concerning the contribution of the human element have been estimated and quantitative values are proposed.

1.2.1.4 All quantitative assumptions used within this analysis are listed in annex C. When they are introduced within the document they are highlighted using **bold blue characters in a box** with a footnote indicating their source.

1.2.1.5 At the start of the safety analysis, a quantitative approach to the assessment of all three components of the system was considered. However it was not always possible to find quantitative figures for all sources of errors and therefore some figures used within the calculation are based on best "expert estimate" obtained from discussion and debate between experts participating in the Mode S Safety Task Force. These figures are highlighted in yellow.

1.2.1.6 The scope of this analysis is limited to the differences brought by the introduction of the use of CAP on the Controller Working Position.

1.2.1.7 The safety analysis has been performed based on a 'generic' operational concept and architecture. This means that the analysis does not provide precise safety results but rather an order of magnitude within which readers can make their own judgement as to whether the CAP safety objectives can be achieved**. As a consequence, ANSPs and other readers should ensure that the assumptions made in this document are applicable to their operations**.

1.2.1.8 The following key assumptions SUPPORT the safety analysis in this document:

- The basic surveillance system (either through Mode S Elementary Surveillance or ‘standard’ SSR) is safe;
- CAP information complements surveillance information within the ATM system;
- Failure of basic surveillance is outside the scope of this document.

1.2.1.9 The analysis concerns the operational aspects provided by the CAP service on the assumption that current operations are safe. It is not the purpose of this document to assess the safety of current operations but rather to assess the operational concept where the CAP provides a service to the controller. Within the OHA this was addressed through the detected classification for each individual parameter. In some cases this was classified as severity class 4 which results in, for example, a slight increase in workload

2 OPERATIONAL DESCRIPTION RELEVANT TO THE CAP SERVICE

2.1 Introduction

2.1.1.1 This section presents the underlying assumptions about the operational and technical environment on which the PSSA is performed.

2.2 Operational Environment

2.2.1 General assumptions

2.2.1.1 A number of basic assumptions are made about the operational environment in which CAP and Mode S Enhanced Surveillance will operate. The assumptions provide a generic framework under which the safety analysis has been performed. The results of the safety analysis are therefore constrained to be applicable when all the assumptions are taken as 'valid'.

2.2.1.2 The assumptions in this section may not be valid for particular regions of Europe or particular operations and, as such, should be reviewed in detail by the ANSP.

2.2.1.3 The analysis was performed assuming the CAP information will be used in both En-Route and the Terminal Manoeuvring Area (TMA)/Approach airspace throughout the ECAC Core Area, where Mode S Elementary Surveillance will be implemented.

2.2.1.4 Surveillance Coverage is assumed to be based on the Eurocontrol surveillance coverage standard [reference 1] updated to include Mode S which equates to:

- En-route - Dual Mode S SSR
- Major terminal areas - Dual Mode S SSR and single Primary Surveillance Radar

2.2.1.5 For the purposes of the analysis, the aircraft under control are assumed to be flying at the minimum separation standard specified within the airspace [reference 2]. For en-route airspace between FL290 and FL410 this includes the use of Reduced Vertical Separation Minima and the use of Required Navigation Performance (RNP) of RNP-5 for En-route and RNP-1 for TMA.

2.2.1.6 The aircraft traffic density levels to be considered are consistent with predictions for the period 2005 to 2010 up to the maximum airspace density.

2.2.1.7 It is assumed that communication with the aircraft is always possible via VHF voice and the concurrent failure of voice communication and surveillance (i.e. both items being in a failed state at the same time) is outside of the scope of this study as there is no additional requirement added on the VHF.

2.2.1.8 Whilst intended to be a unique identification for a particular airframe, the ICAO 24 bit aircraft address is not unique in practice; there are a very small number of repeated addresses. For the purposes of this analysis, it is assumed that the likelihood of repeated addresses occurring within a volume of controlled airspace is improbable, and therefore the ICAO 24 bit address is assumed to be unique.

2.2.1.9 The loss of the Mode S Elementary Surveillance will prevent the transmission of all CAP data.

2.2.1.10 The ground-based interrogators will detect both Mode S and Mode A/C equipped aircraft.

2.2.2 Aircraft Assumptions

2.2.2.1 It is assumed that aircraft are fitted with equipment compliant and certified to the requirements of the appropriate regulatory authorities.

2.2.2.2 It is assumed that within Enhanced Mode S Airspace there will be the following airspace users:

- Aircraft that are fully Mode S Enhanced Mode S equipped;
- Aircraft that are partially Mode S Enhanced Mode S capable;
- Aircraft that are not Mode S Enhanced Surveillance equipped;

2.2.2.3 It is assumed that 'partial' means incapable of a specific CAP (i.e. the avionics may not be capable of filling the appropriate BDS fields). It is assumed that the ground-based systems will only use aircraft CAP data that is indicated as available from the transponder capability report (BDS 17). When the capability report is not available, CAP data will not be presented on the CWP and controllers will only use 'normal' control. It is assumed that procedures are in place to accommodate this mode of operations and there is no safety impact.

2.2.2.4 The system, which is operating within the airspace, is assumed to be able to manage the airspace users identified above during normal operations. It is also assumed that, the airspace can manage, in a safe manor, the change of an aircraft from one type to another (e.g. from fully to partially Mode S Enhanced Surveillance capable), for example, as the result of a failure.

2.2.3 En-Route Operations

2.2.3.1 The operational environment for all controllers can include sequencing of traffic into hold areas and stacks, and includes the potential for crossing traffic.

2.2.3.2 The En-Route airspace Controller is assumed to be controlling aircraft within a relatively ordered traffic flow.

2.2.4 TMA/Approach Operations

2.2.4.1 TMA operations are likely to be more complex than En-Route operations with higher levels of traffic operating with reduced separation than would occur within En-Route airspace. The reaction times required of a controller within the TMA are typically shorter than for a similar role within En-Route airspace.

2.2.4.2 An Approach Controller is assumed to be handling aircraft arrivals.

2.2.4.3 The use of TCAS as mitigation for failure is not claimed through this PSSA and as such represents an additional safety net.

2.2.5 Safety Nets

2.2.5.1 The aircraft ACAS/TCAS system is not claimed as mitigation following any failures of the system.

2.2.5.2 The activation of an STCA alert is based upon prediction and is normally made before the loss of standard separation. It is assumed that STCA is an advisory tool (a "safety net") and it is not used for air traffic control purposes. Mitigation due to STCA will not be claimed within the analysis, nor will the impact on operations due to STCA failures or false alarms.

2.3 Concept for the presentation and use of the CAP service

2.3.1 Mode S Enhanced Surveillance delivery of CAP

2.3.1.1 Some of the CAPs have been available for a number of years and are downlinked to the controller over VHF voice. As a consequence the automatic downlinking of the data does not significantly change the concept of operations for ATC but rather it:

- reduces the VHF voice congestion
- presents the information to the controller on the track label
- provides additional confirmation (above that of voice) for the value of the CAP.

2.3.1.2 The CAPs to be downlinked for Enhanced Surveillance are periodically fed by the avionics equipment via specific interfaces (e.g. data concentrator) into the appropriate register of the transponder. In the case of the Mode S transponder, the Volume III of ICAO Annex 10 SARPS [7] defines 256 registers of 56 bits, each register being able to store 3 or 4 parameters.

2.3.1.3 Mode S Enhanced Surveillance makes it possible for the ground systems to request a specific aircraft's current state parameters and short-term intent parameters, all the said parameters being equivalent in definition to those defined within the ARINC 429 Standard (Mark 33 Digital Information Transfer System).

2.3.1.4 This on-board aircraft data may be used both for indicating specific parameters to the controller workstations (the CAP service) and processing by various ATM systems (i.e. the SAP service[1] which is not covered by this analysis).

2.3.1.5 It is assumed that CAP will be displayed on the Controller Working Position upon request from the controller.

2.3.2 Mixed Mode Operations

2.3.2.1 This analysis considers that aircraft may be Mode S Enhanced Surveillance capable or not, i.e. mixed mode operations are foreseen. However, because the use of the CAP is an additional service to supplement current practices then the unavailability of downlinking CAP for presentation to the controller is still regarded as safe since it is a reversion to current practices which are by definition safe. However, the loss of a CAP may result in the controller reverting to 'normal' operations which may cause a short term, slight

[1] The SAP service may use the same data as the CAP service but is targeted towards ground data processing systems such as tracking systems (in particular improvements in track initialisation and the recognition of flight manoeuvres) and safety net systems such as STCA and MSAW (fewer false alarms).

increase in controller workload (because the data would be obtained via voice rather than datalink). This is captured by the OHA severity classifications (as defined in ESSAR 4, reference [3]), where controllers acknowledged the increase in workload, but anticipated a safe situation would prevail.

2.3.3 Operational use of the CAP service

2.3.3.1 The CAP considered in the safety analysis are (with the equivalent ARINC 429 references included within brackets):

- Magnetic Heading (equivalent to ARINC429 label 320);
- Indicated Airspeed (equivalent to ARINC429 label 205 for Mach number or 206 for Indicated Airspeed);
- Vertical Rate (equivalent to ARINC429 label 365 for inertial velocity rate or 212 for barometric altitude rate);
- Selected Altitude (equivalent to ARINC429 label 102).

2.3.3.2 The operational use for each CAP is summarised below. Further details can be found in reference [4].

2.3.4 Magnetic Heading

2.3.4.1 Magnetic Heading may be used to assist in maintaining separation between aircraft, in particular during active radar vectoring of aircraft.

2.3.4.2 Magnetic Heading is relayed to the controller via voice communications, whereas with Mode S it will be downlinked automatically and presented on the track label. This may be used as a confirmation of the cleared heading and therefore reduce a possible misunderstanding which could occur between controller and pilot by using voice only.

2.3.5 Indicated Airspeed

2.3.5.1 The Indicated Airspeed parameter or Mach number shows the aircraft's indicated air speed (IAS) or the speed as a Mach number. It is used during active radar vectoring of aircraft and may be used to assist in maintaining separation between aircraft.

2.3.5.2 Similar to Magnetic Heading, Indicated Airspeed is relayed to the controller via voice communications, whereas with Mode S it will be downlinked automatically and presented in on the track label.

2.3.6 Vertical Rate

2.3.6.1 Vertical Rate indicates the rate at which an aircraft is climbing or descending.

2.3.6.2 Vertical Rate is used by controllers throughout the flight to support many activities and may be used as a means of separating aircraft vertically (i.e. during take-off), Vertical Rate will be used to improve situational awareness without any change in operational work practice. Vertical Rate may be used to control a climbing/descending manoeuvre, during which Vertical speed control may be applied to establish or maintain a specific separation minimum. Vertical Rate can also be used by controllers to estimate the time when an aircraft will reach its cleared flight level.

2.3.6.3 The rate of change of the Mode C/altitude report indication is used as an estimate of how fast an aircraft is descending or climbing. In some cases the controller performs a 'mental arithmetic to estimate the Vertical Rate of an aircraft. An equivalent to Vertical Rate is calculated today by multi-sensor systems to provide either an indication of climb/descent (Asterix I062/200 mode of movement) or calculated rate of climb/descent (Asterix I062/220). However the value calculated on the ground is a smooth value based on the recent Mode C/altitude reports. Mode S Vertical Rate will allow a more real time view of the aircraft climb or decent profile. It is anticipated that controllers would become more reliant on the Vertical Rate parameter once it is included within the Track Data Block.

2.3.6.4 There are two Vertical Rate parameters encoded in BDS 4.0H, These are

- Barometric altitude rate (BDS 4,0H, bits 35-45),
- Inertial altitude rate (BDS 4,0H, bits 46-56).

It is assumed that the vertical rate information can be provided either by the"Barometric altitude rate" or by the "Inertial altitude rate" depending on the aircraft equipment and that aircraft do not necessarily provide both of them.

2.3.6.5 There is a close link between the Mode C/altitude report and Vertical Rate. The altitude report is a report of barometric altitude and therefore a failure in barometric altitude will result in a failure of both altitude report and barometric altitude rate. However, the source for inertial altitude rate is independent from barometric altitude and therefore an independent failure of inertial altitude rate can occur without impacting on the altitude report. As a consequence, because the two sources are independent it is possible that a controller would quickly recognise a failure in the Vertical Rate presented on the HMI due to a mismatch between the value on the track label of the altitude report and the Vertical Rate.

2.3.6.6 It is therefore more appropriate (i.e. worst case) to assess the use of barometric altitude rate as the Vertical Rate presented to the controller. This is because a failure of barometric altitude may be more difficult to detect by the controller since the altitude report will be similarly also be corrupted (otherwise the controller would detect the failure).

2.3.7 Selected Altitude

2.3.7.1 The Selected Altitude represents the 'cleared flight level' as entered by the pilot on the Altitude Control Panel (ACP). It should represent the altitude to which the aircraft is intending to fly, either under the manual control of the pilot or the autopilot.

2.3.7.2 ICAO annex10 volume III states that the parameter will be available through "Selected Altitude from Altitude Control Panel" parameter contained in transponder register number 40_{16} (BDS 4,0H)

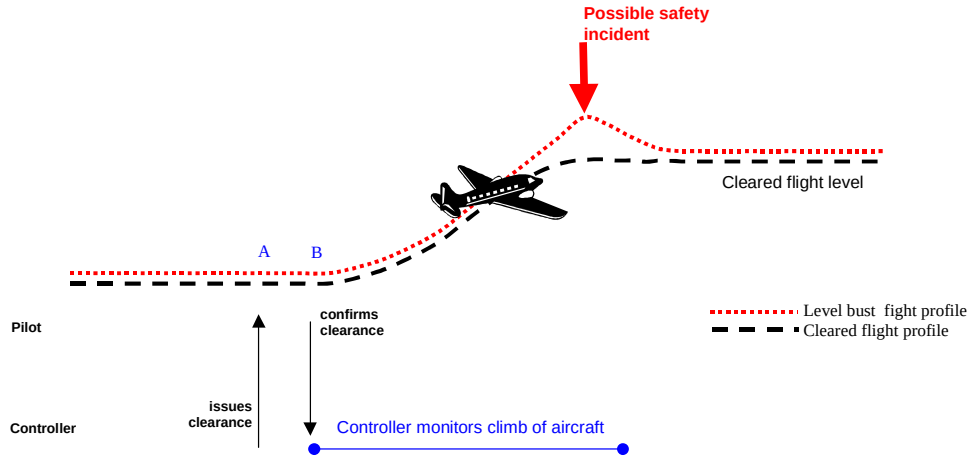


Figure 2 - current operations for Selected Altitude

2.3.7.3 The Cleared Flight Level (CFL) is currently downlinked to the controller via voice. In current operations (illustrated in Figure 2):

- the controller issues a clearance for an aircraft to go to a particular flight level (the CFL), via VHF voice. [A]
- the pilot confirms the CFL to the controller [B]
- the controller monitors the climb/descent of the aircraft at least until the CFL is achieved and maintained.

2.3.7.4 If at any time from when the clearance is issued, if the controller suspects that the pilot has not understood the CFL, the controller will re-issue the clearance. The detection of the mis-understanding is currently through the voice read-back exchange from pilot and controller.

2.3.7.5 In future operations (illustrated in Figure 3) the same procedure will still take place, but will be supplemented by the presentation of the Selected Altitude, downlinked from the Aircraft Control Panel (ACP), on the track label:.

- the controller issues a clearance for an aircraft to go to a particular flight level (the Cleared Flight Level [CFL]), via VHF voice. [A]
- the pilot confirms the CFL to the controller [B]
- the pilot enter the selected altitude (generally the CFL) into the ACP [C]
- the selected altitude is downlinked (via Mode S SSR) and presented to the controller on the track label [D]
- The controller checks the Selected Altitude to detect possible values higher than the CFL for climb or lower than the CFL for descent. If it is the case he contacts the Pilot for verification.
- the controller continues to monitor the climb of the aircraft at least until the CFL is achieved and maintained

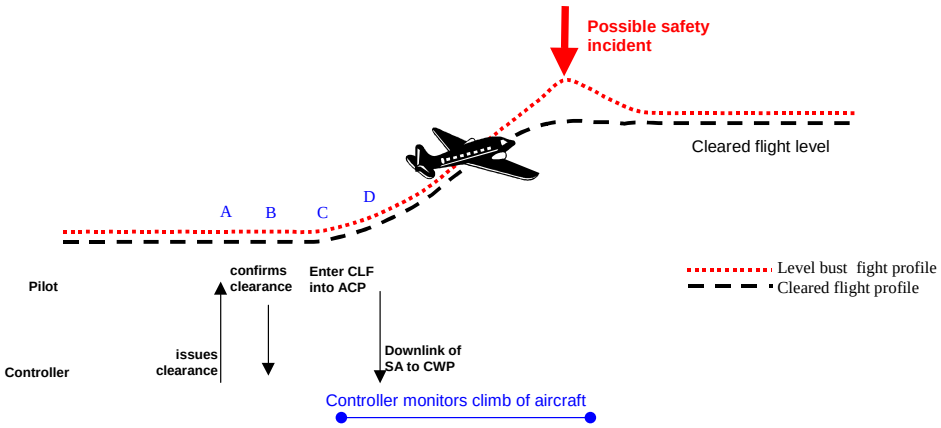


Figure 3 - Future operations for Selected Altitude

2.3.7.6 The controller will be expected to verify the CFL acknowledged via voice and the Selected Altitude value presented on the track label is equal to the CFL. If either of these fail to correlate (i.e. either the voice read-back or the track label value) then the controller will re-issue the clearance. Therefore the use of Selected Altitude is simply as a 'digital readback' to complement voice operations.

2.3.7.7 Selected Altitude does not necessarily represent the aircraft/pilot flight profile (as is the case today with VHF CFL confirmation read-back) but rather the understood CFL of the pilot. Therefore the controller continues to monitor the aircraft throughout the climb/descent manoeuvre in order to ensure the aircraft reaches and does not exceed the CFL. An important assumption used in the later analysis relates to the question “how long is the Selected Altitude used during the climb descent phase?”. It is not applicable during the complete climb, but only applicable during the short term following read-back by the pilot (i.e. shortly after the clearance has been issued). Regardless of the duration of the climb, the analysis assumes the controller will only use Selected Altitude for a time of two minutes following the issue of clearance. This is considered pessimistic, in that the time would probably be lower in reality (i.e. the analysis has assumed much worse than is necessary).

2.3.8 'Level Bust' incident and Selected Altitude

2.3.8.1 In the UK airspace during 2000, the traffic volume was $2x10^6$ flights and approximately 400 level bust incidents [classified as at least 300FT deviation from cleared flight level] were reported. [2]

2.3.8.2 A level bust is an incident that may be caused by many events, ranging from incorrect barometric setting, turbulence, VHF communication confusion and aircrew level busts (see Figure 4). A majority of them can not be detected by the electronic read back of the SA.

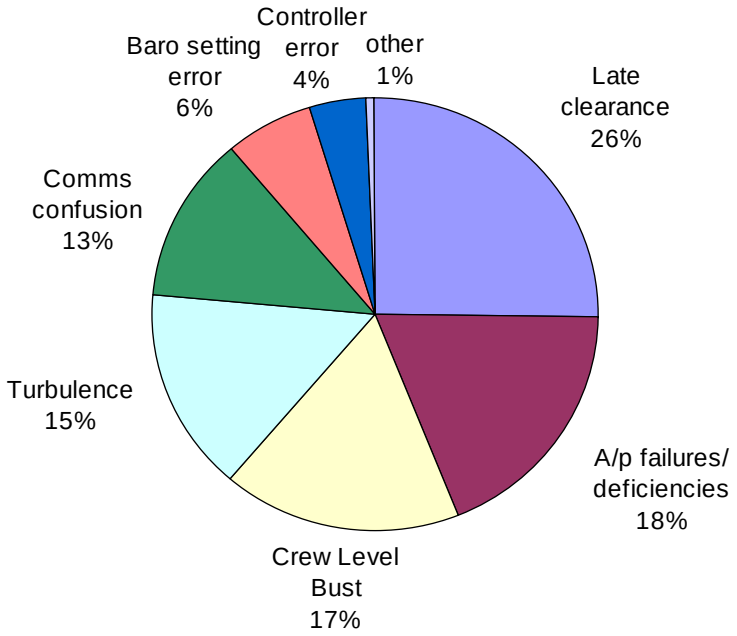


Figure 4 - causes of level bust

2.3.8.3 The use of downlinked Selected Altitude will not eliminate level busts, but may reduce their probability of occurrence. Even if the use of Selected Altitude was 100% reliable, level busts will still occur. However the Selected Altitude can be used by the controller as an early indication of possible level busts and that permits the controller to take corrective measures prior to the possible incident. This implies that there is no guarantee that if the Selected Altitude is equal to the CFL that the aircraft will reach and maintain its CFL, however if they do not match there is high probability that the CFL will not be reached or maintained. **Therefore Selected Altitude shall never be relied upon for separation purposes.**

2.3.8.4 This PSSA examines the use of Selected Altitude as a means to reduce the number of occurrences of VHF communication confusion (13% contributor) and crew level busts (17%) contributor. It is assumes that all other causes for Selected Altitude will still exist and therefore the controller shall remain vigilant and shall continue to monitor the aircraft as is the situation now.

2.3.8.5 Readers should be aware that the future operational scenario assumes that:

[2] Presented at the 2nd Level Bust workshop. Held at Eurocontrol 10-11 October (see http://www.eurocontrol.int/safety/)

- It is general practice for the pilot to enter the CFL into the ACP regardless of what system (the pilot, autopilot or other system) is in control of the aircraft.
- The CFL entered into the ACP corresponds to the Selected Altitude i.e. the Selected Altitude equal the CFL.
- The controller continues to monitor the flight until the CFL is achieved and maintained.

2.3.8.6 It is recognised that, during the course of the execution of a stepped climb/descent, the pilot could enter another value than the CFL (e.g. an intermediate value). In this case the controller will check that the Pilot has not entered a value that goes beyond the CFL. When the Pilot has entered an intermediate value the controller will understand it but might possibly pay more attention to check the conformity of the climb/descent of this aircraft.

2.3.8.7 Similarly, during the final phase of approach the pilot may select a go-around altitude to be prepared for a potential missed approach procedure. This also will have to be recognised and understood by controller/system tools.

2.3.8.8 It is considered in this analysis that, in most of the cases apart from the understood procedures of stepped Climb/Descent and preparation of missed approach, the CFL will be the value entered into the ACP.

2.3.8.9 In summary, Selected Altitude cannot be used to prevent all level busts but the use of Selected Altitude does provide the controller with an additional piece of information to possibly detect the potential for a level bust.

2.3.9 Barometric Pressure Setting

2.3.9.1 It is recognised that the Barometric Pressure Setting parameter could be used in TMAs to complement the use of selected Altitude in the prevention of some level busts (see 2.3.8.2 Baro setting error). Nevertheless this will not protect the system against level bust.

2.3.9.2 When a possible corruption makes a wrong Barometric Pressure Setting not detectable the system will work as the Barometric Pressure setting would not have been available.

2.3.9.3 When a good barometric pressure setting will be corrupted it will generate a false alarm and the controller would try to check the reasons with the pilot.

2.3.9.4 The verification of the impact of this last point on the workload of the controller could only be performed when the operational procedure is established. Such operational procedure details are not available at the moment this document is issued and the necessary safety analysis has to be performed by service providers before implementing such procedure.

3 SYSTEM BOUNDARY AND OPERATION

3.1 System Boundary

3.1.1.1 The system, assessed in the PSSA includes the people, procedures and equipment. The equipment, which is the focus of the PSSA, is the Mode S SSR Enhanced Surveillance system that delivers CAP information to the controller.

3.1.1.2 The principal elements for the delivery of CAP are illustrated in Figure 5. Note that not all the ATM system (e.g. STCA) is considered within the PSSA, but are shown to illustrate the information flows between the pilot, controller and system.

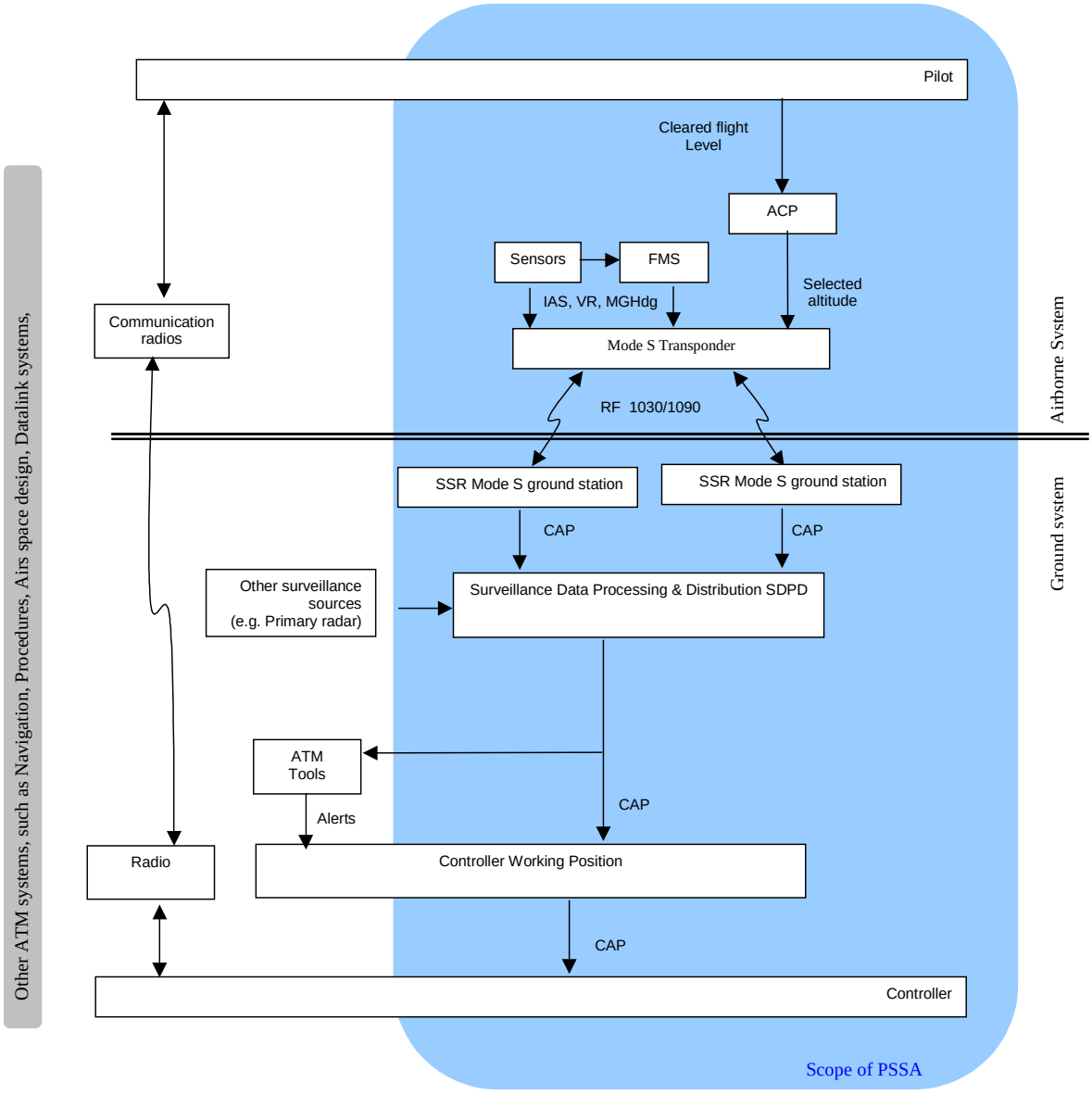


Figure 5 - Principal system elements for the delivery of a CAP service

3.2 System Operation for CAP delivery via Mode S Enhanced Surveillance.

3.2.1.1 All CAPs are entered into various registers in the Mode S transponder, either via the FMS, directly from airborne sensors or the ACP. The source and processing of the CAP are discussed in detail in later sections.

3.2.1.2 The Mode S ground stations first acquire (detect) Mode S equipped aircraft and repetitively interrogate them to develop an accurate estimate of their position. Once acquired and the capability is announced by the aircraft, the CAP data is periodically extracted by the Ground station using a statically defined GICB Mode S protocol.

3.2.1.3 The CAPs are then sent from the ground station to the Surveillance Data Processing and Distribution (SDPD) system and forwarded to the Controller Working Position as data fields in the track item. This implies that:

- A failure in the SDPD will result in a failure of the CAP service. It is assumed that there is a fallback mode providing the Controller Working Position (CWP) directly with radar target reports and CAP if this occurs.
- The SDPD has a management function that collects, stores and forwards CAP to the different users.

3.2.1.4 It is assumed that the system operations meets the performance requirements defined in the CAP service (e.g. the maximum time elapsed between the measurement of the parameter and its delivery to the Controller Working Position shall be less than 8 seconds 99.996% of the time)

3.2.2 CAP presentation on the track label

3.2.2.1 CAP information is presented on the track label in addition to basic surveillance information. Figure 7 presents a "generic" CAP track label as presented at the CWP. Figure 6 augments the illustration with descriptions for each label element.

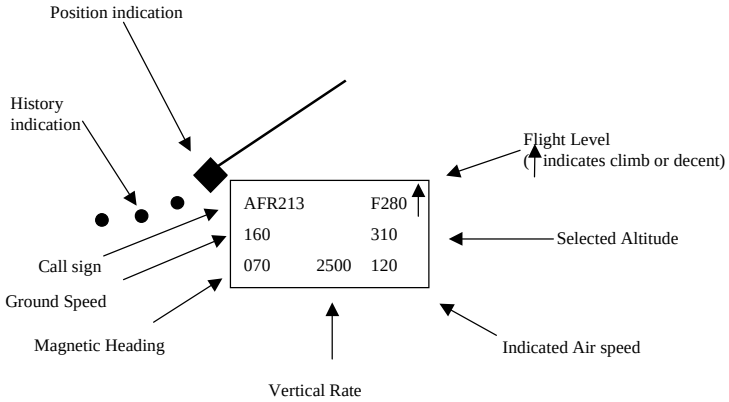
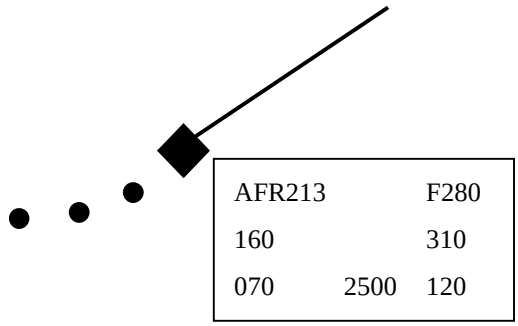


Figure 6 - Track Label Augmented with Parameter Descriptions



Altitude (i.e. Selected and Mode C/altitude report) is displayed at the Workstation in three-digit format, with leading zeros for unused Flight Levels. Thus FL270 is 27,000' (feet) above mean sea level, in standard atmospheric pressure of 1013.2mb.

The Displayed Flight Level is a "passed" level, for example FL271 is 27,100' to 27, 199'. The French Air Navigation System airspace does not increment the displayed flight level until the aircraft is 300ft or more away from the displayed level.

The Controllers will use either IAS or Mach No as appropriate. It is therefore appropriate to assess these as one parameter.

Figure 7 - "Generic" Enhanced Surveillance Track Label

3.2.2.2 Where an equipment failure has occurred and has been detected, it is assumed that the data affected by the failure can be prevented from being presented to the controller either by controller themselves or the supervisor. It is also assumed that such an action would disable the use of the same data in ground tools (i.e. as part of the SAP service) thus reducing the probability of errors being generated by ground systems as a response to the use of that data (e.g. false STCA warning).

3.2.2.3 It is assumed that no modification of the CAP data is performed by the system (but may occur in error) and that the value of the CAP presented on the track label, in normal operations, is the value extracted from the transponder.

4 OPERATIONAL HAZARD ASSESSMENT

4.1 Understanding the results of the OHA

4.1.1 Background

4.1.1.1 The Operational Hazard Assessment (OHA) [reference 6], completed in 2001, defined a number of failure modes and qualifiers to help classify the severity of the failures of the system. For clarity, these are presented in this section.

4.1.2 Failure Modes

4.1.2.1 The failure modes considered within the OHA were as follows:

- Loss of Data
- Misdirected Data
- Delayed Data
- Corruption of Data
- Inconsistent Data
- Spurious and Malicious Data

4.1.2.2 Loss of data by the system results in the data either disappearing from the track label or the track label item not being updated. Clearly if the data disappears from the track label it is reasonable to assume the controller would detect this. However, if it is not updated (i.e. remains at the most recently extracted value) then this is more difficult to detect. If data is misdirected or delayed beyond a reasonable time and hence is not received by the appropriate Controller when required, then the consequences are assumed to be the same as for the Loss of Data failure.

4.1.2.3 Data corruption would result in an incorrect value being displayed on the track label. The controller is increasingly likely to detect corruption as the difference between the expected value and the corrupted value grows. Similarly, inconsistent, spurious and malicious data are treated as examples of data corruption.

4.1.2.4 Therefore the Failure Modes were consolidated into the following:

- Loss of Data (including Misdirected Data, Delayed Data), and;
- Corruption of Data (including Inconsistent, Spurious and Malicious data).

4.1.3 Detected or undetected failure

4.1.3.1 Each failure is either detected or undetected. Detected failures are where the system (equipment, procedures or people) detects the failure and can therefore react to it.

4.1.3.2 An undetected failure occurs when no part of the system detects the loss or corruption of data. This means that the system continues in operation without realising the data is lost or corrupted. Typically the loss of data is detected by the controller (e.g. a value on a track label disappears) and therefore this is considered a ‘detected failure. However where the value on the track label appears correct (e.g. it has not been updated for a period of time) the controller may not detect this.

4.1.4 Number of aircraft affected by the failure.

4.1.4.1 Two aircraft qualifiers are used within the analysis to indicate the aircraft that impact the severity of a failure. Theses are:

- One Mode S equipped aircraft (controlled by a working position);
- More than one Mode S equipped aircraft (controlled by a working position).

4.1.5 Exposure Criteria

4.1.5.1 Exposure criteria capture the speed at which the failure occurs and the duration of the failure.

4.1.5.2 The speed at which a failure occurs is captured as either ‘sudden’ or ‘progressive’. Figure 8 illustrates a sudden and progressive failure for a number of aircraft, where, the sudden failure (e.g. loss of the surveillance function) would impact a large number of aircraft at a particular time, contrasted with a progressive failure impacting on a successive number of aircraft.

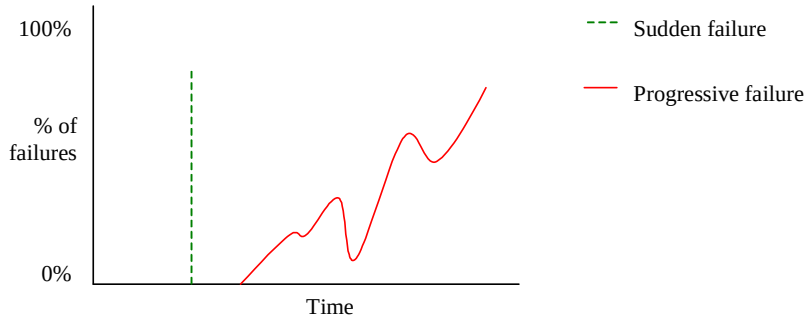


Figure 8 - sudden and progressive failure

4.1.5.3 The duration of a failure is captured as either ‘short’ or ‘continuous, where short is defined as less than two radar scans and continuous greater than two radar scans.

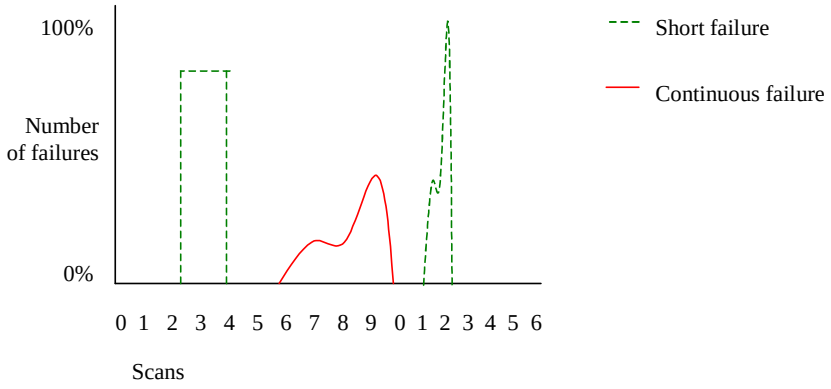


Figure 9 - short and continuous failure

4.2 Severity Classification

4.2.1.1 For each failure mode the impact on air traffic safety is assessed and classified according to the categories in Table 1, based on ESSAR 4 [reference 3].

Severity Class	Effect on Operations	Examples of effects on operations Include:
1 [Most Severe]	Complete loss of safety margins	Accidents, including:- one or more catastrophic accidents, one or more mid-air collisions one or more collisions on the ground between two aircraft one or more Control Flight Into Terrain Total loss of flight control. No independent source of recovery mechanism, such as surveillance or ATC and/or flight crew procedures can reasonably be expected to prevent the accident(s).
2	Large reduction in safety margins	Serious incidents, including:- (a) large reduction in separations (e.g., higher than half the separation minima), without crew or ATC fully controlling the situation or able to recover from the situation. one or more aircraft deviating from their intended clearance, and Abrupt collision or terrain avoidance manoeuvre are required to avoid an accident (or when an avoidance action would be appropriate).
3	Major reduction in safety margins	Major incidents. (a) large (e.g., higher than half the separation minima) reduction in separations with crew or ATC controlling the situation and able to recover from the situation. (a) major (e.g., lower than half the separation minima) reduction in separation without crew or ATC fully controlling the situation, hence jeopardising the ability to recover from the situation (without the use of collision or terrain avoidance manoeuvres).
4	Slight reduction in safety margins	Significant incidents. No direct impact on safety but indirect impact on safety by increasing the workload of the air traffic controller or aircraft flight crew, or slightly degrading the functional capability of the enabling CNS system. (a) major (e.g., lower than half the separation minima) reduction in separations with crew or ATC controlling the situation and fully able to recover from the situation.
5	No effect on safety.	No hazardous condition i.e. in direct or indirect impact to the operations.

Table 1 - ESSAR 4 Severity Classification Scheme

4.2.1.2 In a number of cases the experts performing the OHA recognised that there were different safety implications of the loss of a particular parameter between En-route and TMA/approach airspace. However, based on the definitions in ESSAR 4, the difference did not cause the severity class to change. As a result it was agreed to distinguish between higher and lower levels within a severity in each class. This is indicated as, for example, 4+ and 4- for the higher and lower bounds of severity class 4 where 4+ is closer to severity class 5 and 4- is closer to severity class 3.

4.3 Summary of OHA

4.3.1.1 Table 2 presents a summary of the severity classification for Elementary and Enhanced Surveillance when used in 'En-route' and TMA/Approach, obtained as a result of the OHA. This presents the link between the cause (failure mode) and consequence (severity classification). The severity classification represents the most severe possible consequence of an incident under certain circumstances (the failure mode) and under an operational environment (type of airspace, traffic density, operation procedures,…).

4.3.1.2 It is important to recognise that, in the case of CAP, an ATC incident is not guaranteed to happen if that failure mode occurs because the controller has a large number of other tools available to them to control aircraft safely. For example the use of Selected Altitude is for the early detection, and therefore resolution, of a level bust does not imply that if the use of Selected Altitude fails then a level bust is guaranteed to occur. It does imply that if, for example, the corruption of Selected Altitude was undetected then one means of detecting a potential future level bust has failed and there is a potential for a possible level bust to occur (as it does today if the voice read-back fails).

4.3.1.3 The severity classification is therefore the most severe consequence of a failure mode, but not the guaranteed consequence. In the case of Selected Altitude, one possible consequence of an undetected corruption of Selected Altitude maybe a level bust, which has been classified as severity class 2. Likewise, if Vertical Rate were corrupted and undetected, there is the possibility of loss of separation, which is classified as severity class 3.

Related Safety Objective (see 5.2)	CAP	Failure Mode			Number of Aircraft		Severity Class	
		Sudden [S] or Progressive [P][3]	Short [S] or Continuous [C]	Detected [D] or Undetected [U]	One aircraft	More than one aircraft	En-route	TMA / Approach
SO1	Selected Altitude	S	S	D	✓		5	5
SO2	Selected Altitude	S	S	D		✓	4	4
SO3	Selected Altitude	S	C	D	✓		4+	4-
SO4	Selected Altitude	S	C	D		✓	4	4
SO5	Selected Altitude	P or S	S or C	U	✓		2	2
SO5	Selected Altitude	P or S	S or C	U		✓	2	2
SO6	Vertical Rate	S	S	U or D	✓	✓	5	5
SO7	Vertical Rate	S	C	D	✓		5	5
SO8	Vertical Rate	S	C	D		✓	4	4
SO9	Vertical Rate	P or S	S or C	U	✓		4+	4-
SO10	Vertical Rate	P or S	S or C	U		✓	3+	3-
SO11	Magnetic Heading	S	S	U or D	✓	✓	5	5
SO12	Magnetic Heading	S	C	D	✓		5	4
SO13	Magnetic Heading	S	C	D		✓	4+	4-
SO14	Magnetic Heading	P or S	S or C	U	✓		5	5
SO15	Magnetic Heading	P or S	S or C	U		✓	4+	4-
SO16	Indicated Air Speed	P or S	C	D	✓		5+	5-
SO17	Indicated Air Speed	P or S	C	D		✓	4	4
SO18	Indicated Air Speed	P or S	S or C	U	✓		4	4
SO18	Indicated Air Speed	P or S	S or C	U		✓	4	4

Table 2 - Summary of Severity Classifications

[3] In many cases, progressive failures of CAPs are not applicable because the controller is expecting a single, discrete value (e.g. Selected Altitude). Any deviation from the expected value would be identified immediately by the controller and is therefore considered as a sudden failure.

5 SAFETY OBJECTIVES

5.1 Assumptions for Deriving Safety Objectives

5.1.1.1 Safety Objectives specify the maximum tolerable probability for the occurrence of a hazard of a given severity, including a maximum exposure time.

5.1.1.2 ESARR4 defines maximum tolerable probability (of ATM direct contribution) for incident of severity class 1 as 1.55×10^{-8} accidents per flight hour. No values are presented for severity class 2, 3, 4 or 5.

5.1.1.3 For the analysis within this paper, it is assumed that there is a 10^2 [4] factor between the severity classes and the maximum tolerable probability (of ATM direct contribution) the acceptable number of incidents per flight hour. At present there is no data to support or contradict this assumption. The analysis therefore assumed the following maximum tolerable probability (of ATM direct contribution) incidents per flight hour as a reasonable starting point.

Severity Class	1	2	3	4	5
Maximum tolerable probability (of ATM direct contribution)	1.55×10^{-8}	1.55×10^{-6}	1.55×10^{-4}	1.55×10^{-2}	Not relevant

Table 3 - Maximum tolerable probability for ATM contribution.

5.1.1.4 The maximum acceptable probability of occurrence for each severity class applies to the complete ATM system. The surveillance services, including CAP, provided by the Mode S system are a small part of the complete ATM system. An assumption is required to apportion the contribution of these to the overall system failure.

[4] Expert estimate based on approach currently used for airborne equipment

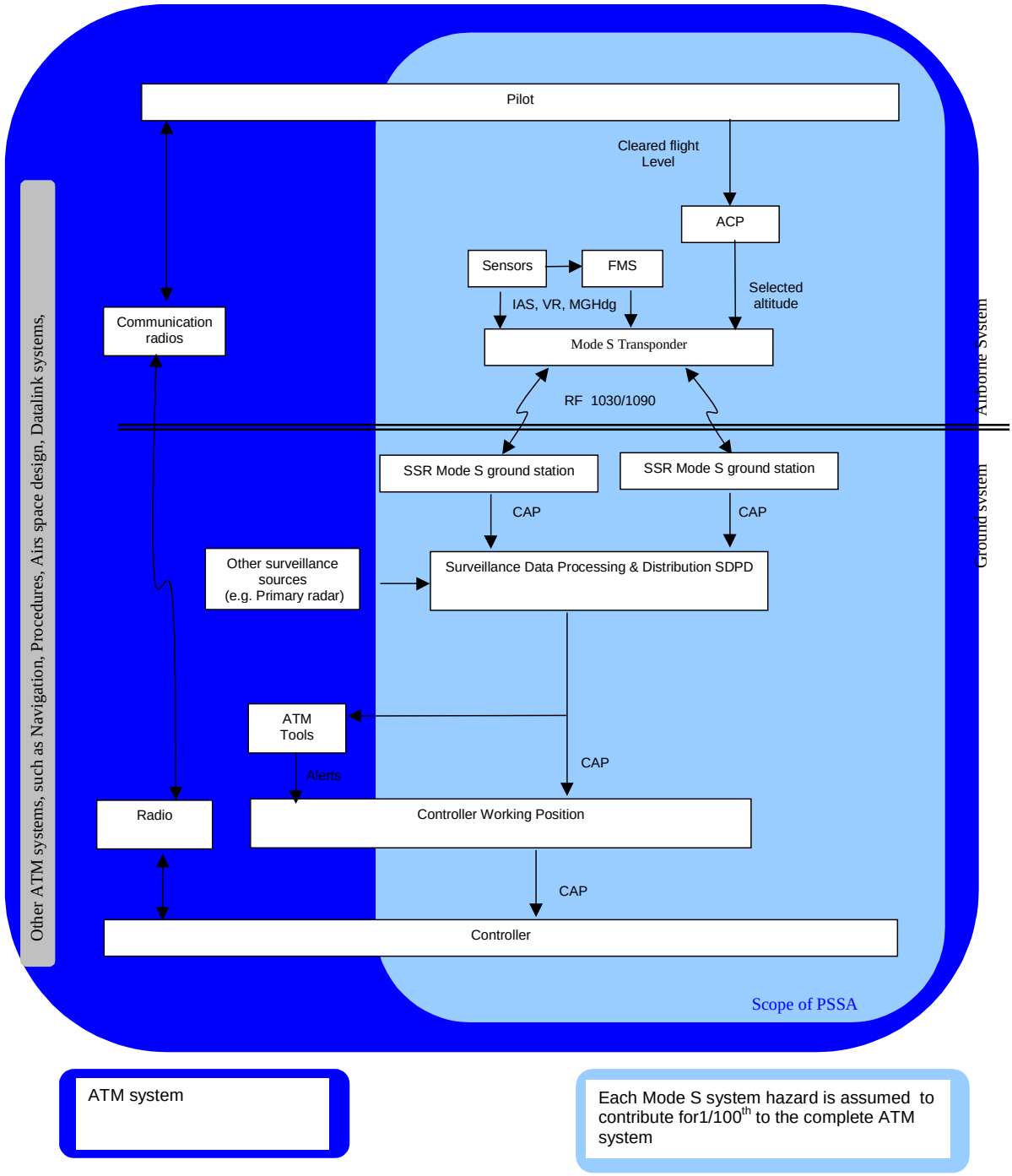


Figure 10 Derivation of Mode S safety Objectives

5.1.1.5 This analysis assumes that any single hazard will be given the 'upper-risk limit' objective of contributing **1%**[5] maximum to the overall ATM contribution for a given severity class.

5.1.1.6 Therefore, the analysis takes the maximum tolerable probability of a single Mode S Surveillance/CAP hazard contributing to the ATM failure incidents per flight hour as defined in Table 4.

[5] Mode S safety task Force Expert estimate based on 10 sub-functions and 10 hazards of the same severity per sub-function resulting in approximately 100 hazards of a given severity in an ATM system..

Severity Class	1	2	3	4	5
Maximum tolerable probability (of a single Mode S failure direct contribution)	$1.55x10^{-10}$	$1.55x10^{-8}$	$1.55x10^{-6}$	$1.55x10^{-4}$	Not relevant

Table 4 - Maximum tolerable probability for each Mode S hazard contribution.

5.2 CAP Safety objectives

5.2.1 Selected Altitude

5.2.1.1 The Mode S Safety Task Force was tasked to classify the impact of corrupted SA. In reality SA is only part of the process which the controller uses to confirm the correct understanding of the issued CFL (i.e. the use of VHF voice is also used as a read-back means). It is not possible to independently assign a safety objective to an undetected corruption of SA without considering it in the complete process of confirming the CFL. Consequently in this section the scope of the safety objectives have been widened to encompass the CFL as opposed to the SA.

SO1. Not relevant

SO2. The occurrence of a detected corruption of CFL due to a corruption of SA (false alarm) for a short period of time for more than one aircraft shall occur with a probability of occurrence less than $1.55x10^{-4}$ per flight hour in en-route and approach environment.

SO3. The occurrence of a detected corruption of CFL due to a corruption of SA (false alarm) for a continuous period of time for one aircraft shall occur with a probability of occurrence less than $1.55x10^{-4}$ per flight hour in en-route and approach environment.

SO4. The occurrence of a detected corruption of CFL due to a corruption of SA (false alarm) for a continuous period of time for more than one aircraft shall occur with a probability of occurrence less than $1.55x10^{-4}$ per flight hour in en-route and approach environment.

SO5. The occurrence of an undetected corruption of CFL for a short or continuous period of time for one or more aircraft shall occur with a probability of occurrence less than $1.55x10^{-8}$ per flight hour in en-route and approach environment.

5.2.1.2 The safety objectives SO1/2/3/4 correspond to an airborne CFL displayed on the CWP not corresponding to the initial clearance not because the pilot had not correctly understood it or entered it but because the system has corrupted it. This results in a wrong value displayed on the CWP. This is detected by the controller and confirmed using RT. This is a false alarm on CFL resulting in an increase of the Controller workload.

5.2.1.3 For the undetected corruption it was not possible to isolate a requirement without considering the complete process associated to the management of CFL. This is why the non detection of an airborne FL not corresponding to the initial clearance has been classified with a severity level 2 because as it will result in a level bust.

5.2.2 Vertical Rate

5.2.2.1 Based on the OHA results the following safety objectives are defined for Vertical Rate when used for the CAP service delivered by Mode S Enhanced Surveillance

SO6. Not relevant

SO7.	Not relevant
SO8.	The occurrence of a sudden, detected corruption of Vertical Rate for a continuous period of time for more than one aircraft shall occur with a probability of occurrence less than $1.55x10^{-4}$ per flight hour in en-route and approach environment.
SO9.	The occurrence of an undetected corruption of Vertical Rate for a short or continuous period of time for one aircraft shall occur with a probability of occurrence less than $1.55x\ 10^{-4}$ per flight hour in en-route and approach environment.
SO10.	The occurrence of an undetected corruption of Vertical Rate for a short or continuous period of time for more than one aircraft shall occur with a probability of occurrence less than $1.\ 55x\ 10^{-6}$ per flight hour in en-route and approach environment.

5.2.3 Magnetic Heading

5.2.3.1 Based on the OHA results the following safety objectives are defined for Magnetic Heading when used for the CAP service delivered by Mode S Enhanced Surveillance

SO11.	Not relevant
SO12.	The occurrence of a sudden, detected corruption of Magnetic Heading for a continuous period of time for one aircraft shall occur with a probability of occurrence less than $1.55x10^{-4}$ per flight hour in a TMA environment.
SO13.	The occurrence of a sudden, detected corruption of Magnetic Heading for a continuous period of time for more than one aircraft shall occur with a probability of occurrence less than $1.55x10^{-4}$ per flight hour in the TMA/approach environment.
SO14.	Not relevant
SO15.	The occurrence of an undetected corruption of Magnetic Heading for a short or continuous period of time for more than one aircraft shall occur with a probability of occurrence less than $1.55x10^{-4}$ per flight hour in an en-route and TMA/approach environment

5.2.4 Indicated Airspeed

5.2.4.1 Based on the OHA results the following safety objectives are defined for Indicated Airspeed when used for the CAP service delivered by Mode S Enhanced Surveillance

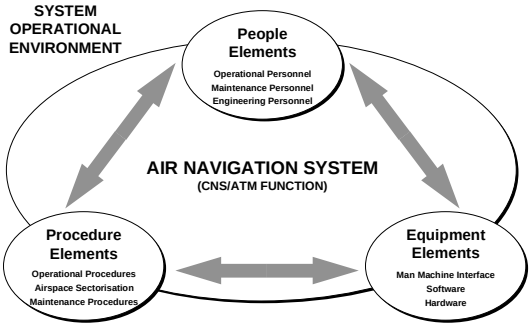
SO16.	Not relevant
SO17.	The occurrence of a detected corruption of Indicated Airspeed for a continuous period of time for more than one aircraft shall occur with a probability of occurrence less than $1.55x10^{-4}$ per flight hour in an en-route and TMA/approach environment
SO18.	The occurrence of an undetected corruption of Indicated Airspeed for a short or continuous period of time for one or more aircraft shall occur with a probability of occurrence less than $1.55x10^{-4}$ per flight hour in an en-route and TMA/approach environment.

6 SAFETY ASSESSMENT.

6.1 Introduction

6.1.1.1 This section assesses whether the end-to-end ATM infrastructure, which includes the Mode S SSR, is capable of meeting the safety objectives for each CAP.

6.1.1.2 The system is comprised of equipment, procedures and humans. Therefore the analysis assumes a corruption of the CAP can occur based on errors by the pilot, corruption by the technical system or errors from the controller. Any or all of these can contribute to an undetected corruption of the CAP and result in the safety consequence.



6.1.1.3 The most stringent Safety Objectives of each CAP are used to assess whether the Mode S Enhanced Surveillance system is a suitable datalink delivery system.

6.2 Probability of undetected corruption caused by the equipment

6.2.1 General

6.2.1.1 Common to all the analysis is the probability of corruption of a particular CAP by the avionics and/or the ground systems. This section develops the probability of corruption, per flight hour, for each component and the resultant probability for the end-to-end technical system. The results presented here are then used by the analysis for each CAP.

6.2.2 Corruption by the Avionics

6.2.2.1 From an airborne perspective, a JAA position paper [8] proposes that the classification for aircraft identification is 'minor'.
AC/AMJ.25.1309 [9] section 8 indicates a probability of loss or corruption (both detected or undetected) for this classification of between 1 and 10^{-5} per flight hour.
This analysis assumed that the probability of loss or corruption of information from the avionics is 10^{-3} per flight hour. Based on the assumption that 10% of these failure are not detected it is furthermore assumed that the probability of undetected loss or corruption of an information from the avionics is P_av:

P_av = 10^{-4} per flight hour [6]

(Initially a figure of 10^{-3} was used but it was recognised as a too pessimistic figure not corresponding to the reality by avionics manufacturers)

[6] Expert estimate based on a minor classification of corresponding avionics. Probability confirmed by an Airframe manufacturer who uses a probability of 5 x 10^{-5}.

6.2.2.2 P_av is the sum of all the failures that can occur in the avionics. The consequences can vary depending on the failure. The PSSA assumes the following decomposition of the consequences relating to avionics failures:

- **90%**[7] of failures result in loss of data (e.g. typically hardware failure where no data is processed or transmitted by the transponder; the consequence is that the aircraft is not detected by the ground system)
- **9%** result in corruption of data content (e.g. corruption of Mode A, or aircraft identification)
- **1%** result in corruption of position information

6.2.2.3 The above assumptions result in the following probabilities for avionics failure per flight hour

P_av_loss	= P_av *.0.9	= 9 x 10^{-5} per flight hour.
P_av_ data_corruption	= P_av *.0.09	= *9 x 10^{-6}* per flight hour.
P_av_pos_corruption	= P_av *.01	= 1 x 10^{-6} per flight hour.

6.2.3 Corruption by the Ground system

6.2.3.1 Corruption by the ground system can occur from when the CAP is transmitted by the avionics (i.e. air/ground transmission) to when it is presented to the controller. These various system component corruption probabilities are listed below

6.2.3.2 The probability of undetected corruption of air to ground (RF) messages is

P_rf = 10^{-7} per message[8].

6.2.3.3 In order to simplify the calculation for Mode S SSR corruption, it is assumed that only one station extracts and sends the CAP. The POEMS safety study estimated the probability of undetected corruption for Mode C/altitude report by radar to be

P_1Radar_uc_data = 5.6 x 10^{-7} per message[9]

6.2.3.4 The probability of undetected corruption by the Ground to ground communication network is

P_ground_net = 10^{-9} per message[10].

6.2.3.5 Therefore, the probability of undetected corruption of a single message by the RF, radar or ground network is:

[7] Mode S Safety Task Force Expert estimate based on experience with SSR Mode A/C transponders (majority of problems results in loss of detection)

[8] ICAO Manual of the Secondary Surveillance radar (SSR) systems (DOC 9684) First Edition 1997. Appendix 1 Paragraph 1.3.

[9] POEMS FTA 6108900/000 Issue 1.0 June 2002 section 7.1 altitude and identity corruption + detailed fault tree indicating the Site undetected corrupted height data at scan 1

[10] Typical values usually used for undetected corruption within X25 ground network

$$P\_extraction\_message = P\_rf + P\_1Radar\_uc\_data + P\_ground\_net$$

$$= 10^{-7} + 5.6 \times 10^{-7} + 10^{-9}$$

$$= 6.6 * 10^{-7} \text{ per CAP extraction}$$

6.2.3.6 It is assumed that one extraction of the CAP will be performed each radar scan. In the TMA (which is faster than en-route) a scan takes place every **4**[11] seconds, therefore during one flight hour, 900 extractions will take place per CAP. This results in a probability of undetected corruption of a single CAP (over one hour of operation) by the RF, radar or ground network is:

$$P\_extraction\_hour = P\_extraction\_message \times 900$$

$$= 5.9 * 10^{-4} \text{ per flight hour.}$$

6.2.3.7 Taking into account the contribution of SDPD, where the probability of undetected partial loss or corruption of track information service indicated for ARTAS is **P_sdpd_hr = 1.2 x 10^{-4} /h**[12].
The probability of error per flight hour is obtained by dividing P_sdpd_hr per the number of flight hours managed by the SDPD in one hour of operation. Based on the hypothesis of **1000 flights per hour of operation** and on a duration of **15mn** for each flight it gives 250 flight hours[13] for a TMA over 1 hour of operation

$$P\_sdpd\_tma = P\_sdpd\_hr / 250$$

$$= 1.2 \times 10^{-4} / 250$$

$$= 4.8 \times 10^{-7} \text{ per flight hour}$$

6.2.3.8 No estimates are available to assess the impact of the Controller Working Position.

6.2.3.9 Hence, the probability of undetected corruption of a single CAP, by the ground system is

$$P\_gnd = P\_extraction\_hour + P\_sdpd\_tma$$

$$= 5.9 * 10^{-4} + 4.8 \times 10^{-7}$$

$$= 5.9 \times 10^{-4} \text{ per flight hour}$$

6.2.4 Corruption by the Equipment

6.2.4.1 The probability of a corruption of a CAP during one flight hour by the equipment is therefore:

[11] Typical rotation period of an approach radar (the surveillance standard allows up to 5s refresh rate)
[12] ARTAS dependability study - Final Report December 1998 CENA/NT97613/SDF version 1.1 section 4 page 130 FE1.2 “undetected partial loss of track information”
[13] A recording of 1 hour at Duesseldorf Mode S station shows 170000 plots corresponding to 283 flight hours when multiplying by the 6s rotation period

P_equipment = P_av_data_corruption + P_gnd

= $9 \times 10^{-6} + 5.9 \times 10^{-4}$

= 6×10^{-4} per flight hour

6.3 CFL/Selected Altitude

6.3.1 Safety Objective

6.3.1.1 The PSSA approach is based on the assessment of the most stringent safety objective. For CFL this is SO5a, which states “The occurrence of undetected corruption of CFL for a short or continuous period of time for one or more aircraft shall occur with a probability of occurrence less than 1.55×10^{-8} per flight hour in en-route and approach environment”.

6.3.2 Method used to estimate the probability of undetected corrupted CFL

6.3.2.1 For an occurrence of undetected corruption of CFL, the following scenario must occur:

- a level change is required and new CFL is passed, via VHF voice to the pilot, and;
- either:
- the voice read-back fails to detect the corruption (i.e. the controller fails to detect the incorrect value) and/or;
- the pilot enters an incorrect flight level (not the cleared flight level issued by the controller), then
- either:
- the airborne or ground systems corrupt the Selected Altitude into a credible value (therefore the controller cannot detect the corruption) or
- the controller fails to detect the incorrect value.

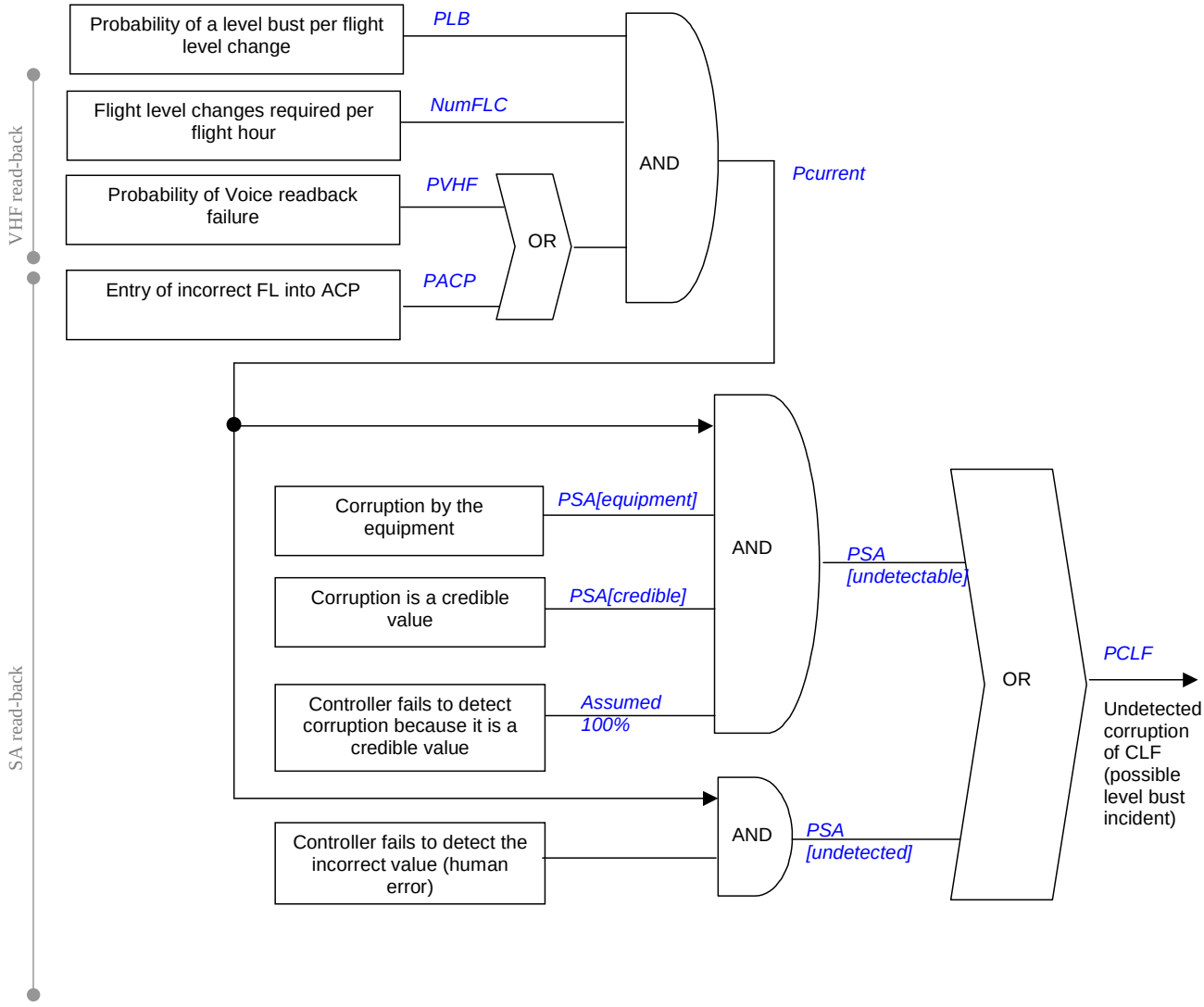


Figure 11 - Contributors to undetected corruption of Selected Altitude

6.3.2.2 These are estimated as follows:

1. *PLB* is the probability of a level bust per flight level change (see 6.3.3.4);
2. *NumFLC* is the average number of flight level changes per flight hour (per flight hour) (see 6.3.3.2);
3. PVHF is the probability that the VHF voice read-back fails (i.e. the controller fails to detect the pilot has responded with an incorrect flight level) (see 6.3.3.5);

4. *PACP* is the probability that the pilot enters an incorrect flight level (not the CFL issued by the controller) into the ACP when following a new change altitude. The probability of such an event will be expressed as pure mathematical value (note that this is not validated in today's operational environment) (see 6.3.3.6);
5. *PSA[undetectable*] is the probability that the 'system' corrupts the incorrect flight level entered into the ACP at least once during the use of the data by the controller and the corruption results in a value expected by the controller. The probability of such an event will be expressed as pure mathematical value (see 6.3.4.2);
6. *PSA [undetected]* is the probability that the controller fails to detect the corruption of Selected Altitude. The probability of such an event will be expressed as pure mathematical value (see 6.3.4.6).

6.3.3 Probability of undetected corruption of cleared flight level in current operations

6.3.3.1 The probability of undetected corruption of cleared flight level per flight hour in current operations is P_current:

P_current = PLB x NumFLC x (PVHF+ PACP)

Number of level changes per flight hour *(NumFLC)*

6.3.3.2 ECAC statistics show that there is on average **13** different altitude changes during 1 flight and the average duration of one flight in the ECAC area is **1.38 hour**, therefore the number of flight level changes per flight hour is NumFLC.

Nb_altitude_changes_per_flight = 13[14] [15]

Average_duration_of_1_flight = 1.38 hour[16]

NumFLC = Nb_altitude_changes_per_flight / Average_duration_of_1_flight

NumFLC = 13 /1.38

NumFLC = 10 changes of flight level per hour

Estimating undetected corruption in current operations (Pcurrent)

6.3.3.3 In the UK airspace during 2000, the traffic level was **$2x10^6$ flights** and approximately **400**[17] level bust incidents [classified as at least 300FT deviation from CFL] were reported.

6.3.3.4 The probability of a level bust, based on average duration of 1 hour[18] per flight and NumFLC per hour in UK airspace is PLB (a simple probability per flight level change).

[14] Estimate based on ECAC statistics
[15] order of magnitude confirmed: 15 level changes per flight in London TMA and 10 in US see Attachment 2 p28 of "CAP 710 LEVEL BUST WORKING GROUP 'ON THE LEVEL' PROJECT FINAL REPORT CAA, LONDON, December 2000
[16] Estimate based on ECAC statistics
[17] See Eurocontrol safety letter 06/2001
[18] It has been highlighted that UK NATS use a figure of 40 minutes for an average flight duration

$$PLB = \frac{\text{Reported incidents per year}}{\text{Nb of flights per year x flight duration in UK x NumFLC}}$$

$$= \frac{400}{2\times10^{6}\times1\times10} = 2\times10^{-5}$$

6.3.3.5 Figure 12 illustrates that 13% of level busts were caused by 'comms confusion'. Therefore the probability of VHF voice readback failure is PVHF.

PVHF = 13%

6.3.3.6 Figure 12 also illustrates that 17% were cause by 'crew level busts' which are assumed to be unintentional mis-entry into ACP, which leads to a probability of an incorrect entry into the ACP by the pilot of PSA[ACP].

PACP = 17%

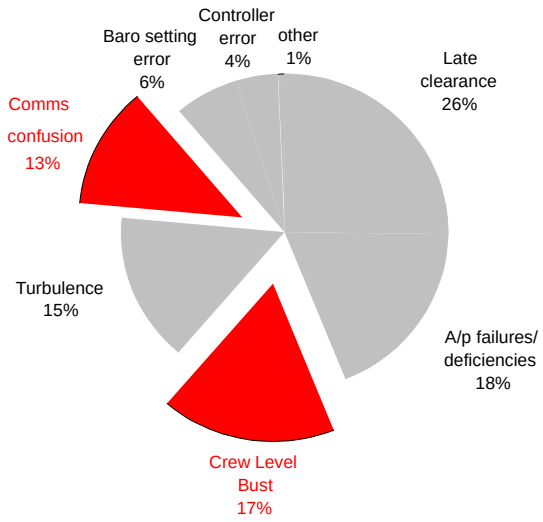


Figure 12 - causes of level bust[19]

6.3.3.7 Assuming that a flight is one hour then, the undetected corruption of CFL, due to either VHF communication or incorrect entry into the ACP is P_current.

P_current = PLB x NumFLC x (PVHF + PACP)

= $(2x10^{-5})$ x 10 x (13% + 17%)

= 6×10^{-5} per flight hour

6.3.4 Probability of undetected corruption of cleared flight level in future operations

6.3.4.1 The use of Selected Altitude in the readback phase reduces the probability of undetected corruption of cleared flight level per flight hour to PCFL:

PCFL= PSA[undetectable] + PSA[undetected]

Corruption by the Equipment of Selected Altitude during the read back (PSA[equipment])

6.3.4.2 Using the assumption that the controller will make use of Selected Altitude for 2 **minutes**[20] during a flight level change (i.e. in the monitoring process during the flight level change) and one undetected corruption in the two minute period constitutes a failure then the probability that the equipment corrupts at least once the Selected Altitude over a two minute period for 1 flight level change is PSA[equipment]

[19] Presented at the 2nd Level Bust workshop. Held at Eurocontrol 10-11 October (see http://www.eurocontrol.int/safety/)
[20] Mode S Safety Task Force Expert estimate

PSA[equipment] = P_equipment x 2 mn /60 mn

$= 6 \times 10^{-4} \times 2 / 60$

$= 2 \times 10^{-5}$

Corruption by the Equipment of Selected Altitude into a credible value (PSA[undetectable])

6.3.4.3 A credible occurrence of undetected corrupted Selected Altitude by the controller can only happen when the value presented to the controller is equal to the value of the CFL. This can only happen when the random corruption of the 12 bits which encode Selected Altitude in BDS 4,0 equals the CFL[21]

6.3.4.4 The probability of a random corruption from the ACP entry into the clear flight level is PSA[credible]:

$$PSA[credible] = \frac{1}{2^{12}} = \frac{1}{4096} = 2.4x10^{-4}$$

6.3.4.5 The probability that corruption of the second read-back (using Selected Altitude) is undetectable by the controller is PSA[undetectable].

PSA [undetectable] = P_current x PSA[equipment] x PSA[credible]

$= (6 \times 10^{-5}) \times (2 \times 10^{-5}) \times (2.4 \times 0^{-4})$

$= 2.9 \times 10^{-13}$

Undetected by the controller (PSA[undetected])

6.3.4.6 The probability that the controller fails to detect a corruption is much harder to quantify. Therefore an assumption must be made. For the purpose of this analysis, it is assumed that the controller fails to detect this at a rate of P_controller which states that 1 in 1000 errors of a CAP on the track label will be missed by the controller. In context, this implies that, if a controller handles 20 aircraft per hour and each aircraft performs 10 flight level changes per hour (i.e. NumFLC), then the controller will fail to detect a fault in the track label once every five hours.

P_controller = 1 x 10^{-3} [22]

6.3.4.7 It is assumed that no additional mitigation means are implemented in order to detect a corrupted CFL during the second read-back. Therefore the probability that corruption of the second read-back (using Selected Altitude) is undetected by the controller is PSA[undetected].

[21] Note the 12 bits have 2^{12} possible combinations

[22] Errors of omission when the actions are embedded in a well-rehearsed procedure are estimated to be **3.0 x 10^{-3}** in IEC 300-3-8 Dependability management/ Part3 sect.8: Human reliability.

PSA[undetected] = P_current x P_controller

$= 6 \times 10^{-5} \times 1 \times 10^{-3}$

$= 6 \times 10^{-8}$

6.3.5 Probability of an undetected corruption of Cleared Flight Level in future operations with the downlinking of SA.

6.3.5.1 The probability of an undetected corruption of the Selected Altitude per flight hour is PCFL.

PCFL = PSA[undetectable] + PSA[undetected]

$= (2.9 \times 10^{-13}) + (6 \times 10^{-8})$

$= 6 \times 10^{-8}$ per flight hour

6.3.6 Discussion on undetected corruption of CFL (SO5)

6.3.6.1 The safety objective (SO5) for an undetected corruption of Cleared Flight Level during the readback process is **1.55×10^{-8}** per flight hour.

Operations are currently achieving (P_current) **6×10^{-5}** per flight hour.

The introduction of an additional readback through the use of Selected Altitude, reduces the probability of undetected corruption to **6×10^{-8}** per flight hour, thereby improving safety to within a factor of three of the safety objective.

6.3.6.2 If it is noted that if the controller detects all errors on the track label (i.e. PSA[undetected] is reduced to zero) then the probability of an undetected corruption of the Selected Altitude per flight hour is P[undetectable], i.e. 3.5×10^{-13} per flight hour. This is clearly not achievable, but a possible step towards this may be possible through the use of an automated tool, such as a Level Bust Alerting Tool (LBAT)

6.3.6.3 Even though the PSSA has indicated that the safety objective is achievable, it is extremely important to emphasise that a level bust can still occur even with a perfect technical system (i.e. no corruption). This is because there are many other factors which cause a level bust that cannot be resolved simply through the read-back process (e.g. manual flight, turbulence, …). It is therefore important that the training of controller emphasises that the use of Selected Altitude, as for today's use of VHF read-back, does not guarantee an aircraft will level at the cleared flight level. A level bust can still occur whether the value on the track label is equal to the cleared flight level or not.

6.3.6.4 The PSSA has assumed that an undetected failure in the readback process (either through VHF or SA) may result in a level bust, which the Operational Hazard Assessment classified as severity class 2. This is based on the possibility that a controller makes '*decisions with respect to separation of aircraft based on incorrect information where a number of aircraft may not be flying to their cleared flight level, or flying to the cleared flight level occupied by other aircraft*."

6.3.6.5 It should be emphasised that PCFL is not the probability of a Level Bust. The use of Selected Altitude as a CAP may contribute to a reduction of the number of level busts. However the results in this paper should not be mis-interpreted to indicate that the use of

Selected Altitude will eliminate level busts. Level busts will not be entirely prevented by the presentation of Selected Altitude on the track label. There will remain safety risks in the fact that the pilot understands the clearance and selects the correct Selected Altitude, but nevertheless flies the aircraft across the cleared level and generates a level bust. Controllers will still be required to monitor the climb/descent to ensure that the cleared level is achieved and not over-shot, irrespective of whether the track label indicates a correct value.

6.3.6.6 The analysis is based on an operational concept that is augmented from current practices, by the provision of Selected Altitude on the track label. Therefore the use of voice communications in the initial read-back of the cleared flight level and the role of the controller in monitoring the climb of the aircraft throughout the complete operation until the cleared flight level is achieved and maintained shall continue unchanged. In addition, the assumption is that the pilot will enter, as normal practice, the cleared flight level into the ACP. All of these are, to some extent, implemented today but training should re-enforce their continued application when Enhanced Surveillance becomes widespread.

6.3.7 Discussion on detected corruption of CFL (SO2/SO3/SO4)

6.3.7.1 The objective is check if the system is not corrupting too often the displayed Selected Altitude in order to avoid too much load for the controller to check for errors which do not exist.

6.3.7.2 SO2: The occurrence of a detected corruption of CFL due to a corruption of SA (false alarm) for a short period of time for more than one aircraft shall occur with a probability of occurrence less than $1.55x10^{-4}$ per flight hour in en-route and approach environment.

The independent corruption of Selected Altitude for a short period of time is equal to the probability of corruption during the read back and corresponds to PSA[equipment]. For two aircraft the probability is PSA [equipment] x PSA[equipment] = $2 \times 10^{-5} \times 2 \times 10^{-5} = 4 \times 10^{-10}$.

If we consider the SDPD as a common point of failure the probability of failure is P_sdpd_tma = $4.8 \times 10^{-7.}$

6.3.7.3 SO3: The occurrence of a detected corruption of CFL due to a corruption of SA (false alarm) for a continuous period of time for one aircraft shall occur with a probability of occurrence less than $1.55x10^{-4}$ per flight hour in en-route and approach environment.

The probability to have two subsequent errors is very low (PSA[equipment] x PSA [equipment] = 4×10^{-10}).

6.3.7.4 SO4: The occurrence of a detected corruption of CFL due to a corruption of SA (false alarm) for a continuous period of time for more than one aircraft shall occur with a probability of occurrence less than $1.55x10^{-4}$ per flight hour in en-route and approach environment.

If we consider the SDPD as a common permanent point of failure the probability of failure is P_sdpd_tma = 4.8×10^{-7}.

6.3.8 Key Conclusions for Selected Altitude

6.3.8.1 A number of key conclusions can be drawn from the PSSA.

1. The use of Selected Altitude in the read-back process for cleared flight level will reduced the probability of occurrence of one of the contributing factors in the causes of a level bust.
2. The Mode S Enhanced Surveillance technology has a very low probability of corrupting the Selected Altitude in such a way that the controller will not detect it. This takes into account the proposal by the JAA for a 'minor' classification for the Selected Altitude parameter within the Mode S transponder.
3. The controller is the most critical element in the system. The analysis indicates the key driver in the result is the (extremely pessimistic) assumption that the controller will fail to detect 1 in 1000 errors on the track label.
4. If an automated tool were used to confirm that Selected Altitude is equal to the cleared flight level and alert the controller if it were not the case (e.g. in form of a 'level bust alerting tool [LBAT]) then the controller error would reduce towards zero and the resulting probability from a system error of an undetected corruption becomes much less (i.e. 6×10^{-13}).
5. Controllers shall continue to monitor the climb/descent to ensure that the cleared level is achieved and not over-shot, as performed in current operations, irrespective of whether the track label indicates a correct value.
6. Controller training shall emphasis that level busts may still occur regardless of whether the voice or automatic readback of cleared flight level is positive.
7. The Mode S Enhanced Surveillance technology has a very low probability of corrupting the Selected Altitude and will therefore not create too much of false alarms which could have resulted in an unacceptable increase of Controller workload.

6.3.9 Recommendation

6.3.9.1 When the OHA was performed (Year 2000), the operational concept for Selected Altitude was not mature. As a consequence a number of 'new' assumptions have been made within the PSSA with respect to the use of Selected Altitude. It is recommended to perform the necessary action to ensure that the OHA and the PSSA are consistent in their assumed use of Selected Altitude.

6.3.9.2 The separation is not assured by the check of the Selected Altitude and could never be achieved by a such method as independent factors can make the CLF not reached and maintained by the aircraft.. The controller shall continue to monitor the climb/descent as today and not take any decision of separation other than today when an expected selected altitude is received. When the received Selected Altitude value is unexpected the controller can re-issue the clearance and check with the pilot the reasons. In this case the undetected corruption of Selected Altitude results in a system working as today.

6.4 Vertical Rate

6.4.1 Assumptions and Method

6.4.1.1 The most strict safety objective for Vertical Rate is S010, which states "The occurrence of undetected corruption of Vertical Rate for a short or continuous period of time for more than one aircraft shall occur with a probability of occurrence less than 1. 55x 10^{-6} per flight hour in an en-route and TMA/approach environment". The ability of the system to meet this objective will be assessed

6.4.1.2 Unlike the safety objective for Selected Altitude, this objective requires a failure condition for two or more aircraft. For this failure mode to occur and safe separation infringed to occur, the following are assumed to be true (although the chances of these being true at the same time are 'low and therefore reduce the probability of occurrence of the failure mode)

- The two aircraft are in the close proximity to each other such that a failure may cause the two aircraft to infringe separation minima (if they were not in close proximity the failure may be equivalent to two single aircraft failures);
- The failure event occurs at the same time (otherwise the two events would be considered a single aircraft failure).

6.4.1.3 When the event occurs, the controller either fails to detect it because of 'human error' or is presented with two values of Vertical Rate which are credible for the two aircraft under their control, whereas all the aircraft are actual doing something different. Examples are:

- the controller expects Vertical Rate to indicate a climbing or descending aircraft, whereas the aircraft is either maintaining level or climbing;
- the Vertical Rate indicates a level flight whereas the aircraft is actually climbing or descending;
- The Vertical Rate indicates the anticipated rate of climb or descent, whereas the aircraft is climbing faster or slower.

6.4.1.4 The possible reasons for an undetected corruption of Vertical Rate of two aircraft in a control sector are:

- Common environmental conditions (sudden change of barometric pressure). Although this is not 'corruption' in the classical sense it may impact on ATC. This is considered a very remote probability and is not analysed in this paper. If however this event did occur, all aircraft are likely to experience the same impact and their relative climb/descend rates remain constant.
- Undetected corruption by the system at the same time for two or more aircraft.

6.4.1.5 The possible contributors to corruption by the system, illustrated in Figure 13, are:

- Either,
  - PVR[both], where two or more aircraft avionics could 'fail' at the same time or;
  - PVR[gnd] where the ground system could corrupt two or more of the Vertical Rate data or ;
  - PVR[both] when one aircraft avionics may corrupt the Vertical Rate and the ground system may corrupt the Vertical Rate from a different aircraft
- AND
  - PVR[controller] when the controller fails to detect the corruption.

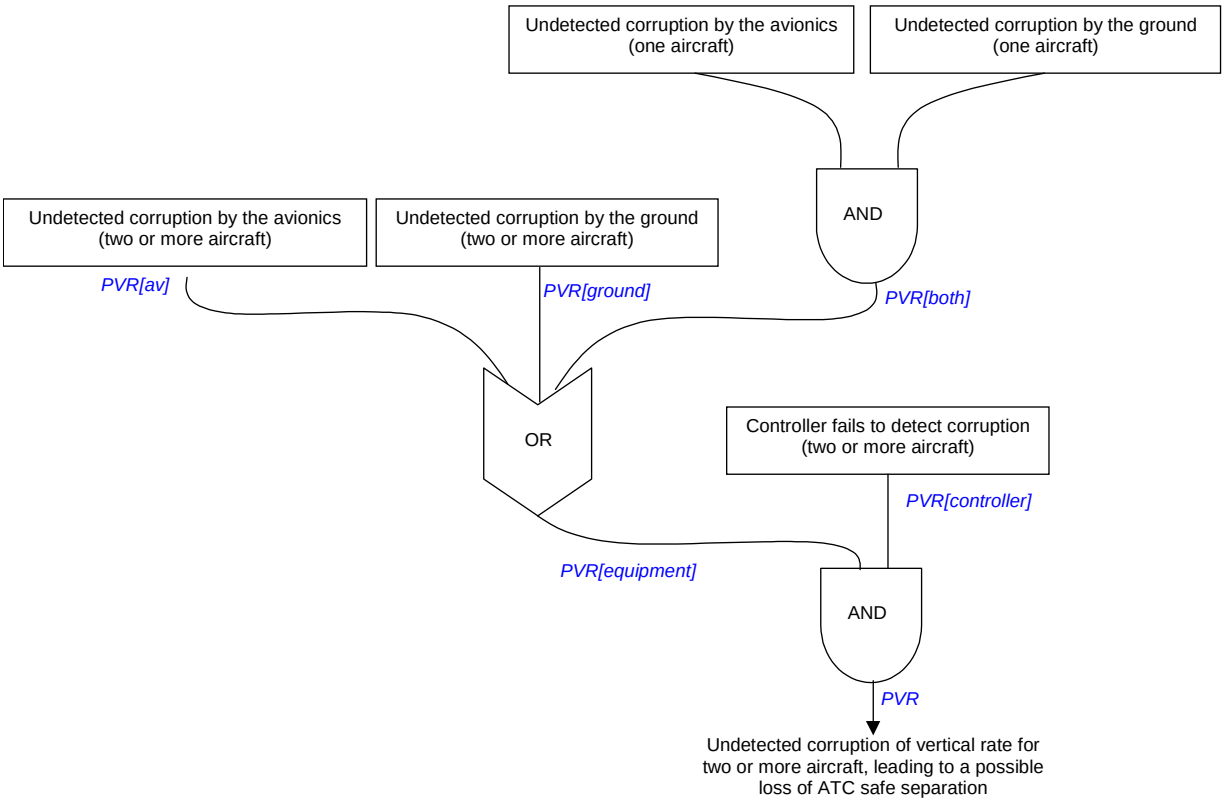


Figure 13 - Contributors to undetected corruption of Vertical Rate

6.4.2 Calculating the Probability of undetected corruption of Vertical Rate

Corruption by the avionics

6.4.2.1 The probability of a simultaneous undetected corruption for two instances, assuming the incidents are unrelated and independent, of Vertical Rate by the avionics for two aircraft is PVR[av]

$$PVR[av] = P\_av\_data\_corruption \times P\_av\_ data\_corruption$$

$$= 9 \times 10^{-6} \times 9 \times 10^{-6}$$

$$= 8 \times 10^{-11} \text{ per flight hour.}$$

Corruption by the ground system

6.4.2.2 [P_gnd] (See 6.2.3.9) states that the undetected corruption of a single CAP by the ground systems is 5.9×10^{-4} hour.

6.4.2.3 The worst case scenario for ground failure is a 'common cause failure' when multiple failures occur due to a single cause (e.g. a timing drift or memory failure). Using this case the probability of simultaneous undetected corruption for two instances of Vertical Rate by the ground system is the same as for a single failure, therefore PVR[gnd]

$$\text{PVR [gnd]} = \text{P\_gnd}$$

$$= 5.9 \times 10^{-4} \text{ per hour.}$$

6.4.2.4 [P_gnd] states that the undetected corruption of a single CAP by the ground systems is 5.9×10^{-4} hour; [P_av_data_corruption] states that the undetected corruption of a single CAP by the avionics is 9×10^{-6} per flight hour. Therefore the probability of a corruption of one Vertical Rate by one avionics and one by the ground systems is PVR [both]

$$\text{PVR [both]} = \text{P\_gnd} \times \text{P\_av\_ data\_corruption}$$

$$= 5.9 \times 10^{-4} \times 9 \times 10^{-6}$$

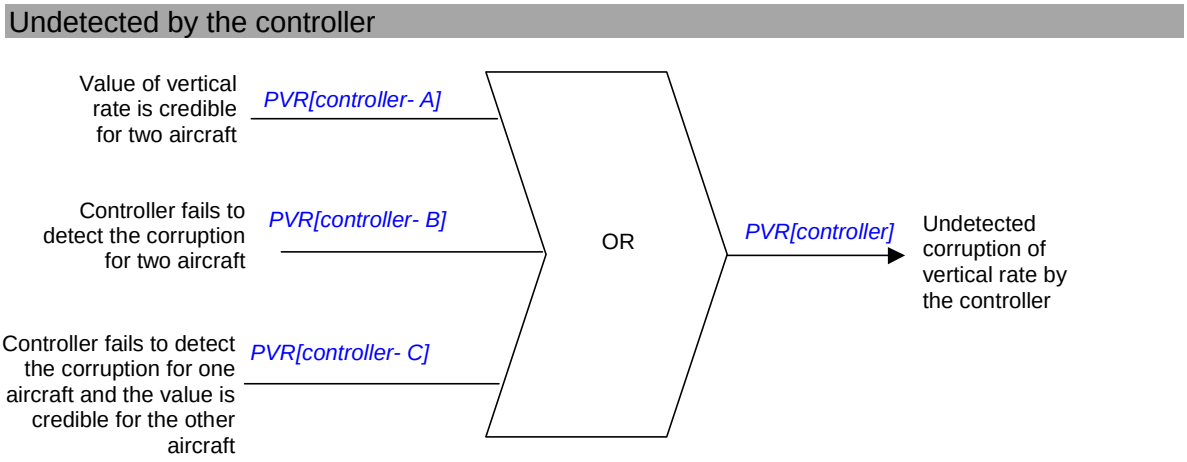
$$= 5.3 \times 10^{-9} \text{ per hour.}$$

6.4.2.5 The probability that the equipment corrupts Vertical Rate for two aircraft and does not detect the corruption is driven by the CCF (Common Cause Failure) in the radar (PVR[gnd], and therefore PVR [equipment]

$$\text{PVR [equipment]} = \text{PVR [gnd]} + \text{PVR [av]} + \text{PVR [both]}$$

$$= 5.9 \times 10^{-4} + 8 \times 10^{-11} + 5.3 \times 10^{-9}$$

$$= 5.9 \times 10^{-4} \text{ per hour}$$



6.4.2.6 Three scenarios exist where the controller could fail to identify a corrupted Vertical Rate for two aircraft. These are either:

- the value presented on the track label for both aircraft is credible, whereas in reality it is a corrupted value
- the controller fails to detect the corruption for both aircraft
- the value presented on the track label for one aircraft is credible and the controller fails to detect the corruption for the other aircraft

6.4.2.7 A credible value for which the controller may not detect a corrupted Vertical Rate, would be approximately **+/- 500 ft per minute**[23], of the expected value (i.e. if the corruption resulted in a value +/- 500 ft per minute of the expected value), as illustrated in Figure 14. Either the corruption of Vertical Rate would result in minor changes in Vertical Rate (e.g. the lower resolution bits) or, if the higher resolution bits changed the controller would be instantly aware of the failure (for example changing from 100ft to 500 feet per minute in a single radar scan for all aircraft).

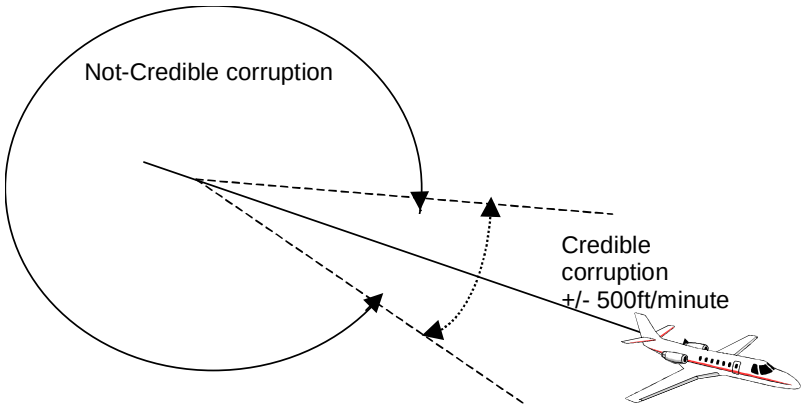
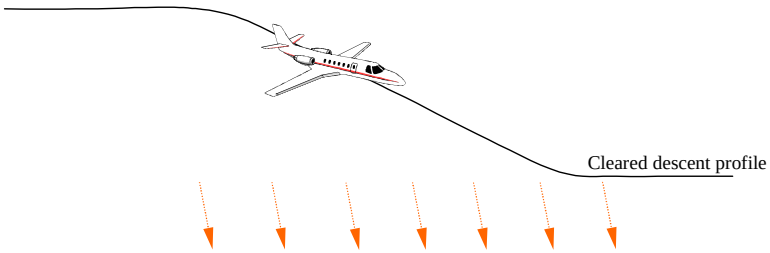


Figure 14 - Credible and non-credible corruption of Vertical Rate.

6.4.2.8 The practical consequence of this assumption is that, for the controller not to detect the corruption, the corruption shall be less than 500 feet per minute over five seconds of the expected value, otherwise the controller would detect and react to it.



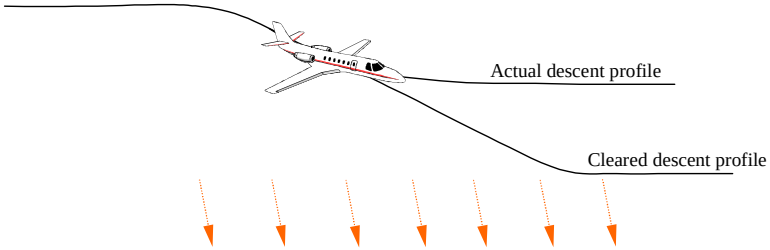
Expected value on track label	0	600	2000	2000	2000	2000	500	0
Credible value on track label	0	800	1900	2300	1700	1700	900	0 (i.e all within +/- 500 ft)
Non- credible value on track label		0	800	1400	2300	1700	900	0 (i.e not within +/- 500 ft)

Figure 15 - Examples of credible and not-credible values for Vertical Rate

6.4.2.9 Illustrated in Figure 15 are credible values for Vertical Rate during a typical descent manoeuvre. A controller will be expecting values of 2000 ft/minute during the manoeuvre and the regular update of the track label will be used to confirm this. The values, which will confirm this, are all considered 'normal' with +/-500 ft/minute of the expected value.

[23] A measurement campaign (ref 5) showed that Vertical Rate tended to deviate +/- 500 ft per minute when an aircraft was flying level. This is indicative of the level of variation in Vertical Rate that would be delivered to the controller on a regular basis and therefore becomes acceptable and 'normal'. Any deviation outside of this value would be a cause for concern for the controller.

When a value outside that range is presented, then the controller will intervene to ascertain the cause of the possible error by the pilot. In the case in Figure 15 the 1400ft/minute value is a case of either failed sensors or detected corruption of Vertical Rate. However, for Figure 16, the error is non-detectable by the controller.



Expected value on track label	0	600	2000	2000	2000	2000	500	0
Accurate value track label	0	800	1900	500	300	0	0	0
Non-detectable failed value	0	800	2000	2000	2000	2000	500	0

Figure 16 - Further examples of credible and not-credible values for Vertical Rate

6.4.2.10 BDS 6,0 encodes Vertical Rate in 10 bits including the sign bit (i.e. the value is encoded in 9 bits). The LSB is 32 ft/minute. 500 ft per minute is therefore contained within the five lower bits. Consequently, the probability of a corruption of the remaining five bits into a credible value is PVR[credible]

$$\text{PVR[credible]}\frac{1}{2^6} = \frac{1}{64} = 0.015$$

6.4.2.11 The probability of this occurrence for two aircraft is PVR[controller -A].

$$\text{PVR[controller-A]} = \text{PVR[credible]} * \text{PVR[credible]}$$

$$= 1.5 \text{ x } 10\text{-}^{2} \text{ x } 1.5 \text{ x } 10^{-2}$$

$$= 2.25 \text{ x } 10^{-4}$$

6.4.2.12 The probability that the controller fails to detect a corruption is much harder to quantify. Using the same assumptions as taken for Selected Altitude (P_controller). It is assumed that the controller fails to detect this at a rate of PVR[controller-Ba].

$$\text{PVR[controller} - \text{Ba]} = \frac{1}{1000} \times \frac{1}{1000} = 1\text{x}10^{-6}$$

6.4.2.13 PVR[controller-Ba] assumes that the failures are independent. This may be the case but in the worst case the failures may be the result of a common component failure and therefore PVR[controller-B] is equal to P_controller, i.e. PVR[controller-B]

$$\text{PVR[controller} - \text{B]} = 1\text{x}10^{-3}$$

6.4.2.14 The probability that the value presented on the track label for one aircraft is credible and the controller fails to detect the corruption for the other aircraft is PVR[controller-C].

$$PVR[controller - C]\frac{1}{1000} \times 0.015 = 1.5x10^{-5}$$

6.4.2.15 Therefore the probability of undetected corruption of Vertical Rate for two aircraft by the controller is PVR[controller]

$$PVR[controller] = PVR[controller\text{-}A] + PVR[controller\text{-}B] + PVR[controller\text{-}C]$$

$$= 2.25 \times 10^{-4} + 1 \times 10^{-3} + 1.5 \times 10^{-5}$$

$$= 1.23 \times 10^{-3}$$

6.4.3 Probability of a undetected corruption of Vertical Rate

6.4.3.1 The probability of undetected corruption of Vertical Rate for two aircraft at the same time is PVR

$$PVR = PVR[equipment] \times PVR[controller]$$

$$= 5.9 \times 10^{-4} \times 1.23 \times 10^{-3}$$

$$= 7.3 \times 10^{-7} \text{ per flight hour.}$$

6.4.3.2 This figure does not include the probability of the aircraft being in the same proximity. If this were included the value would further decrease.

6.4.4 Discussion

6.4.4.1 The most strict safety objective for Vertical Rate is S010, which states “The occurrence of undetected corruption of Vertical Rate for a short or continuous period of time for more than one aircraft shall occur with a probability of occurrence less than 1. 55x 10^{-6} per flight hour in an en-route and TMA/approach environment”. The analysis indicates that, assuming common cause failure, the system meets this objective. If the incident were cause by un-related events then the probability of occurrence is reduced.

6.4.4.2 This event is highly improbable and the safety objective is met, even when including the assumption that the controller ‘misses’ 1 in 1000 errors on the track label. However once again the analysis has illustrated that the probability of technical infrastructure producing an undetectable error is low and the controller is still the critical factor in detecting failures.

6.4.4.3 This analysis does not consider the impact (either positive or negative) with respect to addition controller tools to aid in the detection of corrupted Vertical Rate. For example, within the SDPD simple cross-checking between Mode C/altitude report, when inertial altitude is available, or in more sophisticated SDPD, to provide simple verification using the vertical tracking algorithms.

6.4.4.4 The vertical rate information can come from different sources within the aircraft (barometric/inertial). It is understood that the Barometric altitude rate might be provided with a time lag when compared to the inertial vertical rate (see ref[5]). Additionally the vertical rate measurement is by nature subject to noise and erratic variation (see ref[5]).

The use of such information shall therefore take into account the limitations expressed above.

6.5 Magnetic Heading

6.5.1 Safety Objectives

6.5.1.1 The most strict safety objective for Magnetic Heading is S015, which states "The occurrence of undetected corruption of Magnetic Heading for a short or continuous period of time for more than one aircraft shall occur with a probability of occurrence less than 1.55×10^{-4} per flight hour in an en-route and TMA/approach environment".

6.5.2 Discussion

6.5.2.1 The calculation of P_equipment indicated the probability of system corruption of CAP for one aircraft is 6×10^{-4} per flight hour. This factor, coupled with the probability of a controller failing to detect the corruption (P_controller at 1×10^{-3}) gives an order of magnitude for this failure of 6×10^{-7}. For multiple aircraft, where one can assume the errors are indecent then the probability of simultaneous failure decreases considerably. This alone would indicate that the safety objective can be achieved.

6.5.2.2 It is worth noting that P_equipment does not take into account any mitigation by the system in detecting the corruption of Magnetic Heading. For example, mitigation for such an event could be to utilise the tracker state vector information as a means of detecting large errors in the Magnetic Heading. This would permit, for example, the generation and presentation of a warning to the controller of a possible error in Magnetic Heading.

6.5.2.3 In addition the probability of an occurrence of this event being credible for the controller also reduces the probability of occurrence of this event (in a similar manner to the Vertical Rate analysis because a **+/- 10 degree deviation**[24] from the expected value would be detectable by the controller).

6.5.2.4 It is not possible to assess the impact of Procedures on the occurrence of this event.

6.6 Indicated Airspeed

6.6.1 Safety Objectives

6.6.1.1 The most strict safety objective for Indicated Airspeed is SO18, which state "The occurrence of undetected corruption of Indicated Airspeed for a short or continuous period of time for one or more aircraft shall occur with a probability of occurrence less than 1.55×10^{-4} per flight hour in an en-route and TMA/approach environment".

6.6.2 Discussion

6.6.2.1 The calculation of P_equipment indicated the probability of system corruption of CAP for one aircraft is 6×10^{-4} per flight hour. This factor, coupled with the probability of a controller failing to detect the corruption (P_controller at 1×10^{-3}) gives an order of magnitude for this failure of 6×10^{-7}. For multiple aircraft the probability decreases considerably. This alone would indicate that the safety objective can be achieved.

[24] Expert estimate discussed within the Mode S Task Force

6.6.2.2 In a similar manner to Magnetic Heading, it is worthy of note that P_equipment does not take into account any mitigation by the system in detecting the corruption of Indicated Airspeed. For example, mitigation for such an event would be to utilise the tracker state vector information as a means of detecting large blunders in the Indicated Airspeed. This would permit, for example, the generation and presentation of a warning to the controller of a possible error in Indicated Airspeed. Additionally, as for other CAPs, a credible value must be presented to the controller in order for the undetected event to occur. This therefore reduces the probability of occurrence.

6.6.2.3 It is not possible to assess the impact of Procedures on the occurrence of this event.

6.7 Summary

6.7.1.1 Detailed analysis of the contributing events leading to undetected corruption of CAP Selected Altitude and Vertical Rate have been presented in this document. It illustrates that, based on the assumptions made in the analysis, the safety objective for those parameters can be achieved.

6.7.1.2 A discussion concerning the CAP Magnetic Heading and Indicated Airspeed illustrates that the equipment contribution to the occurrence of the event and the credibility of such a failure suggests that the safety objectives for these two CAP items can also be achieved.

7 SUMMARY AND CONCLUSIONS

7.1 General

7.1.1.1 This document has developed a preliminary safety analysis of four controller access parameters (CAP) which are delivered by Mode S Enhanced Surveillance.

7.1.1.2 The document has been produced by the Eurocontrol Mode S Programme as a support to the implementation of Mode S Enhanced Surveillance.

7.1.1.3 The CAP considered in the safety analysis are (with the equivalent ARINC 429 references included within brackets):

- Magnetic Heading (equivalent to ARINC429 label 320)
- Indicated Airspeed (equivalent to ARINC429 label 205 for Mach number or 206 for Indicated Airspeed)
- Vertical Rate (equivalent to ARINC429 label 365 for inertial velocity rate or 212 for barometric altitude rate))
- Selected Altitude (equivalent to ARINC429 label 102)

7.1.1.4 CAP may be delivered by a number of communications systems. This analysis considered the use of Mode S Enhanced Surveillance as a means of delivering CAP to the controller.

7.2 Conclusions

7.2.1.1 Detailed analysis of the contributing events leading to undetected corruption of CAP has been presented in this document.

7.2.1.2 Selected Altitude:

The corruption of the Selected Altitude resulting in a false alarm detected by the controller will remain very low and acceptable when compared to the corresponding Safety Objectives (SO2, SO3, SO4). Display of the Selected Altitude will not generate unacceptable additional workload (new check using the RT) due to its corruption.

The safety objective for an undetected corruption of CFL is 1.55×10^{-8} per flight hour. Current operations are currently achieving 6×10^{-5} per flight hour. The introduction of an additional readback through the use of Selected Altitude, reduces the probability of undetected corruption to 6×10^{-8} per flight hour, thereby improving safety within a factor of three.
This is clearly an improvement over the performance of the system today. Nevertheless necessary action shall be taken in order to ensure that controllers do not use this information to confirm that the aircraft has reached the Cleared Flight Level. The monitoring of climb/descent shall continue as in the today system.
This monitoring is mandatory, as there are other independent sources of Level Bust which will make the aircraft not maintaining the CFL even if it is well delivered and display on the Controller display.
Making the assumption that such procedure is kept the worst consequence of the non-detection of a corrupted CFL is the non-early detection of a possible Level Bust going back to the level of Safety provided by the current systems. The system itself will not

generate too much undetectable bad CFL. The non-detection of the bad CFL is mainly due to the limit of a human check.

7.2.1.3 Based on the assumptions made in the analysis the safety objective for Vertical Rate can be achieved.

7.2.1.4 A discussion concerning the CAP Magnetic Heading and Indicated Airspeed illustrated that the equipment contribution to the occurrence of the event and the credibility of such a failure suggests that the safety objectives for these two CAP items can also be achieved.

7.2.1.5 In conclusion based on the assumptions described in this document including the “minor” classification of airborne system the analysis shows that CAPs delivered through Mode S Enhanced Surveillance can be used once Controllers are trained to their acceptable use.

7.3 A word of caution

7.3.1.1 The analysis presented in the document relies on all the assumptions being true and valid. ANSPs and other readers should ensure that the assumptions made in this document are applicable to their airspace, using this document as a contribution to their local safety case.

APPENDIX A: ABBREVIATIONS

ACAS	Airborne Collision Avoidance System
ACP	Aircraft Control Panel
ANS	Air Navigation Service
Approach Control	Unit charged with control of traffic around one or more airports and responsible for the spacing of traffic on final approach. It is concerned with departing and arriving aircraft. Arriving aircraft are transferred from area control via approach to tower control, departing aircraft are transferred from tower control via approach to area control.
Approach Control Unit	The ATC unit providing ATC service to arriving, departing and over-flying flights within the airspace in the vicinity of an aerodrome.
Area	An en-route airspace volume corresponding to an Area Control Centre.
Area Control Centre	That part of ATC that is concerned with en-route traffic coming from or going to adjacent centres or APP. It is a unit established to provide air traffic control service to controlled flights in control areas under its jurisdiction.
Area Control Service	A unit established to provide air traffic control service to controlled flights in control areas under its jurisdiction. (Ref. ICAO Doc 9569 Definitions).
ARINC	Aeronautical Radio Incorporated (USA)
ARTAS	ATM suRveillance Tracker and Server
ATC	Air Traffic Control
ATCO	Air Traffic Controller Officer
ATM	Air Traffic Management
ATS	Air Traffic Service
ATSU	Air Traffic Service Unit
BAR	Barometric Altitude Rate
BDS	Comm-B Data Selector (or sometimes with reference to the same item, Binary Data Store)
CAP	Controller Access Parameter
CFL	Cleared Flight Level
CWP	Controller Working Position
ECAC	European Civil Aviation Conference
En-Route	The airspace under the control of the Area Control Centre
FIR	Flight Information Region
FL	Flight Level
FMS	Flight Management System
GICB	Ground Initiated Comm B
HMI	Human Machine Interface
IAS	Indicated Air Speed
ICAO	International Civil Aviation Organisation
LSB	Least Significant Bit
MODE-S	Mode Select
MTCD	Medium Term Conflict Detection
OHA	Operational Hazard Assessment
PSR	Primary Surveillance Radar
R/T	Radio Transmission
RNP	Required Navigation Performance
SA	Selected Altitude
SAP	System Access Parameter
SDPD	Surveillance Data Processing and Distribution
SDPS	Surveillance Data Processing System
Sector	1- A part of airspace controlled by a team of controllers, defined, notably, by its geographical co-ordinates and its assigned radio frequency. 2- An area in which aircraft are under control of a single executive controller (ATCO). Several sectors make up the entire FIR.

SSR	Secondary Surveillance Radar
TCAS	Traffic Collision Avoidance System
Terminal Area	A general term used to describe airspace in which approach control service or airport traffic control service is provided.
Terminal Control Area	A control area normally established at the confluence of ATS routes in the vicinity of one or more major aerodromes.
TMA	Terminal Manoeuvring Area
VHF	Very High Frequency (radio waves)

APPENDIX B: REFERENCES

1 Eurocontrol Standard Document for Radar Surveillance in En-Route Airspace And Major Terminal Areas SUR.ET1.ST01.1000-STD-01-01, Edition 1.0, March 1997

2 Eurocontrol Standard Document for Area Navigation Equipment Operational requirements and Functional Requirements 003-93, Edition 2.2. December 1998

3 Risk Assessment and Mitigation in ATM ESARR 4, Edition 1.0 05/04/2001

4 The airborne impact of Mode S Enhanced Surveillance and Down-linked Aircraft Parameters. Eurocontrol reference SUR3.82.ST03.2150. 24th November 1999

5 An assessment of Downlink Airborne Parameters for Enhanced Surveillance. DERA/ATCSG/EDAP/01, issue 1, 24th September 1998

6 Operational Hazard Assessment Hazard of Elementary and Enhanced Surveillance ModeS/OHA/001 Edition 1.0 October 2001

7 ICAO Annex 10 Volume III Amendment 77 28/11/02

8 JAA CNS/ATM Steering Group on ENHANCED SURVEILLANCE WITH SSR MODE S No. and Revision pp025_76 17th April 2003

9 FAA/JAA AC/AMJ No: 25.1309 dated Date: 6/10/2002

APPENDIX C: LIST OF THE MAIN QUANTITATIVE ASSUMPTIONS USED

Nb		Name + value	Short description	Reference
	28	**P_1Radar_uc_data = 5.6 x 10-7 per message**	Probability that 1 radar will corrupt a data coming from airborne and will not detect it.	POEMS FTA 6108900/000 Issue 1.0 June 2002 section 7.1 altitude and identity corruption + detailed fault tree indicating the Site undetected corrupted height data at scan 1
		Nb_altitude_changes_per_flight = 13	Number of altitude changes per flight in ECAC area	Estimate based on ECAC statistics
		P_av = 10-4 per flight hour	Probability of failure for avionics	Expert estimate based on a minor classification of corresponding avionics. Probability confirmed by an Airframe manufacturer who uses a probability of 5 x 10-5
		9%	Avionics failure resulting in corruption of data	Mode S Safety Task Force Expert estimate based on experience with SSR Mode A/C transponders (majority of problems results in loss of detection)
		1%	Avionics failure resulting in corruption of position	Mode S Safety Task Force Expert estimate based on experience with SSR Mode A/C transponders (majority of problems results in loss of detection)
		90%	Avionics failure resulting in loss of data	Mode S Safety Task Force Expert estimate based on experience with SSR Mode A/C transponders (majority of problems results in loss of detection)
		2 minutes	Duration for which a controller will monitor the Selected Altitude after a clearance	Mode S Safety Task Force Expert estimate
		P_controller = 1 x 10-3	Controller Human Error Probability	Mode S Safety Task Force Expert estimate
		Average_duration_of_1_flight = 1.38 hour	Average duration of flight in ECAC area	Estimate based on ECAC statistics
		P_ground_net = 10-9 per message	Probability of undetected error of ground communication	
		1%	Contribution of 1 Mode S hazard to the ATM srverity class	Mode S safety task Force Expert estimate based on 10 sub-functions and 10 hazards of the same severity per sub-function resulting in approximately 100 hazards of a given severity in an ATM system..
		+/- 10 degree deviation	Magnetic Heading variation around which the value will remain credible for the controller	Expert estimate discussed within the Mode S Task Force
		1000 flights per hour of	Number of flights seen by one	

		operation	radar for 1 hour of operation	
		P_rf = 10-7per message	Probability of undetected corruption of an RF Mode S message	ICAO Manual of the Secondary Surveillance radar (SSR) systems (DOC 9684) First Edition 1997. Appendix 1 Paragraph 1.3.
		P_sdpd_hr = 1.2 x 10-4 /h	Probability that the SDPD corrupt track data over 1 hour of operation	ARTAS dependability study - Final Report December 1998 CENA/NT97613/SDF version 1.1 section 4 page 130 FE1.2 “undetected partial loss of track information”
		102	Factor between severity classes	Expert estimate based on approach currently used for airborne equipment
		15mn	Average duration of 1 flight in a TMA radar coverage	
		+/- 500 ft per minute	Difference beyond which the controller will question the Vertical Rate value	A measurement campaign (ref 5) showed that Vertical Rate tended to deviate +/- 500 ft per minute when an aircraft was flying level. This is indicative of the level of variation in Vertical Rate that would be delivered to the controller on a regular basis and therefore becomes acceptable and ‘normal’. Any deviation outside of this value would be a cause for concern for the controller.

APPENDIX D: CAP OPERATIONAL HAZARD ASSESSMENT

OHA CAP extract

CAP	Failure Mode	Qualifier	Effect on ATC	Mitigation	Severity Class En-Route	Severity Class TMA/ Approach
Magnetic Heading	All sudden, short duration failure modes	All qualifiers	No effect on ATC operations.	N/A	5	5
Magnetic Heading	Sudden, continuous, detectable loss or corruption	One aircraft	The verbal verification of the Magnetic Heading will result in increased controller workload due to the need for increased VHF voice activity.	Experience and ability of controllers, which enables them to identify that the failure, has occurred. Availability of Procedures which determine the course of action to be taken by Controllers in the event of failure.	5	4
Magnetic Heading	Sudden, continuous, detectable loss or corruption	All Mode S aircraft	The verbal verification of the Magnetic Heading will result in increased controller workload due to the need for increased VHF voice activity. Heading is used more frequently within the TMA environment. The effect on TMA operations is therefore more severe. The severity classification for TMA effects is therefore at the top of the definition of Class 4. The associated classification for En-Route is towards the lower boundary of the Class definition.	Experience and ability of controllers, which enables them to identify that the failure, has occurred. Availability of Procedures which determine the course of action to be taken by Controllers in the event of failure (Procedures as without Mode S derived surveillance parameter).	4+	4-
Magnetic Heading	Undetectable loss or corruption[25]	One aircraft	The Magnetic Heading is used assist in maintaining separation between aircraft and may contribute to medium term planning.	As result of the experience of the controllers, this failure will be detected within a short period of time and may result in a slight increase in controller workload, but will have no effect on ATC	5	5

[25] MSSTF6 determined that it was not possible for there to be undetectable loss of this function/ parameter. It was also determined that corruption would only remain undetectable if it remained with ±10°.

OHA CAP extract

CAP	Failure Mode	Qualifier	Effect on ATC	Mitigation	Severity Class En-Route	Severity Class TMA/ Approach
Magnetic Heading	Undetectable loss or corruption [26]	All Mode S aircraft	The Magnetic Heading is used to assist in maintaining separation between aircraft and may contribute to medium term planning.	As result of the experience of the controllers, this failure will be detected within a short period of time and may result in a slight increase in controller workload, but will have no effect on ATC.	4+	4-
Indicated Air Speed	All sudden, short duration failure modes	All qualifiers	No effect on ATC operations.	N/A	5	5
Indicated Air Speed	Sudden, continuous, detectable loss or corruption	One aircraft	The verbal verification of the IAS will result in increased controller workload due to the need for increased VHF voice activity.	Experience and ability of controllers, which enables them to identify that the failure, has occurred. Availability of Procedures which determine the course of action to be taken by Controllers in the event of failure.	5-	5+
Indicated Air Speed	Sudden, continuous, detectable loss or corruption	All Mode S aircraft	The verbal verification of the IAS will result in increased controller workload due to the need for increased VHF voice activity.	Experience and ability of controllers, which enables them to identify that the failure, has occurred. Availability of Procedures which determine the course of action to be taken by Controllers in the event of failure (Procedures as without Mode S derived surveillance parameter).	4	4

[26] MSSTF6 determined that it was not possible for there to be undetectable loss of this function/ parameter. It was also determined that corruption would only remain undetectable if it remained with ±10°.

OHA CAP extract

CAP	Failure Mode	Qualifier	Effect on ATC	Mitigation	Severity Class En-Route	Severity Class TMA/ Approach
Indicated Air Speed	Undetectable loss or corruption[27]	One aircraft	Possible loss of separation	As result of the experience of the controllers, this failure will be detected within a short period of time and may result in a slight increase in controller workload, but will have no effect on ATC. When detection occurs, then the verbal verification of the IAS will result in increased controller workload due to the need for increased VHF voice activity. Availability of Procedures which determine the course of action to be taken by Controllers in the event of failure (Procedures without Mode S derived surveillance parameter).	4	4
Indicated Air Speed	Undetectable loss or corruption[28]	All Mode S aircraft	Possible loss of separation	As result of the experience of the controllers, this failure will be detected within a short period of time and may result in a slight increase in controller workload, but will have no effect on ATC. When detection occurs, then the verbal verification of the IAS will result in increased controller workload due to the need for increased VHF voice activity. Availability of Procedures which determine the course of action to be taken by Controllers in the event of failure (Procedures without Mode S derived surveillance parameter).	4	4
Vertical Rate	All sudden, short duration failure modes	All qualifiers	No effect on ATC operations.	N/A	5	5

[27] Loss could not remain undetected if the parameter was in use. Therefore corruption only was considered.
[28] Loss could not remain undetected if the parameter was in use. Therefore corruption only was considered.

OHA CAP extract

CAP	Failure Mode	Qualifier	Effect on ATC	Mitigation	Severity Class En-Route	Severity Class TMA/ Approach
Vertical Rate	Sudden, continuous, detectable loss or corruption	One aircraft	No effect on ATC	Experience and ability of controllers, which enables them to identify that the failure, has occurred. The verbal verification of the Vertical Rate will result in a slight increase in controller workload due to the need for increased VHF voice activity Availability of Procedures which determine the course of action to be taken by Controllers in the event of failure.	5	5

OHA CAP extract

CAP	Failure Mode	Qualifier	Effect on ATC	Mitigation	Severity Class En-Route	Severity Class TMA/ Approach
Vertical Rate	Sudden, continuous, detectable loss or corruption	All Mode S aircraft	The verbal verification of the Vertical Rate will result in increased controller workload due to the need for increased VHF voice activity.	Experience and ability of controllers, which enables them to identify that the failure, has occurred. The verbal verification of the Vertical Rate will result in a slight increase in controller workload due to the need for increased VHF voice activity Availability of Procedures which determine the course of action to be taken by Controllers in the event of failure (Procedures as without Mode S derived surveillance parameter).	4	4
Vertical Rate	Undetectable loss or corruption[29]	One aircraft	The corruption of Vertical Rate data may lead to a wrong assumption by the controller regarding the vertical behaviour of an Aircraft. If this remains undetected a dangerous situation could arise. This represents a potential reduction in the safe operation of the system over the existing situation unless the content of the adjacent note is implemented.	Experience and ability of controllers, which enables them to identify that the failure, has occurred. It was assumed that a STCA alert would occur. Availability of Procedures which determine the course of action to be taken by Controllers in the event of failure (Procedures without Mode S derived surveillance parameter). Note: it was anticipated that a controller could be required, by procedure to compare the Vertical Rate parameter with the rate of change of the Mode C/altitude, however it was felt that it was more realistic for the Equipment to make the comparison.	4+	4-

[29] MSSTF6 determined that it was not possible for there to be undetectable corruption of this function/ parameter. It was also determined that corruption would only remain undetectable if it remained within a small deviation.

OHA CAP extract

CAP	Failure Mode	Qualifier	Effect on ATC	Mitigation	Severity Class En-Route	Severity Class TMA/ Approach
Vertical Rate	Undetectable loss or corruption	All Mode S aircraft	The corruption of Vertical Rate data may lead to a wrong assumption by the controller regarding the vertical behaviour of an Aircraft. If this remains undetected a dangerous situation could arise. This represents a potential reduction in the safe operation of the system, potential resulting in loss of separation between multiple aircraft	Experience and ability of controllers, which enables them to identify that the failure, has occurred. Availability of Procedures which determine the course of action to be taken by Controllers in the event of failure (Procedures without Mode S derived surveillance parameter). Note: it was anticipated that a controller could be required, by procedure to compare the Vertical Rate parameter with the rate of change of the Mode C, however it was felt that it was more realistic for the Equipment to make the comparison.	3+	3-
Selected Altitude	Sudden, short duration, detectable loss or corruption	One aircraft	No effect on ATC operations.	N/A	5	5
Selected Altitude	Sudden, short duration, detectable loss or corruption	All Mode S aircraft	With all aircraft involved it is more likely than single aircraft that Controller may seek information via VHF voice resulting in an increase in the workload.	Experience and ability of controllers, which enables them to identify that the failure, has occurred. The verbal verification of the selected will result in a increased in controller workload due to the need for increased VHF voice activity Availability of Procedures which determine the course of action to be taken by Controllers in the event of failure (Procedures without Mode S derived surveillance parameter).	4	4
Selected Altitude	Sudden, continuous, detectable loss or corruption	One aircraft	There will be increased controller workload due to the need for increased VHF voice activity. Due to the increased aircraft movements and reduced time available within the TMA environment, the effect on TMA operations is more severe than En-Route.	Experience and ability of controllers, which enables them to identify that the failure, has occurred. Availability of Procedures which determine the course of action to be taken by Controllers in the event of failure.	4+	4-

OHA CAP extract

CAP	Failure Mode	Qualifier	Effect on ATC	Mitigation	Severity Class En-Route	Severity Class TMA/ Approach
Selected Altitude	Sudden, continuous, detectable loss or corruption	All Mode S aircraft	There will be increased controller workload due to the need for increased VHF voice activity.	Experience and ability of controllers, which enables them to identify that the failure, has occurred. Availability of Procedures which determine the course of action to be taken by Controllers in the event of failure (Procedures as without Mode S derived surveillance parameter).	4	4
Selected Altitude	Undetectable loss or corruption[30]	One aircraft	The controller may make decisions with respect to separation of aircraft based on incorrect assumptions. The result may be an aircraft not flying to its cleared flight level, or flying to the cleared flight level occupied by another aircraft.	Potential STCA alert.	2	2
Selected Altitude	Undetectable loss or corruption[31]	All Mode S aircraft	The controller may make decisions with respect to separation of aircraft based on incorrect assumptions. A number of aircraft may not fly to its cleared flight level, or flying to the cleared flight level occupied by other aircraft.	Potential STCA alert.	2	2

[30] MSSTF6 determined that it was not possible for there to be undetectable loss of this function/ parameter.
[31] MSSTF6 determined that it was not possible for there to be undetectable loss of this function/ parameter.