Bernd Tiemeyer

PERFORMANCE EVALUATION OF SATELLITE NAVIGATION AND SAFETY CASE DEVELOPMENT

PERFORMANCE EVALUATION OF
SATELLITE NAVIGATION AND
SAFETY CASE DEVELOPMENT

eingereicht von

Dipl.-Ing. Bernd Tiemeyer

Vollständiger Abdruck der an der Fakultät für Bauingenieur- und Vermessungswesen der Universität der Bundeswehr München zur Erlangung des akademischen Grades eines Doktors der Ingenieurwissenschaften (Dr.-Ing.) eingereichten Dissertation.

Vorsitzender: Univ.-Prof. Dr.-Ing. B. Eissfeller
1. Berichterstatter: Univ.-Prof. Dr.-Ing. G. W. Hein
2. Berichterstatter: Univ.-Prof. Dr.-Ing. R. Onken

Die Dissertation wurde am 17. Mai 2001 bei der Universität der Bundeswehr München, Werner-Heisenberg-Weg 39, D-85577 Neubiberg, eingereicht.

Tag der mündlichen Prüfung: 17. Januar 2002

To Katrin, Andrew and my Parents

Who will never realise
how much they contributed
to this work.

" Together with people outside the field of aviation,
we find ourselves moving in a vicious cycle,
where the machine, which depend on modern man
for its invention, has made modern man dependent
on its constant improvement for his security
- even for his live. "

Charles A. Lindbergh
in "The Spirit of St. Louis", 1953

PREFACE

The present thesis was developed during my activities as Project Manager in the area of Satellite Navigation and Safety at the EUROCONTROL Experimental Centre, Brétigny-sur-Orge, France.

EXECUTIVE SUMMARY

Operational approval of satellite navigation applications for civil aviation exists for supplemental use in continental airspace and for primary use during oceanic en-route phases of flight for a small number of operators and in exceptional cases for Non-Precision Approach. This situation, that the operational approval does not keep pace with the technical capabilities of satellite navigation, is mainly the result of insufficient knowledge about the system's integrity and institutional limitations including concern over single-State control, lack of 'traceability' and a complete absence of binding performance guarantees.

In order to achieve progress towards extending the operational approval for satellite navigation applications, for the first time an attempt is made to combine parameters describing the Required Navigation Performance and those describing the performance of satellite navigation. The established set of parameters forms the basis for an exhaustive system evaluation comprising a unique flight trial programme which involves a wide-body commercial airliner. The overall aim is to build-up confidence in the satellite navigation system's performance, in particular, concerning integrity and continuity of service by developing a total system concept.

A world-wide unique database system has been developed – following rigorous software engineering and quality assurance procedures – to contain the data recorded onboard the airliner. The subsequent data evaluation process demonstrates to what extend GPS RAIM satisfies the Required Navigation Performance for civil aviation during different phases of flight. It is demonstrated how an augmentation such as barometric-aiding can improve the system performance and can allow a wider range of operational applications. These results are the major input, via a hazard identification tree, into the GNSS Safety Case, the concept of which is developed herein. The Safety Case, incorporating a Risk Model at its core, is proposed for the first time as a methodology for an Traffic Service Provider to demonstrate that the operational use of satellite navigation can achieve its Target Level of Safety and that it can therefore be approved for operational use by Safety Regulatory Authorities.

This work is the unique attempt to use a scientific-technical approach to develop a total system concept which can contribute to progressing the operational approval of satellite navigation applications in civil aviation. Although the investigations are based on applications for civil aviation, research was conducted into the requirements of maritime and terrestrial user communities and how the Safety Case concept developed in this document could be applied in the context of multi-modal transport.

<u>ÜBERSICHT</u>

Anwendungen der Satellitennavigation für die Zivilluftfahrt wurden bisher als ergänzendes Navigationsmittel im kontinentalen Luftraum und als primäres für eine geringe Anzahl von Flugzeugbetreibern im ozeanischen Luftraum operationell zugelassen, in besonderen Fällen erfolgten Genehmigungen des Einsatzes als primäres Navigationssystem für Nicht-Präzisionsanflüge. Diese Situation, in der die operationelle Zulassung mit den technischen Entwicklungen nicht Schritt halten kann, ist vornehmlich die Folge des nicht ausreichenden Kenntnisstandes bezüglich der System-integrität und der institutionellen Einschränkungen. Im einzelnen beziehen diese sich auf die System-kontrolle, die von einem einzelnen Staat durchgeführt wird, auf die Nichtverfügbarkeit wichtiger Systeminformationen und das Fehlen verbindlicher Garantien für die Leistungsfähigkeit des Systems.

Um Fortschritt in der operationellen Zulassung von Satellitennavigationsanwendungen zu erzielen, werden in dieser Arbeit erstmalig Parameter, die die allgemeinen Anforderungen an Navigationssysteme darstellen mit denen verknüpft, die die Leistungsfähigkeit der Satellitennavigation beschreiben. Der entwickelte Parametersatz stellt die Grundlage für eine umfangreiche Systembewertung dar, welche ein einmaliges Flugversuchsprogramm mit einem Großraumflugzeug umfasst. Erklärtes Ziel ist es, zuverlässige Aussagen über die Leistungsfähigkeit, insbesondere die Integrität und die Kontinuität der Satellitennavigation, machen zu können, indem ein gesamtheilicher Systemansatz entwickelt wird.

Dazu ist ein weltweit einzigartiges Datanbanksystem, das strengen Anforderungen von ‹‹Software Engineering›› und Qualitätssicherung gerecht werdend, entwickelt worden, welches die Daten enthält, die an Bord des Verkehrsflugzeuges aufgezeichnet worden sind. Der sich anschließende Daten-auswertungsprozess zeigt, in wieweit GPS RAIM den Anforderungen der Zivilluftfahrt an ein Navigationssystem gerecht werden kann, das für die unterschiedlichen Phasen eines Fluges eingesetzt werden soll. Es wird aufgezeigt, wie die Leistungsfähigkeit des Navigationssystems durch eine Augmentierung, z.B. mit Hilfe der Information eines barometrischen Höhenmessers, gesteigert wird, und damit das operationelle Einsatzspektrum erweitert werden kann. Die erzielten Ergebnisse fließen über einen Fehleridentifikationsbaum in das in dieser Arbeit entwickelte Konzept des GNSS ‹‹Safety Case›› ein. Der ‹‹Safety Case››, der in seinem Kern auf einem Risikomodell basiert, wird erstmalig den Flugsicherungsorganisationen als eine Methode vorgeschlagen, die diese einsetzen können um nachzuweisen, dass der operationelle Einsatz der Satellitennavigation die gestellten Sicherheitsanforderungen erfüllt und damit von Zulassungsbehörden genehmigt werden kann.

Diese Arbeit stellt den erstmaligen Versuch dar, mit Hilfe eines technisch-wissenschaftlichen Ansatzes ein gesamtheitliches Systemkonzept zu entwickeln, das einen Beitrag zum Fortschritt in der operationellen Zulassung von Satellitennavigationsanwendungen liefern kann. Die Untersuchungen basieren auf Anwendungen für die Zivilluftfahrt. Es werden jedoch auch Nachforschungen angestellt welches die Anforderungen von maritimen und terrestrischen Nutzern sind und wie das in dieser Arbeit entwickelte Konzept des ‹‹Safety Case›› in den Kontext des multi-modalen Transports übertragen werden kann.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

NOTATION

ACC_{hor}	estimated horizontal position error
c	speed of light
D	Decision Variable
d_{ion}	ionospheric error
d_{trop}	tropospheric error
δt	satellite clock error
δT	receiver clock error
$\delta HDOP_i$	Increase in HDOP when excluding satellite 'i'
$\delta HDOP_{i\,max}$	Increase in HDOP after exclusion of 'worst-case' satellite 'i'
$\underline{\varepsilon}$	n x 1 vector of Gaussian-distributed measurement errors
$\underline{\varepsilon}_k$	n x 1 vector of bias due to failure
ε_n	measurement noise
FR_U	Undetected Failure Rate (Integrity Risk)
$\underline{H}$	n x 4 measurement matrix (direction cosine matrix)
HAL	Horizontal Alarm Limit
$HDOP$	Horizontal Dilution of Precision
$HDOP_i$	HDOP calculated after exclusion of satellite 'i'
I_n	n x n unity matrix
λ	Non-Centrality Parameter
$MTBF$	Mean Time Between Failure
N_{SV}	Total number of satellites in the constellation
n	Number of Satellites
P	Probability Function
P_{FA}	Probability of False Alarm
P_{MD}	Probability of Missed Detection
Q	Complementary Probability Function / n x n orthogonal matrix
$r = n-4$	Degrees of Freedom
ρ	geometrical range
σ	Standard Deviation
T	Threshold
$VDOP$	Vertical Dilution of Precision
$\underline{v}$	n x 1 vector of measurement noise
$\underline{x}$	n x 1 innovation vector
$\hat{\underline{x}}$	least squares estimates of innovation vector

ξ	scalar containing the normally-distributed, zero-mean measurement noise
z	measured pseudo-range
$\underline{z}$	n x 1 vector of linearised measurements compensated by *a priori* information
$\bar{\underline{z}}$	vector of measurement residuals

1. **INTRODUCTION**

1.1 **OBJECTIVE**

With the advent of the United States' Global Positioning System (GPS) the civil aviation community has been anxious to ensure that satellite navigation be certificated for a wide range of applications as quickly as possible.

Today, the latest generation of commercial airliners has GPS receivers already included in standard avionics fits based on approvals which airframe manufacturers, together with avionics suppliers, obtain from safety regulation authorities [TSO-C129A, 1996], [JAA/TGL-3, 1997]. However, these approvals only cover airworthiness and technical certification. Subsequently, they have to be complemented by operational approvals, which allow the aircraft operators to use the equipment during the intended operations.

Currently, operational approval exists for supplemental use of satellite navigation in continental airspace and for primary use during oceanic en-route phases of flight for a small number of operators and in exceptional cases for Non-Precision Approach. This situation, that the operational approval does not keep pace with the technical capabilities of satellite navigation, is mainly the result of technical and institutional limitations including concern over single-State control, lack of 'traceability' and a complete absence of binding performance guarantees.

The lack of system visibility and transparency puts any safety regulator in a difficult situation to grant an approval for use of GPS during critical phases of flight such as Non-Precision Approach (NPA) and Precision Approach (PA). Safety regulation authorities need to be in the position to judge which level of operational use of satellite navigation can be permitted. Therefore, the most demanding question to be answered is:

Can Satellite Navigation meet the Required Navigation Performance parameters of Accuracy, Integrity, Availability and Continuity of Service for it to be approved and certificated as safe for operational use in civil aviation?

But, this question directly leads onto another:

What is the Required Navigation Performance expressed in terms of Accuracy, Integrity, Availability and Continuity of Service?

A number of documents [RTCA/DO-208, 1991], [RTCA/DO-217, 1993], [RTCA/DO-229, 1996] and [GNSSP, 1997/1999] provide requirements for satellite navigation performance during different phases of flight, but no validated set of RNP parameters exists today which in its entirety is acceptable to safety regulation authorities. Therefore:

Today's Required Navigation Performance has to be analysed and
a consistent set of parameters has to be proposed and validated.

The capabilities of satellite navigation have been demonstrated during numerous simulations and limited flight tests against various sets of RNP parameters. But, based on experience and best practices during the certification of Instrument Landing Systems (ILS), it is vital to obtain a comprehensive and statistically representative database of measurements recorded onboard aircraft in revenue service to complement any theoretical results.

Such a database would provide the means for statistical analysis of real data, because:

A comprehensive description of the satellite navigation system capabilities in
the operational environment of commercial aircraft needs to be established
to provide conclusive evidence of its performance.

Different approaches, in particular for monitoring of the system's integrity, have to be investigated to verify whether they meet the respective requirements. Augmentations may be considered when satellite navigation performance achieved from basic constellations on their own falls short of achieving the Required Navigation Performance.

Consequently, it shall be possible to verify a set of RNP parameters and to provide conclusive evidence of satellite navigation system performance. This evidence can then form the basis for the development of a Safety Case as input to a comprehensive approval of satellite navigation as safe for operational use in civil aviation.

If such a Safety Case can be successfully established to meet the most stringent requirements of civil aviation, it is expected that the other modes of transport - maritime and land – can directly benefit from these developments.

1.2   BACKGROUND

Today, a variety of systems are installed onboard of commercial airliners for navigation during the different phases of a flight. Inertial Navigation Systems (INS) are used for oceanic and remote continental en-route operations. Ground-based radionavigation aids such as NDB/ADF, VOR and DME support continental en-route down to Non-Precision Approach operations. For Precision Approaches airport operators provide localiser and glideslope transmitters for instrument landing capabilities to three different categories of operational minima (CAT I-III).

This multi-system environment is one reason for the limitation of the capabilities of Air Traffic Flow Management (ATFM), because the ground-based radionavigation aids restrict aircraft mainly to following pre-defined air traffic routes. In **Figure 1** average sector capacities for the European Civil Aviation Conference (ECAC) Air Traffic Control Centres (ACC) are displayed for 1996.

Increasing air traffic makes route and sector capacity bottlenecks inevitable. Assuming that ACC capacities would remain at their 1996 level ('do nothing option') and that the air traffic develops according to the forecast of an increase of 46% by 2006, then ATFM delays would increase by a factor of 21 [EUROCONTROL, 1997]. However, these delays are very sensitive to the traffic increase: 1% of traffic increase (elasticity) would result in an increase in delay of 20%. The geographical distribution of the average delays estimated for 2006 is displayed in **Figure 2**. They occur in particular over areas with a high density of air traffic or a low density of ground navigation aids, e.g. Paris/Reims/Karlsruhe and the Mediterranean Area and East Europe respectively. To maintain an orderly flow of traffic in these areas ATFM has to be improved by, for example, reducing separation minima and implementing flexible routing through the introduction of more competitive navigation systems.

An initial improvement was forthcoming from the introduction of Basic Area Navigation (BRNAV) for en-route operations in Europe in April 1998 [EUROCONTROL, 1993], [JAA/TGL-2, 1997]. A costly multi-sensor navigation system had been recommended to meet the performance requirements. During 1997, however, it became clear that a number of operators would not achieve the BRNAV requirements on time. In particular, for operators of smaller or old aircraft it would not be technically or economically feasible to install such expensive equipment. In consequence they requested that GPS be approved for BRNAV operation. Feasibility studies were carried out [HEIN, 1997], [TU DELFT, 1997] which revealed that GPS in theory would be technically capable of meeting the BRNAV requirements. Nevertheless, concerns about safety issues remained and GPS was only approved as a BRNAV sensor with
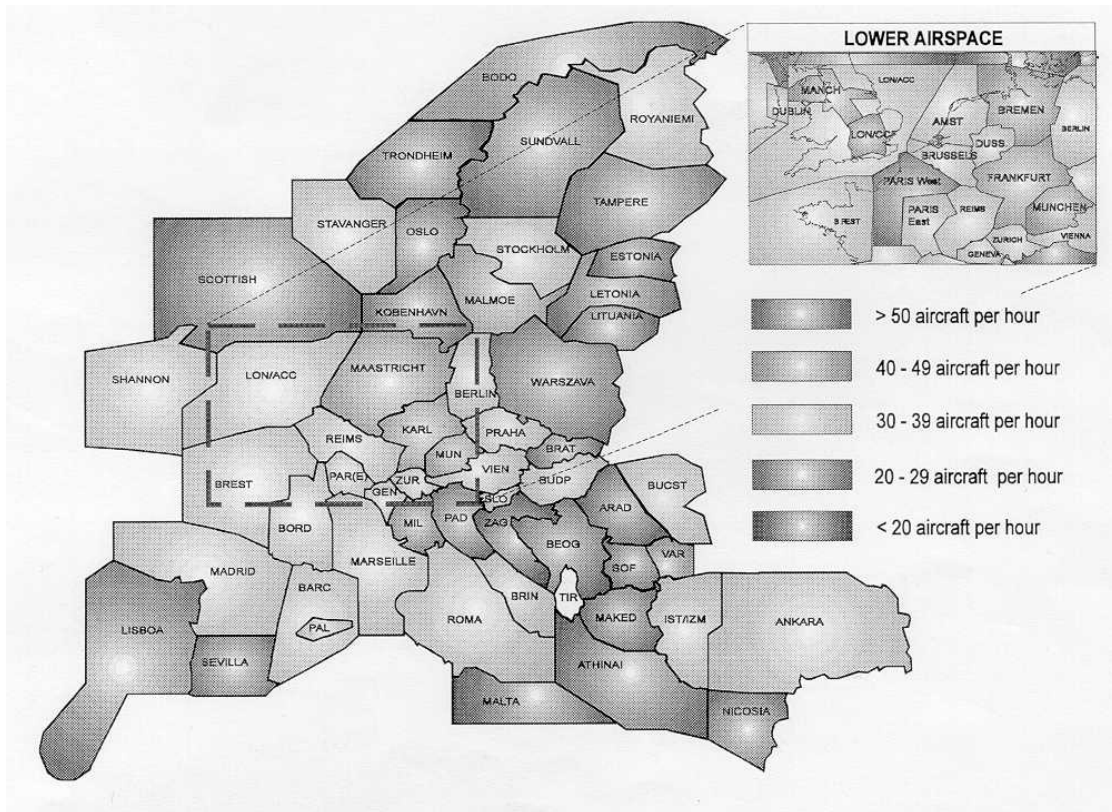
Figure 1: ACC Sector Capacities in 1996 (Aircraft/Hour) [EUROCONTROL, 1997]

strict limitations, which could result in operational penalties for those operators who chose it.

However, if a seamless navigation system could be made available, whose safe operation was undoubtedly proven, a global service could be provided during all phases of flight on free routings with reduced separation minima independent from any ground installation. ATFM could increase air traffic capacities and achieve more efficient routing of the individual aircraft, resulting in shorter flight times accompanied by a higher probability of arriving on time at the destination.

A multitude of advantages would result from such a seamless system:

- Each aircraft need have only one navigation system installed onboard;
- Air crew training can be simplified, workload and system operation errors can be reduced;
- Operating costs of the aircraft can be reduced;
- After a transition phase ground equipment can be decommissioned saving maintenance costs and future investments for replacement;
- Reduced separation minima can be implemented to increase air traffic capacities;
- Lower visibility limits at airports not equipped with Instrument Landing Systems (ILS);
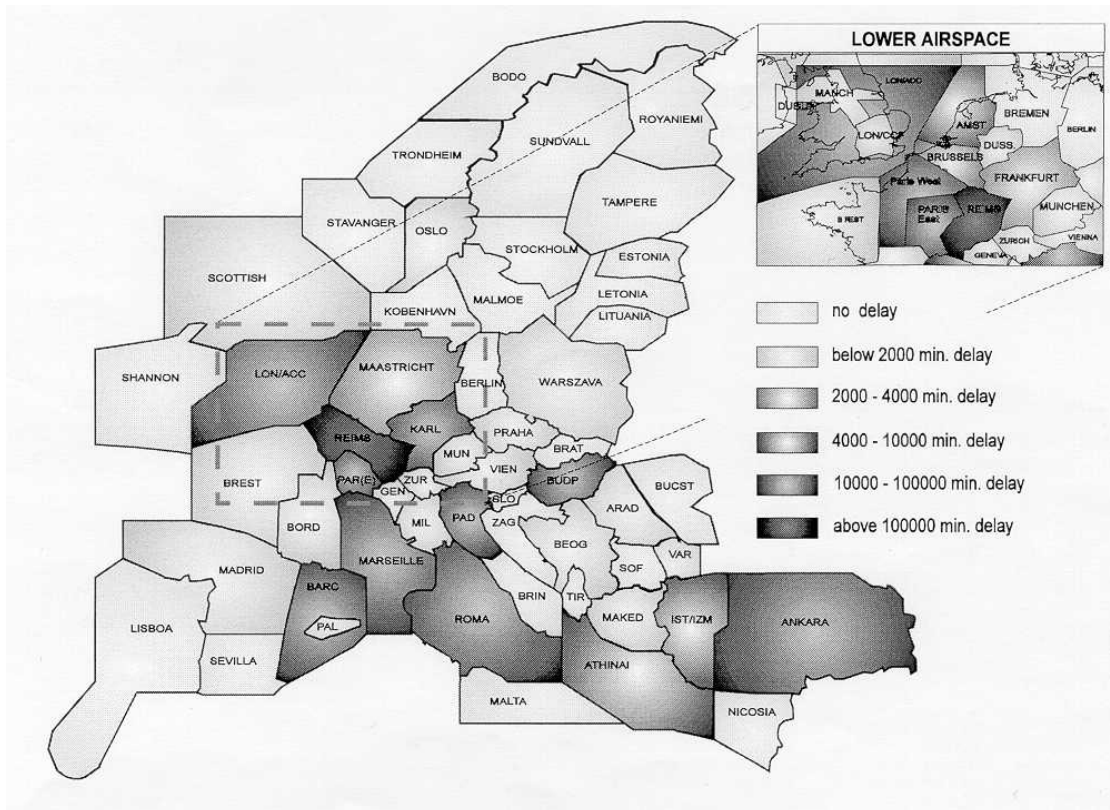
Figure 2: Air Traffic Flow Management Delays in 2006 [EUROCONTROL, 1997]

- Increased runway capacities;
- Operations in areas with insufficient conventional navigation aid infrastructure;
- Air Navigation Safety can be improved over some areas of Europe and over other regions of the globe.

Operational benefits and the improvement of safety on such a scale can, however, only be realised once a global navigation system can be made available to the civil aviation community which fulfils the relevant Required Navigation Performance (RNP) and safety regulatory requirements.

Since the early 1980's, the United States of America has been deploying the NAVSTAR Global Positioning System (GPS) satellites, which provide military and civil users with global navigation capabilities. In 1994 the system reached its operational status with 21 satellites and 3 operational spares orbiting the Earth on six 12h-orbits at 55° inclination with their ascending nodes equally separated. **Table 1** summarises the Standard Positioning Service (SPS) performance specification of GPS as Published by the U.S. Department of Defense for civil users (for more details see Annex C).

Standard	Conditions and Constraints
≥ 99.9% coverage[1]	• 4 or more satellites providing PDOP of 6 or less • 5° mask angle with no obscura • Predicated on 24 operational satellites
≥ 99.85% availabilty[1]	• Conditioned on coverage
≥ 99.97% reliability[1]	• Conditioned on coverage and service availability • 500 meter Not-to-Exceed (NTE) predictable horizontal error reliability threshold
≤ 100 m horizontal accuracy[1] ≤ 156 m vertical accuracy[1] 95% of time	• Conditioned on coverage, service availability and service reliability

Table 1: GPS SPS Minimum Performance Standards [U.S. DoD, 1995]

In parallel the Russian Federation has developed its own navigation satellites and thereby implemented the Global Orbiting Navigation Satellite System (GLONASS) to provide users with a standard navigation service. This constellation of 24 satellites should have been completed by the end of 1997, however, at the time of writing only 10 were operational. The GLONASS satellites orbit the Earth equally spaced on three 11h15min-orbits at 64.8° inclination with their ascending nodes 120° apart. The GLONASS standard navigation service enables the users to determine their positions within 50-70 m accuracy (3σ). The characteristics of GLONASS are regarded as being competitive with GPS [SHIENOK, 1997].

Position Error	95% of Time	99.99% of Time
Horizontal	28 m (92 ft)	140 m (460 ft)
Vertical	60 m (195 ft)	585 m (1920 ft)

Table 2: GLONASS Channel of Standard Accuracy [ICAO/SARPS, 1998]

However, it is obvious that the official U.S. and Russian governmental statements about the performance of GPS and GLONASS cannot provide exhaustive evidence and thereby guarantee that the Required Navigation Performance for civil aviation users can be met in terms of Accuracy, Integrity, Availability and Continuity of Service[2].

Therefore, it is necessary for the civil aviation community to implement monitoring schemes for these satellite navigation systems to ensure that the RNP parameters

---

[1] U.S. DoD Definition (Annex A)

[2] ICAO Definition (Annex A)

are fulfilled or that alarms are generated when they are not met [WATT, 1995], [RTCA/DO-229, 1996]. This will form the basis that operational approval can be granted by Safety Regulation Authorities and that, subsequently, operational and safety benefits can be obtained from the introduction of satellite navigation as discussed above.

Today, it is possible to achieve technical certification of GPS user equipment in accordance with [TSO-C129A, 1996] as a supplemental means[3] of navigation for en-route down to non-precision approach phases of flight. These certifications require the implementation of a specific algorithm which monitors - inside the receiver - the integrity of the signals received from the GPS satellites. Different test cases are prescribed which have to be successfully met to provide evidence in a simulation environment that the equipment meets the requirements.

Recently there have been reports that certain equipment and the implemented algorithms do not behave in-flight as the simulations predict. In one case, the simulation to predict the availability of the required system performance had been carried out with positive results for a number of Non-Precision Approaches. Subsequently, the approaches were flown and during a third of them the actual in-flight performance did not meet the Required Navigation Performance.

These discrepancies between theoretical and measured performance have further increased the Regulatory Authorities' concern about the safety of GPS applications given their existing reluctance to grant approvals for operations purely relying on satellite navigation, because of the numerous unsolved technical and institutional problems.

Based on the described difficulties it is, therefore, currently difficult - if not impossible - to obtain operational approval from Safety Regulators for primary[3] or sole means[3] satellite navigation services except in some isolated cases. This hinders any progress towards gaining operational and safety benefits by improving the current performance of Air Traffic Flow Management in the ECAC area and beyond through a highly competitive and seamless global navigation system.

Currently it is not possible to identify any ongoing activities which address the above described problems in order to propose a practical way forward towards obtaining the respective operational approvals from Safety Regulators. This is where the present thesis commences by developing a unique database independent of any manufacturing industry which allows to answer questions about the performance of

---

[3] ICAO Definition (Annex A)

satellite navigation with a high level of confidence and which develops a practical way forward to subsequently achieve operational approvals.

1.3   OUTLINE

Extensive in-flight data collections are now needed to provide such a database for analyses and subsequent improvement of GNSS integrity monitoring schemes in the airborne environment to demonstrate that GNSS can technically support all aspects of Required Navigation Performance. The results of such a campaign and its subsequent developments shall form the basis for a convincing argument, or 'case', to Safety Regulators about the safety of operations depending primarily or solely on satellite navigation services [LLOYD'S REGISTER/EUROCONTROL, 1997]. Such an undertaking should draw on the experience obtained during the certification of Instrument Landing Systems during the 1960's and 1970's, when extensive flight testing was carried out to gather the evidence that such systems would provide guidance to aircraft during landing in adverse weather conditions with an integrity of only one fatal incident in 10^7 approaches.

One aspect such a flight test campaign should focus on is the validation of Required Navigation Performance (RNP) parameters for the different phases of flight. It has already been mentioned that a number of documents [RTCA/DO-208, 1991], [RTCA/DO-217, 1993], [RTCA/DO-229, 1996] and [GNSSP, 1997/1999] exist which provide a non-validated set of requirements which in its entirety is difficult for Safety Regulation Authorities to accept.

Therefore, the presented work is intended to focus on the following main objectives:

1. Establish a consistent set of Required Navigation Performance (RNP) parameters;

2. Provide conclusive evidence of satellite navigation performance in the operational environment of commercial aircraft and verify, through the obtained results, the set of Required Navigation Performance (RNP) parameters;

3. Develop the Safety Case concept for the use of satellite navigation onboard commercial airliners;

4. Translate the applicability of the developed Safety Case concept into the context of multi-modal transport.

In order to achieve these objectives set above the following proceeding has been chosen:

1. Establish and explain a consistent set of RNP parameters;

2. Implement algorithms capable of describing and evaluating the satellite navigation performance with respect to these RNP parameters;

3. Obtain relevant data from recordings onboard commercial airliners;

4. Develop a database system which allows to validate the RNP parameters using the implemented algorithms and the recorded data;

5. Evaluate the results obtained from the database system;

6. Establish the extend to which the RNP parameters can be validated; use simulated error scenarios where appropriate and describe the representativity of the used data;

7. Develop the Safety Case concept for the use of satellite navigation onboard commercial airliners;

8. Provide the link of the obtained performance validation results into the Safety Case via a risk model including hazard identification and hazard assessment;

9. Describe the applicability of the developed Safety Case concept in the context of multi-modal transport.

Figure 3 outlines the methodology in further details, which provides the framework for the extensive flight trial programme and the development and operation of an appropriate data evaluation tool in order to lead into the Safety Case development.

Having established the RNP parameters, the pre-flight availability of the system integrity monitoring function is predicted and statistically described based on these RNP parameters and real flight data. The predicted and actually obtained in-flight results are compared to carry out a comprehensive evaluation of the system performance both in theory and in the real airborne environment so as to validate the RNP parameters.

In parallel, the particular importance of software engineering and quality assurance is highlighted for the software tool development process in order to provide evidence for
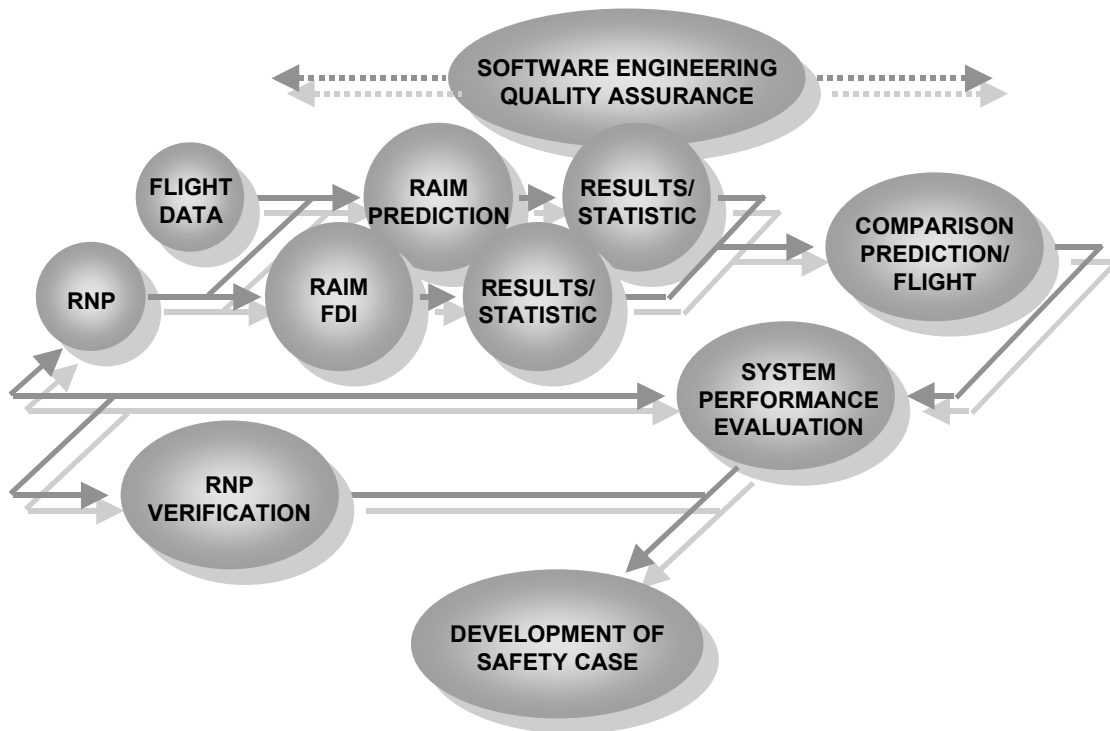
Figure 3: Methodology for the Development of the Safety Case

the high level of confidence which can be placed into the obtained results. These results will then be input to the Safety Case via a hazard identification and hazard assessment.

In order to achieve the objectives through the proceeding and its associated data evaluation methodology – both described above – the work has been structured into the following chapters:

Chapter 2 – Satellite Navigation – summarises the historical background of satellite navigation, in particular, GPS and GLONASS and their technical and performance characteristics. It is discussed why these core systems may fail to meet civil aviation requirements and how this can be solved by introducing augmentation systems. The chapter reflects also on recently proposed system developments.

In **Chapter 3 – Required Navigation Performance –** currently existing specifications for the Required Navigation Performance are extracted from different sources and summarised. A consistent set of parameters is proposed, explained and interpreted in preparation for their input to the system performance evaluation process.

Chapter 4 – Theory of Autonomous Integrity Monitoring – contains a review of different integrity monitoring schemes, which are mathematically capable of describing the satellite navigation system's performance in terms of the established set of RNP parameters. Their mathematical background is explained and the

required input parameters are defined to close the link to the provided RNP parameters before further details are given concerning the monitoring function availability and Failure Detection and Identification (FDI).

The relevant data which are recorded onboard the aircraft during the flight trial programme and the recording procedure itself are described in **Chapter 5 – Flight Trials onboard Commercial Airliners**.

Software engineering and quality assurance procedures, which have been applied during the software development for the data evaluation tool, are explained in **Chapter 6 – Software Development and Quality Assurance**. They are of particular interest to demonstrate the high level of confidence, which can be placed on the results obtained to provide the basis for the Safety Case and, therefore, make them acceptable within a safety regulatory regime.

Chapter 7 – Data Evaluation – introduces the functionality of the data evaluation system and describes different aspects of the data evaluation processes such as satellite visibility scenarios, aircraft and antenna models, the definition of the phases of flight and flights included in the database. Considerations are provided concerning the representativity of the flight data, which form the basis for the obtained data evaluation results. Subsequently, details are provided in order to explain how the different results have to be interpreted with respect to the RNP parameters. The simulator for satellite navigation system error behaviour is briefly described, which has been implemented to investigate the performance of the different monitoring schemes in known error scenarios. These results are used as an additional input to the process of verifying the Required Navigation Performance.

Chapter 8 – Results – describes the results from the data evaluation processes and contains the comprehensive evaluation of the system performance in different airborne scenarios during different phases of flight and the verification of the RNP parameters.

Chapter 9 – Safety Case Development – introduces the development of the Safety Case concept including aspects such as the 'ALARP' Principle, safety standards and the proposal of a risk model and a regulatory mechanism. It is demonstrated how the results obtained in Chapter 8 can be used to lead towards the development of a conclusive Safety Argument or Case in favour of the use of satellite navigation onboard of commercial airliners by applying the risk model through a systematic hazard identification and hazard assessment.

Chapter 10 – Multi-Modal Applicability – discusses the applicability of the achieved results and the Safety Case concept in the context of multi-modal transport.

Chapters 11 – Conclusions – and **12 – Recommendations –** summarise the major conclusions which can be drawn from the work and make recommendations.

2. **SATELLITE NAVIGATION**

2.1 **HISTORY**

In the 1960s the U.S. Navy opened a new era of navigation technology and capability with the navigation satellite system TRANSIT which was developed by the Applied Physics Laboratory (APL) of the John Hopkins University in Maryland [PARKINSON, 1995], [WATT, 1996]. It was followed by a second system, developed by the USSR, with a concept similar to TRANSIT called TSIKADA. By the mid-1960s, two more satellite navigation concepts were under development in the United States: TIMATION by the Naval Research Laboratory (NRL) and program 621B by the Air Force Space and Missile Organization (SAMSO). TRANSIT, 621B and TIMATION were the keys to the development and deployment of the Global Positioning System (GPS).

The TRANSIT system was the result of two things: a vital military need and the advent of advanced technology. The vital need was to have an accurate navigation system available for a new class of submarines dedicated to carry nuclear Polaris missiles. At the time of a missile launch an accurate position solution would be indispensable to ensure that the missile hit the target accurately. Although the submarines were equipped with the latest inertial systems technology, this did not prevent inertial drift. Periodical position updates were required to compensate, which at that time could only be achieved by automated star trackers mounted on the submarine's deck forcing it to surface completely for an update which then was subject to weather conditions.

At the same time as this military need became clear, scientists at the APL discovered the predictability of the entire orbit of low-altitude satellites by measuring Doppler frequency shift data from Sputnik 1 at one ground site during a single pass of the satellite. It was realised that by inverting the process a user position could be determined if the satellite's orbit was already known. This process would require several minutes during which time the satellite would travel several thousand kilometres, providing an excellent baseline. The key advantage with this concept was that a world-wide coverage with periodic updates could be obtained with just one satellite. TRANSIT was born, with the objectives to provide data to analyse the Earth's gravity field, develop stable frequency sources and test ionospheric refraction correction techniques. The TRANSIT satellites orbited the Earth every 107 min on circular, polar orbits at an altitude of approximately 1075 km.

TRANSIT was released to the civil community in 1967 and quickly adopted by oceanographers, off-shore oil exploration companies and surveyors and was soon being integrated into civil marine navigation systems.

The Soviet Union's first satellite navigation system, already mentioned as TSIKADA, was only declared operational in 1971, seven years later than TRANSIT. It was designed as a passive Doppler satellite navigation system similar to its American predecessor.

In 1972, another U.S. Navy satellite system started experimental operation. Known as TIMATION, its satellites were used to provide very precise time and time transfer between various points on the Earth. The ranging signals used a technique called 'side-tone' ranging, which broadcast a variety of synchronised tones to resolve phase ambiguities and allowed the user to estimate the distance between his antenna and the satellite. Preliminary work had begun during the 1960s with the objective of developing an improved quartz frequency standard to reduce the error in the passive ranging links and to determine the most effective satellite constellation for world-wide coverage. TIMATION satellites were flown in inclined orbits: the first two at altitudes of 500 mi and the third at 7500 mi. The latter was also used as a technology demonstrator for GPS.

In 1968 new requirements were issued to precisely locate U.S. military forces world-wide. The most stringent navigation requirements were those for aircraft and became, therefore, the driving parameters. This resulted in a number of comparative studies and ultimately led to the GPS program. As a preparatory step TIMATION was turned into an advanced development program and its third satellite's design and fabrication as an experimental demonstrator began in April 1971. A major experiment incorporated into its payload was an Air Force System 621B transmitter generating a sophisticated spread-spectrum ranging signal based on pseudo-random noise (PRN) techniques. The signal modulation consisted of a repeated digital sequence of almost random bits, generated by using a shift register. The start or phase of the sequence could be detected by the navigation user equipment to determine the range to the satellite. The signals could even be detected when their power density was less than 1/100th of that of the ambient noise, and all satellites could broadcast on the same nominal frequency since properly selected PRN coding sequences would allow a user receiver to identify clearly which satellite's ranging signal was being received. Furthermore, the property of this technique to reject noise also provided a powerful ability to reject most forms of jamming or deliberate interference. A communication channel could be added by inverting the entire code sequence at a slow rate to modulate a stream of digital data to allow the user to receive satellite orbital data. Program 621B was, therefore, the immediate predecessor of GPS.

2.2   GLOBAL POSITIONING SYSTEM (GPS)

During the early 1970's a number of changes within the U.S. Department of Defense (DoD) led to a reform of the systems acquisition process; 'joint' programs were formed which forced the various services to work together. One of the earliest examples was, in fact, GPS thereby bringing together TIMATION and Project 621B. The U.S. Air Force was designated as the executive service and a Joint Program Office (JPO) was established in which all forces were represented.

The first operational prototype GPS satellite was launched into orbit in February 1978. By this time the basic ground control segment had also been deployed, consisting of one master control station at Falcon Air Force Base in Colorado Springs, and four monitor stations at Hawaii, Diego Garcia, Kwajalein and Ascension Island. Since 1978 a total of 38 GPS satellites have been successfully launched representing two generations or 'blocks'. Twelve Block I satellites were built for navigational development although one did not reach its orbit because of a launch failure. Twenty-nine Block II/IIA operational satellites have been built, of which 27 have been successfully launched. The first satellite in this series was declared operational in August 1989. The entry into service was, however, delayed by the loss of the Space Shuttle 'Challenger', the shuttle being planned as the U.S. Air Force launch vehicle for the Block II satellites. This decision was subsequently revised with the result that the Delta II booster is the GPS launch vehicle. Full operational capability was declared by the end of 1994. A further 20 Block IIR satellites are currently being built with options for another six. These satellites have enhanced autonomy, including the capability to meet a degraded range error specification of up to 180 days since the last ground control segment upload. Given the average satellite lifetime of seven years, a full service can be guaranteed until at least 2003. This is the date for which the first launch of a new generation Block IIF satellite is planned to start-off the GPS modernisation programme to be concluded by 2013. The most prominent new feature on board these satellites is the new civil frequency (L5). However, the JPO currently assumes a satellite lifetime of eight years - instead of seven - extendable to 10.6 years for the Block IIA satellites. Paradoxically, this could lead to a delay of the GPS modernisation programme due to the reliability of the current satellites.

In its operational status the GPS satellite constellation consists of 24 satellites including 3 spares orbiting the Earth with an orbital radius of 26560 km relative to the Earth's mass geo-centre. This radius results in two orbital periods per sidereal day and produces repeating ground tracks, with each satellite positioned 4 minutes earlier

each day. The satellites are equally distributed on six orbital planes which are inclined at 55° to the equator.

The fundamental positioning technique for GPS is to use one-way ranging measurements to the GPS satellites, which also broadcast their orbital parameters and error correction values to allow the user to calculate the exact satellite position. Ranges are measured to all satellites simultaneously in view by correlating the incoming signals with a replica signal generated in the user receiver, and measuring the received phases against the user's crystal clock. With a minimum of four satellites in an appropriate geometry, four unknowns can be determined, namely the three-dimensional position and a correction to the user receiver's clock.

The GPS ranging signal is broadcast at two frequencies: a primary signal at 1575.42 MHz (L1-Band) and a secondary broadcast at 1227.6 MHz (L2-Band). These signals are generated synchronously, so that a user who receives both signals can directly correct for the ionospheric error. Two modulations are transmitted: the Clear Acquisition (C/A-) Code on L1 and the Precise (P-) Code on L1 and L2. These modulations provide two services: the Standard Positioning Service (SPS) from the C/A-Code and the Precise Positioning Service (PPS) from the P-Code. The PPS is encrypted and only available to authorised users. The SPS, while available to all users, can be intentionally degraded by the system operator by desynchronising the satellite clock or introducing small errors in the broadcast orbital parameters (ephemeris). This is known as Selective Availability (SA).

2.3   GLOBAL ORBITING NAVIGATION SATELLITE SYSTEM (GLONASS)

Russia's GLONASS was also conceived in the early 1970's, drawing on the experience with TSIKADA. The 24 satellites of its operational constellation are evenly arranged in three orbital planes which are inclined at 64.8° to the equator and spaced 120° apart. It is worth noting that this constellation corresponds to the initial GPS plans until the Challenger loss, obliging the U.S. to use rocket boosters instead, which were not capable of injecting the satellites into such inclined orbits. GLONASS, like GPS, is a pseudo-ranging system. However, there are some important differences. Firstly, the orbital radius of the constellation is 25510 km, 1050 km less than that of GPS, resulting in an orbital period equal to 8/17 sidereal days. Secondly, GLONASS employs Frequency Division Multiple Access (FDMA) requiring every satellite to broadcast on a slightly different frequency. FDMA does not require special code modulation to distinguish satellites, therefore all satellites transmit the same code. Thirdly, GLONASS co-ordinates are expressed in the geodetic system 'Parameters of the Earth 1990' (PZ90) whereas those for GPS are given in the 'World

Geodetic System 1984' (WGS 1984), which has been promulgated by the International Civil Aviation Organisation (ICAO) as the global co-ordinate system for aviation with effect from the 1st January 1998. Finally, GLONASS is referenced to the 'Universal Time Co-ordinated (SU)' (UTC-SU) while GPS is synchronised to western UTC.

The GLONASS satellites emit signals on two basic carrier frequencies: 1602 MHz (L1) and 1246 MHz (L2), the exact frequency being a function of the GLONASS satellite's channel number. Like GPS, a C/A-Code is modulated on L1 only and a P-Code is modulated on both frequencies.

2.4 GPS, GLONASS AND CIVIL AVIATION

The 'Special Committee for the Monitoring and Co-ordination of Development and Transition Planning for the Future Air Navigation System (FANS)', set up in 1983 by the Council of the International Civil Aviation Organisation (ICAO), concluded its work in 1988 with the recommendation that ICAO move to a satellite-based Communications, Navigation and Surveillance/Air Traffic Management (CNS/ATM) concept. During follow-up work it was argued that the introduction of new technologies such as GNSS into ATM would improve efficiency, maintain safety and reduce costs [FANS(II)/4, 1993]. This would be achieved by increased airspace and optimised airport capacity, dynamic flight planning and reduced controller and pilot workload. The benefits of GNSS were seen, in particular, to provide world-wide service up to ICAO CAT I Precision Approach and enable aircraft to navigate using a single set of avionics.

However, technical and institutional limitations have prevented both GPS and GLONASS from being introduced as a sole means of navigation for civil aviation. GPS and GLONASS are, if at all, only capable of meeting horizontal accuracy requirements up to Non-Precision Approach operations. On their own, they cannot meet any other requirements such as Integrity. Neither GPS nor GLONASS have been designed to provide rapid warnings to the users in case of problems with individual satellites. In addition, both systems are under control by single States, which causes major difficulties for national safety regulation authorities in granting technical and, in particular, operational approvals [LLOYD'S REGISTER, 1997], [TIEMEYER, ET.AL., 1997].

If GPS and GLONASS are proposed to be used in civil aviation today, aircraft-, ground- or satellite-based augmentation techniques have to be implemented to

improve their performance and to monitor the systems' status which, subsequently, will allow them to be approved as safe for the intended use. These techniques are:

RAIM - Receiver Autonomous Integrity Monitoring uses the redundancy of simultaneous measurements to more than four satellites to check whether they are consistent or if one satellite signal may be erroneous. In the case of five received satellites, simple redundancy allows detection that a satellite is transmitting inaccurate information. However, a minimum of six satellites is required to identify which satellite is faulty, provided that the local satellite constellation satisfies a number of geometric requirements.

AAIM - Aircraft Autonomous Integrity Monitoring combines the measurements obtained from satellite receivers with information from independent onboard sensors to improve integrity and availability.

GBAS - Ground-based Augmentation Systems are designed to improve accuracy and integrity and, hence, availability for precision approach operations according to ICAO CAT I-III requirements. These local-area ground stations monitor the satellite system status and calculate correction terms which are uplinked to the approaching aircraft to enhance the onboard position calculation. A second technique includes installing beacons - so-called pseudolites - on the approach path to provide the aircraft with additional ranging information. This allows the onboard system to improve positioning accuracy considerably and to have increased measurement redundancy available for integrity checks.

SBAS - Satellite-based Augmentation Systems are currently under development by the United States (WAAS), Europe (EGNOS) and Japan (MSAS). These systems operate navigation payloads flown on geostationary satellites. Their role is to augment the performance of GPS – in case of EGNOS also of GLONASS – by improving their service integrity and accuracy of their measurements. SBAS are based on a specific signal that would allow the same user functionalities to be suitable for multi-modal transport applications.

However, these augmentation techniques are fully dependent on the core positioning service provided by GPS and GLONASS. As long as their performance can deliberately be degraded over some areas of the Earth or access to their signals can even be denied for civil users an approval as a sole-means of navigation is almost impossible. Offers have been made by the FAA to the ICAO Council *"to make GPS-SPS available for the foreseeable future on a continuous, world-wide basis and free of direct user fees"* [HINSON, 1994]. A similar offer has been received from the Russian Federation concerning GLONASS [KOTAITE, 1996]. Depending on solutions

to these institutional problems a final solution may only come along with the development and introduction of the next generation satellite navigation system, control of which would be in civil hands.

2.5   RECENT DEVELOPMENTS - GALILEO

Galileo is an initiative of the European Union (EU) and the European Space Agency (ESA) [Ec, 1999]. It comprises the development, implementation and operation of a state-of-the-art global navigation satellite system under civil control. Galileo will be Europe's second step towards satellite navigation following EGNOS.

Within the Galileo system, 21 or more satellites will provide navigation signals to the users world-wide. Most of the satellites will be in medium altitude Earth orbits. Geostationary satellites, typically three over the European region, may complement them. Galileo will pursue an open system architecture, interoperable with GPS and open for augmentations depending on the specific requirements. The performance of Galileo is planned to be much beyond the current GPS standard positioning service. At least two different service classes will be offered. The basic service will be available to everybody free of charge. A 'controlled access service' will be offered with availability and liability guarantees. It will be available to registered users only. This premium service enables Galileo, because of its civil control and related performance and service guarantees, to fulfil certification and standardisation requirements for safety critical applications, such as in civil aviation.

Galileo is intended to constitute, together with GPS, the future Global Navigation Satellite System (GNSS). Galileo and GPS will be independent systems, but fully compatible and interoperable in order to provide maximum benefits for the users. The combined use of both systems is considered as being crucial to achieve the required performance levels for certain applications. As of today it is estimated that road transport will account for 77% of the user equipment market. The maritime sector, railways and civil aviation may take a market share of 1% each.

According to the current planning Galileo will be fully operable in 2008 at the latest, with the start of signal transmission in 2005. The programme decision was taken in June 1999 and the definition phase is kicked-off to be finished by the third quarter of the year 2000. Subsequently, the development phase will be finished before the validation and test phase will be kicked-off in 2004. The latter phase will be performed by 3 to 5 satellites and will overlap to the serial production and deployment phase of the remaining satellites.

3. REQUIRED NAVIGATION PERFORMANCE

3.1 OVERVIEW

Today a number of sources are available, which provide sets of parameters and numbers to describe the Required Navigation Performance (RNP) for civil aviation applications [RTCA/DO-208, 1991], [AWOP/15, 1994], [RTCA/DO-229, 1996], [TSO-129A, 1996], [GNSSP, 1999]. The concept of RNP was initially defined by ICAO [ICAO, 1994]. Unfortunately, the definitions used in these different sources are not always compatible and, as a result, requirements are difficult to compare with each other. All sources are using the following parameters as a baseline:

1. Accuracy,
2. Integrity,
3. Availability and
4. Continuity of Service.

This chapter is an attempt to first define these four parameters in a consistent manner, secondly to express them in mathematical terms, which can be implemented for the data evaluation, and thirdly to provide requirements associated with these mathematical terms.

3.2 DEFINITIONS

3.2.1 Accuracy

The only official accuracy definition describing the GPS Standard Positioning Service has been published by the U.S. Department of Defense [U.S. DOD, 1995] (Section 1.2):

> *The percentage of time over a specified time interval that the*
> *difference between the measured and expected user position or time*
> *is within a specified tolerance at any point on or near the Earth.*

This definition contains major difficulties for civil aviation applications: The time interval has been specified with 24 hours, it is not clear what effect a shorter time interval may have, e.g. the interval covering an approach. It is referred to one location and no information is given on the error distribution and spectrum.

The ICAO All Weather Operations Panel [AWOP/15, 1994] has defined Accuracy for the approach phase of flight as follows:

> *Accuracy is the ability of the total system to maintain the aircraft position within a Total System Error (TSE) limit with a 95% probability at each point along the specified procedure and to keep it within an outer performance boundary with a probability of no less than $1-1.0\cdot10^{-7}$ per approach.*

Here accuracy is defined through the Total System Error (TSE) which is the combination of the Navigation System Error (NSE) and the Flight Technical Error (FTE). Two points of a probability distribution are specified without any details whether a temporal or spatial distribution is assumed nor of which type the distribution may be. In addition the difficulty arises to isolate the NSE from the TSE to formulate requirements for the navigation system.

In order to determine TSE, NSE and FTE it will be necessary to use a position reference system, which independently from the navigation system is capable of measuring the position of the aircraft at any instant in time. Such a system was not available during the data recording campaign, which provided the basis for the presented results. It had been decided to simplify the data evaluation related to Accuracy, in order to be able to provide assumptions on the Accuracy, which would be required to present consistent results on the four RNP parameters. The simplified Accuracy evaluation is presented in Section 7.2.6 and implies the following definition of Accuracy [BREEUWER ET.AL., 1998]:

> ***ACCURACY:*** *The position error that will be experienced by a user with a certain probability at any instant in time and at any location in the coverage area. In general, the probability is required to be 95%.*

This definition is applicable only to non-precision applications such as en-route operations up to Non Precision Approach (NPA); for applications such as Precision Approach (PA) more information on the error distribution than only the 95%-percentile of the probability distribution will be required.

3.2.2 Integrity

A definition for integrity is given in [BREEUWER ET.AL., 1998], which is self-explanatory:

INTEGRITY: The integrity risk is defined as the probability that a user will experience a position error larger than the Alert Limit without an alarm being raised within the specified Time-to-Alarm at any instant in time and at any location in the coverage area.

3.2.3 Availability

The availability of the navigation service for the user is established by fulfilling the Accuracy and Integrity requirements at the same time:

AVAILABILITY: The probability that a user is able to determine his position with the required accuracy and is able to monitor the integrity of his determined position at any instant in time and at any location in the coverage area.

3.2.4 Continuity of Service

Continuity of Service requires that the navigation service is available for the user during a certain time interval for the relevant phase of flight:

CONTINUITY: The probability that a user is able to determine his position with the required accuracy and is able to monitor the integrity of his determined position at any location in the coverage area over a minimum time interval applicable to the corresponding phase of flight.

3.3 PROPOSAL FOR A CONSISTENT SET OF RNP PARAMETERS

Accuracy

The Accuracy requirements for the different phases of flight are expressed in the form of Navigation System Errors in **Table 3**. These are derived from RNP 1 and RNP 0.3 figures following the methodology of [AWOP/16, 1997]. RNP 1 and RNP 0.3 are described by an alert limit of 1 nm and 0.3 nm (= 5σ NSE), respectively. The accuracy limit is subsequently set to the 2σ NSE value [AWOP/16, 1997].

Phase of Flight	Departure	En-route	Terminal	Initial Approach	NPA
RNP Environment	RNP 0.3	RNP 1	RNP1	RNP 0.3	RNP 0.3
Horizontal Accuracy Limit [m]	220	740	740	220	220

Table 3: Required Accuracy Performance (Navigation System Error)

Standard Deviation of Pseudorange Measurement

Table 4 contains the requirements related to Integrity, Availability and Continuity. For a number of calculations in Chapter 4 the *a priori* standard deviation of the pseudorange measurements is set to 33.3 m according to [RTCA/DO-208, 1991]. This value can be calculated from equation 7.1 assuming an average position accuracy of 100m for GPS and an average HDOP of the nominal 24-satellite constellation of 1.5.

Horizontal Alert Limit and Time-to-Alarm

The Horizontal Alert Limit - as required by the definition for Integrity - is set to 1850 m (RNP 1) and 555 m (RNP 0.3), respectively, for the different phases of flight. If the position error experienced by the user exceeds the Alert Limit, an alarm has to be raised within the specified Time-to-Alarm.

Integrity

The following paragraphs shall explain – using the example of final approach – how the Integrity requirement for satellite navigation can be derived from the high-level Target Level of Safety (TLS). The TLS is the index against which the calculated risk can be compared, in order to make a judgement of whether the operation of the system under consideration will be safe. The TLS in aviation is expressed in units of hull losses (rather than passenger fatality rates) per aircraft flight hour. The TLS generally is determined through historic accident data (see also Section 9.2) and is subsequently allocated to sub-system elements.

431 Hull Loss Accidents 230 Million Flights 339 Million Flight Hours	Historical Data Average Hull Loss per Mission 1.87×10^{-6} (excl. Taxi, Load, Unload)	→	Based on World-wide Jet Operators for Aircraft Heavier than 60,000 lbs. (Does not include Turbo-Prop Aircraft) 1959 - 1990

Take-Off Risk 27×10^{-8}	Initial Climb Risk 22×10^{-8}	Climb Risk 13×10^{-8}	Oceanic or En-route Risk 9×10^{-8} /h	Descent Risk 14×10^{-8}	Initial Approach 24×10^{-8}	Final Approach 51×10^{-8}	Landing Risk 27×10^{-8}

Risk Allocation Based upon ICAO Historical Data

TLS Improvement

Target Level of Safety 1.5×10^{-7} per Mission → TLS 1×10^{-7} per Hour (1.5 Hour Average Mission Time)

Take-Off Risk 1×10^{-8}	Initial Climb Risk 1×10^{-8}	Climb Risk 2×10^{-8}	Oceanic or En-route Risk 5×10^{-8} /h	Descent Risk 2×10^{-8}	Initial Approach 2×10^{-8}	Final Approach 1×10^{-8}	Landing Risk 1×10^{-8}

Figure 4: Hull Loss Risk per Mission [AWOP/15, 1994]

Figure 4 sets out that the average hull loss per mission is 1.87×10^{-6}, based on the fact that the world-wide commercial jet operations – from 1959 until 1990 – totalled 339 million flight hours during 230 million departures and had 431 hull loss accidents. This yields a TLS expressed in hull losses per flight hour of 1.27×10^{-6}. In [AWOP/15, 1994] the historical data are apportioned for accident rate and exposure time for each phase of flight leading to a hull loss risk per mission for all phases of flight as presented across the top of Figure 4.

For [AWOP/15, 1994] the necessity arose to propose a TLS for the average flight mission. Partial support for the risk allocation improvements over the historic accident rates was seen in the reduction of piloting errors by the use of glass-cockpit aircraft. The indicated TLS improvement for each phase of flight is roughly inversely proportional to the piloting errors, which were identified as the root-cause of the hull loss accidents during the different phases of flight. Another reason for the considerable improvement in the TLS lies in the fact that it is desirable to maintain the absolute number of hull loss accidents per year as constant although the air traffic volume will drastically be increasing over the coming years. Returning to the initial example, final approach (grey box, Figure 4) is allocated the portion of 1×10^{-8} from the overall TLS.
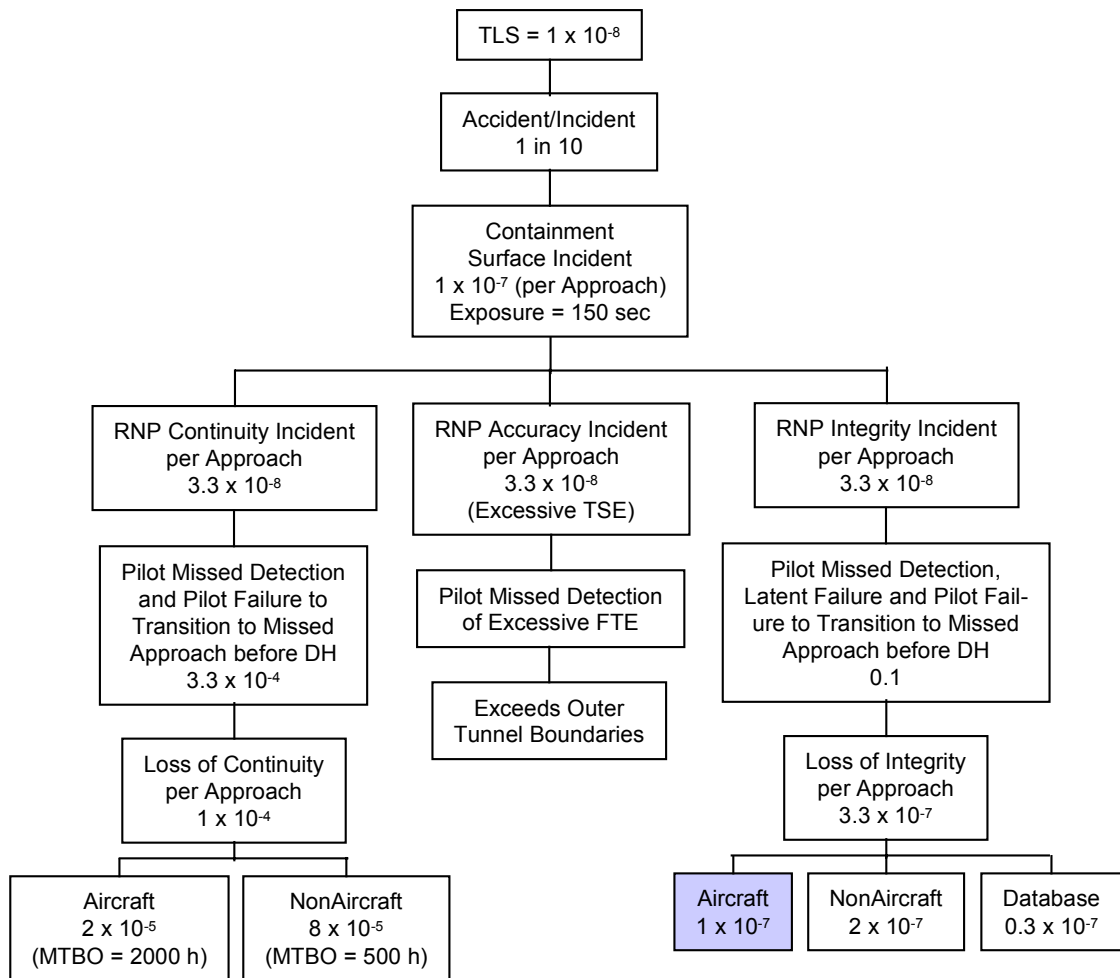
Figure 5: RNP Risk Allocation [ICAO, 1995]

The apportionment of the TLS needs a further break down to arrive at the navigation system level at the aircraft. The respective risk allocation is displayed in **Figure 5** [ICAO, 1995]. In the risk tree, parallel boxes represent an addition of risks and serial boxes represent a multiplication of risks. Following the risk allocation tree, the risk of loss of integrity onboard the aircraft is determined to be 1×10^{-7} per approach. These facts led ICAO [GNSSP, 1999] finally to the decision to fix the Integrity Risk – or Undetected Failure Rate (FR_U) – to 1×10^{-7} per flight hour or approach, respectively. In the context of ICAO requirements it is standard practice to express any of these rates either per flight hour or per approach operation by using the same numerical value.

Probability of Missed Detection

For RAIM algorithms the allowable Probability of Missed Detection is specified as 1×10^{-3} in [RTCA/DO-208, 1991]. The following considerations explain how this number was initially determined and how it relates to the integrity requirement of 1×10^{-7}.
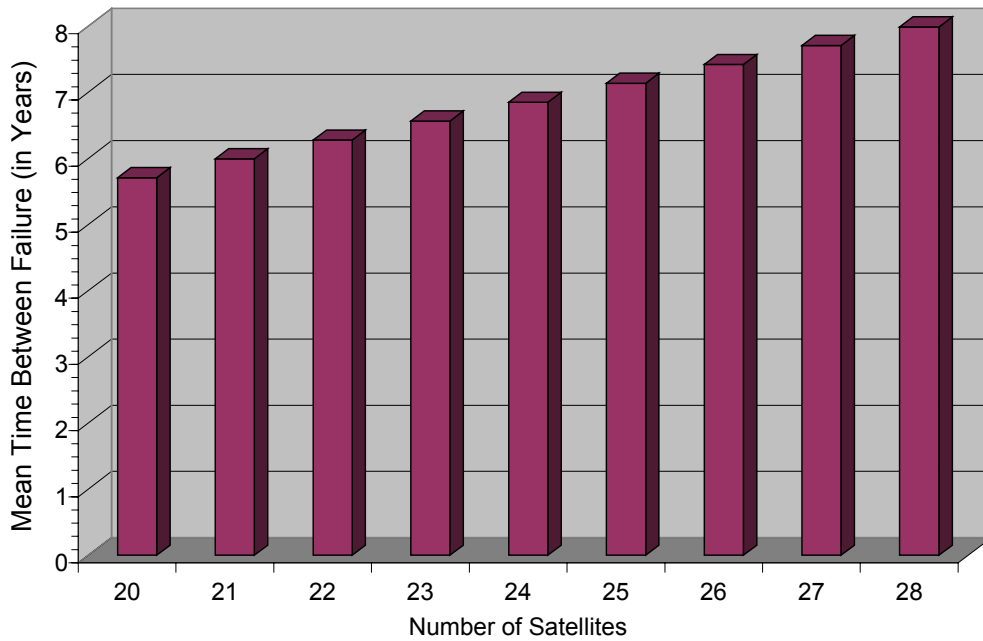
Figure 6: Required Minimum MTBF as a Function of the Number of Satellites

Equation 3.1 describes the relationship between the Probability of Missed Detection (P_{MD}) and the Undetected Failure Rate (FR_U) as a function of the Mean Time Between Failure (MTBF) of the individual satellites, the total number of satellites (N_{SV}) and the assumption that any user can see on average a quarter of the entire constellation:

$$P_{MD} = FR_U \cdot \frac{MTBF \cdot 4}{N_{SV}} \qquad (3.1)$$

with P_{MD} Probability of Missed Detection
            FR_U Undetected Failure Rate (Integrity Risk)
            $MTBF$ Mean Time Between Failure
            N_{SV} Total number of satellites in the constellation.

Using an estimated MTBF of 60,000 hours (6.85 years) for any satellite in the nominal 24 satellite constellation yields the above result for the allowable Probability of Missed Detection of 1 x 10^{-3}.

Figure 6 illustrates the minimum MTBF as a function of the number of satellites to fulfil the requirements for the Probability of Missed Detection (P_{MD}) and the Undetected Failure Rate (FR_U) at the same time. A constellation of currently 26 active satellites, therefore, has to achieve an MTBF for the individual satellites of 7.42 years at least.

<u>False Alarm Rate</u>

The acceptable maximum False Alarm Rate is specified with 1×10^{-5} false alarms per hour [RTCA/DO-229, 1996]. There is no source available how this requirement was derived. However, it can be related to the 'loss of continuity' referred to in Figure 5.

Loss of continuity can be caused either through false alarms or real alarms. The frequency of the latter to occur can be determined from equation 3.1 to 1×10^{-4} per hour for a 24-satellite constellation. In order to not exceed the share for the loss of continuity the false alarm rate is required to be of one magnitude lower.

The required False Alarm Rate, the Undetected Failure Rate and the Probability of Missed Detection have only to be achieved during times when the geometry of the satellite constellation is sufficient to allow for the integrity monitoring functions to work reliably [RTCA/DO-208, 1991].

<u>FD and FDI Availability</u>

The availability of these integrity monitoring functions is specified through Failure Detection (FD) Availability and Failure Detection & Identification (FDI) Availability requirements [RTCA/DO-229, 1996]. Detailed explanations of these functions are provided in Chapter 4. In [RTCA/DO-229, 1996] it is explained that the numerical values are based upon simulations and analysis of the practical availability provided by the satellite constellation. The figures are intended to ensure a consistent minimum capability which can be used by airspace designers.

<u>Continuity of Service</u>

The Continuity of Service is specified through 300 seconds and 150 seconds Total Outage Duration respectively [EUROCONTROL, 1998]. A Final Approach shall only be commenced if Availability is predicted. After commencement the Total Outage Duration is 0 seconds during the final 150 seconds until touch-down.

The parameters and their numerical values derived from different sources, have been set into a satisfactory context to each other and, consequently, a consistent set of RNP requirements has been established which describe sufficiently the navigation performance required by aviation users.

Phase of Flight	Departure	En-route	Terminal	Initial Approach	NPA
σ of Pseudorange Noise [m]	33.3	33.3	33.3	33.3	33.3
Horizontal Alert Limit [m]	555	1850	1850	555	555
Time to Alarm [s]	10	15	15	10	10
Integrity Risk [h^{-1}]	10^{-7}	10^{-7}	10^{-7}	10^{-7}	10^{-7}/150 s
Probability of Missed Detection	$1 \cdot 10^{-3}$	$1 \cdot 10^{-3}$	$1 \cdot 10^{-3}$	$1 \cdot 10^{-3}$	$1 \cdot 10^{-3}$
False Alarm Rate [h^{-1}]	10^{-5}	10^{-5}	10^{-5}	10^{-5}	10^{-5}
FD Availability	0.998-0.999	0.998-0.999	0.998-0.999	0.998-0.999	0.998-0.999
FDI Availability	0.9455-0.982	0.9455-0.982	0.9455-0.982	0.9455-0.982	0.9455-0.982
Continuity of Service [s]	150	300	150	150	0s/150s

Table 4: Required RAIM Performance

3.4   REQUIREMENTS FOR OTHER MODES OF TRANSPORT

[EGS, 1999] is an attempt to develop a set of requirements for maritime navigation applications based on expert judgement. Tables are established which contain parameters defined similar to those for civil aviation. Numbers reported for Accuracy vary between 500 m for ocean and 1 m for port operations. Some numbers are given for Integrity and Availability, although many requirements remain 'to be decided'. Terrestrial users are likely to develop a market for safety-critical navigation applications in the near future. However, it is currently not possible to identify any published documentation concerning requirements from this user community.

4. **THEORY OF AUTONOMOUS INTEGRITY MONITORING**

4.1 GENERAL

GPS provides basic Integrity information via the navigation message transmitted by each satellite, but this information is not provided in a timely manner such that a user receiver could meet civil aviation application requirements. Consequently, additional means of providing Integrity information are required. Different approaches have been briefly introduced in Section 2.4. One of these approaches - namely Receiver Autonomous Integrity Monitoring (RAIM) - will be detailed in this chapter.

A variety of RAIM schemes have been proposed in the literature. They are all based on the same principle of carrying out a self-consistency check amongst redundant measurements using statistical decision theory. Two hypothesis-tests are considered: i) Does a failure exist and ii) which satellite is transmitting a faulty signal? The first test is called Failure Detection (FD) the second Failure Identification (FI). For all these tests it is assumed that only one satellite at a time will be transmitting an unpredicted erroreonus signal. This assumption is based on information provided by the United States Air Force, who consider two unpredicted GPS satellite outages as 'improbable' [SOLAT, 1996].

Three RAIM algorithm schemes which have been proposed for implementation are:

- Parity Method: [STURZA, 1988], [STURZA/BROWN, 1990], [BROWN/STURZA, 1990]
- Least-Squares-Residuals Method: [RTCA/DO-208, 1991], [PARKINSON, AXELRAD, 1988]
- Constant-Detection-Rate/Variable-Protection-Level Method: [BRENNER, 1990]

Although the first two algorithms are different in their approach a linear transformation can be found to demonstrate their equivalence [BROWN, 1992]. Therefore, the following section concentrate on two groups of algorithms, namely BROWN/STURZA and BRENNER.

Before these algorithms can be applied in-flight, a prediction is needed to determine whether the geometry of the available constellation of satellites will be sufficient to allow for RAIM (RAIM Availability).

Four satellites are the minimum to calculate the user position and the time offset between the receiver clock and the GPS time standard. However, this assumes that

the satellites are in a favourable geometric distribution. With a minimum of five satellites it is possible to detect whether an error exists in one of the measurements - again assuming a certain geometrical quality of the constellation. At least six satellites are required to carry out Failure Detection & Identification (FDI).

4.1.1 Observation Equation

The basic principle of satellite navigation by simultaneous range measurements to all satellites in view has been introduced in Section 2.2. A range measurement to an individual satellite can be described by the following observation equation:

$$z = \rho + c(\delta t - \delta T) + d_{ion} + d_{trop} + \varepsilon_n \qquad (4.1)$$

with z measured pseudo-range
     ρ geometrical range
     c speed of light
     δt satellite clock error
     δT receiver clock error
     d_{ion} ionospheric error
     d_{trop} tropospheric error
     ε_n measurement noise.

The geometrical range ρ_i between the receiver and the satellite 'i' is expressed by:

$$\rho_i = \sqrt{(x_i - x)^2 + (y_i - y)^2 + (z_i - z)^2} \qquad (4.2)$$

with (x, y, z) receiver position
     (x_i, y_i, z_i) satellite position.

Since the satellite positions and a number of the errors included in the observation equations can be modelled, an equation system remains which has four unknowns: the receiver position (x, y, z) and the receiver clock error δT.

4.1.2 Measurement Model

The observation equations for the individual satellites result in the following non-linear equation system:

$$\underline{z} = \underline{\underline{H}}\,\underline{x} + \underline{\varepsilon} \tag{4.3}$$

with $\underline{z}$ n x 1 vector of linearised measurements compensated by *a priori* information

        $\underline{H}$ n x 4 measurement matrix (direction cosine matrix)

        $\underline{x}$ n x 1 innovation vector

        $\underline{\varepsilon}$ n x 1 vector of Gaussian-distributed measurement errors

        n   Number of Satellites.

This equation system is over-determined in the case of more than four measurements and is usually solved by a least-square adjustment.

The least squares estimate of the position innovation vector is given by:

$$\hat{\underline{x}} = \left(\underline{\underline{H}}^{T}\,\underline{\underline{H}}\right)^{-1}\underline{\underline{H}}^{T}\,\underline{z} \tag{4.4}$$

with $\hat{\underline{x}}$ least squares estimates of innovation vector

and $\underline{\underline{C}} = \left(\underline{\underline{H}}^{T}\,\underline{\underline{H}}\right)^{-1}$ (4.5)

known as the Covariance-Matrix.

The difference between the linearised measurements and the least square estimates describes the measurement - or pseudorange - residuals:

$$\overline{\underline{z}} = \underline{z} - \hat{\underline{z}} \tag{4.6}$$

with $\overline{\underline{z}}$ vector of measurement residuals.

By employing (4.3) and (4.4) the vector containing the pseudorange residuals can be expressed as:

$$\overline{\underline{z}} = \left[\underline{\underline{I}} - \underline{\underline{H}}\left(\underline{\underline{H}}^{T}\,\underline{\underline{H}}\right)^{-1}\underline{\underline{H}}^{T}\right]\cdot\underline{\varepsilon} \tag{4.7}$$

4.1.3 Dilution of Precision

The Dilution of Precision (DOP) represents a scalar, which describes the geometrical quality of a particular constellation of satellites included in the measurement model.

There is a number of different DOPs, which can be derived from the main diagonal (trace) of the Covariance-Matrix. For the present investigations the Horizontal Dilution of Precision (HDOP) and the Vertical Dilution of Precision (VDOP) are of interest only. They are calculated from the first two elements and the third element of the main diagonal, respectively:

$$HDOP = \sqrt{C_{11}^2 + C_{22}^2}$$
$$VDOP = C_{33}$$

(4.8)

with   *HDOP*   Horizontal Dilution of Precision
       VDOP   Vertical Dilution of Precision.

All RAIM strategies are based on tests of sub-set satellite constellations. Individual satellites are excluded from the total constellation and the decrease of geometrical quality is expressed by the following equation:

$$\delta HDOP_i = HDOP_i - HDOP$$

(4.9)

with $\delta HDOP_i$ Increase in HDOP when excluding satellite 'i'
       $HDOP_i$ HDOP calculated after exclusion of satellite 'i'.

4.2   RECEIVER AUTONOMOUS INTEGRITY MONITORING (RAIM)

Based on the fundamental considerations applied to satellite navigation presented in Section 4.1, this section provides the mathematical background (i) to evaluate the geometrical quality of a given satellite constellation and whether it is sufficient to allow for the application of RAIM algorithms and (ii) to subsequently detect and identify a faulty satellite.

4.2.1   Hypothesis Testing

To determine whether an error has occurred in one of the measurements, statistical hypotheses can be formulated about the assumption that a defined event - here: no failure - will occur:

Null-Hypothesis H_0:   assumption that no failure will occur
Alternate Hypothesis H_1:   assumption that a failure will occur.
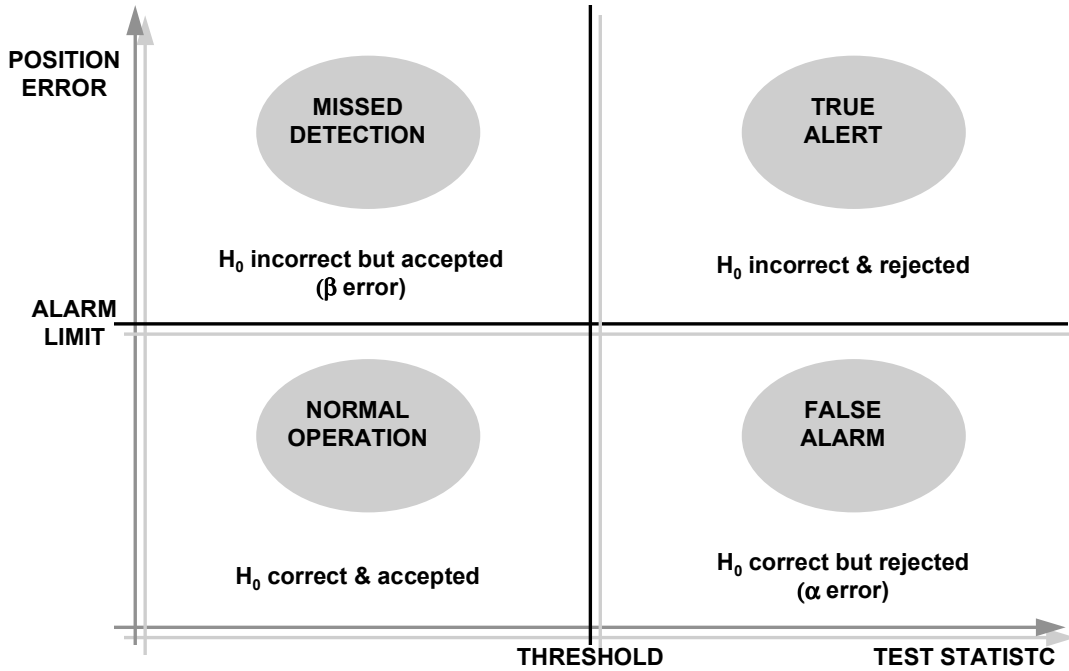
Figure 7: Probability Domain

The test methods, which are applied by the different RAIM algorithms, are based on a number of random samples to decide whether the Null-Hypothesis H_0 has to be rejected or can be accepted in the probability domain. This decision process is implemented by a comparison of a decision Variable D with a Threshold T:

$$D < T \quad \text{Null-Hypothesis } H_0 \text{ accepted} \tag{4.10}$$

$$D \geq T \quad \text{Alternate-Hypothesis } H_1 \text{ accepted} \tag{4.11}$$

with D Decision Variable

         T Threshold.

Figure 7 illustrates the four possible situations, which can result from these tests: normal operation, true alert, missed detection and false alarm. The probability of occurrence for the latter two situations are expressed by the following equations:

$$P_{MD} = P\big(D < T \big| H_1\big) \tag{4.12}$$

$$P_{FA} = P\big(D \geq T \big| H_0\big) \tag{4.13}$$

with P Probability Function

         P_{FA} Probability of False Alarm

         P_{MD} Probability of Missed Detection.
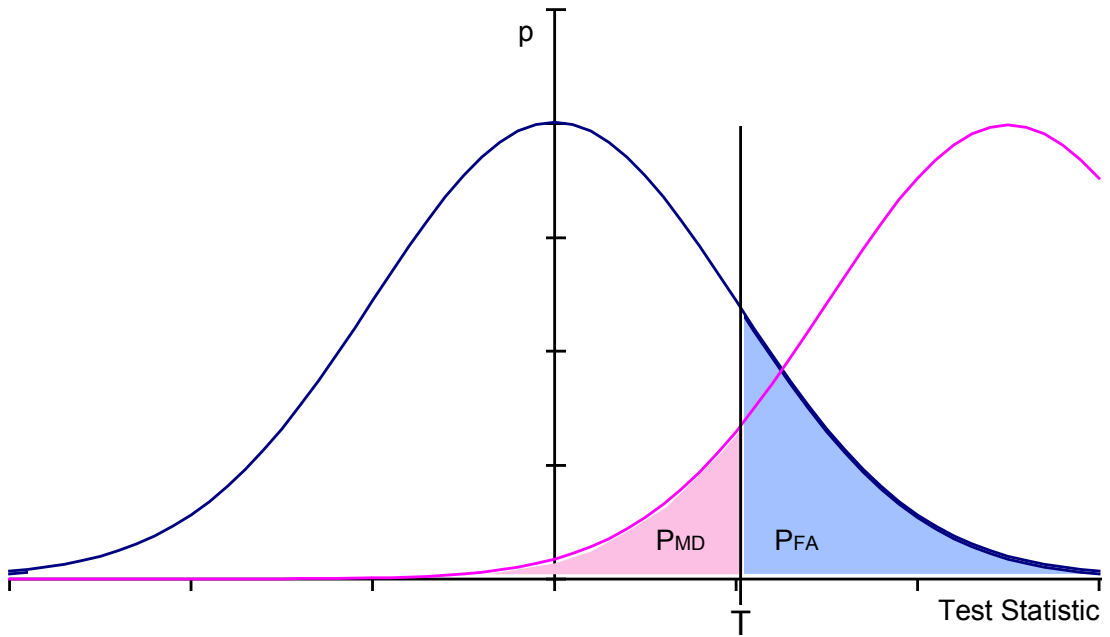
Figure 8: Central and Non-Central Probability Distribution

The threshold *T* is dependent on the maximum allowable position error - called the Horizontal Alarm Limit (HAL) -, the Probability of False Alarm (P_{FA}), and the Probability of Missed Detection (P_{MD}).

These dependencies are illustrated in **Figure 8**. If during normal operation (no failure) the Decision Variable appears to be larger than the threshold a False Alarm will occur. The Probability of False Alarm is represented by the integration of the right tail of the probability distribution function. The 'Non-Centrality' of the probability distribution during erroneous operations is a measure of the Horizontal Alarm Limit. Consequently, the Probability of Missed Detection is represented by the integration of the left tail of this probability distribution.

4.2.2   Parity and Least-Squares-Residuals Method

For the first group of algorithms - the Parity Method and the Least-Squares-Residuals Method - the Decision Variable is calculated from squared, Gaussian-distributed residuals. This allows the assumption of a χ^2 -Distribution of the test statistics. The Probability of False Alarm can consequently be expressed by the complementary probability function:

$$P_{FA} = Q\left(T/\sigma^2 \,|\, r\right) \qquad\qquad (4.14)$$

with P_{FA} Probability of False Alarm

       Q   Complementary Probability Function

       T   Threshold

       σ Standard Deviation

       r = n-4   Degrees of Freedom

       n   Number of Satellites

and $Q = 1 - P\left(\chi^2 \middle| r\right)$ (4.15)

with   *P* χ^2-Probability Function.

The central χ^2-Probability Function is defined as:

$$P = \left(\chi^2 \middle| r\right) = \left[2^{r/2} \cdot \Gamma\left(r/2\right)\right]^{-1} \int_0^{\chi^2} t^{r/2-1} \cdot e^{-r/2} dt$$ (4.16)

The Threshold T can be isolated from the Probability of False Alarm:

$$T = \sigma^2 Q^{-1}\left(P_{FA} \middle| r\right)$$ (4.17)

The Probability of Missed Detection can be expressed accordingly:

$$P_{MD} = P\left(T/\sigma^2 \middle| r, \lambda\right)$$ (4.18)

with λ Non-Centrality Parameter.

The non-central χ^2-Probability Function can be approximated by applying the '3-Moments-Approximation' of Pearson:

$$P\left(\chi^2 \middle| r, \lambda\right) \approx P\left(\chi^{*2} \middle| r^*\right)$$ (4.19)

with $\chi^{*2} = \dfrac{\chi^2 + c}{h}$ (4.20)

$$r^* = \frac{(r + 2\lambda)^3}{(r + 3\lambda)^2}$$ (4.21)

$$c = \frac{\lambda^2}{r + 3h}$$ (4.22)

$$h = \frac{r + 3\lambda}{r + 2\lambda}$$ (4.23)

The Non-Centrality Parameter has been derived in [STURZA/BROWN, 1990]:

$$\lambda = \frac{HAL^2}{\sigma^2} \frac{1}{\delta HDOP_{i}^2{}_{max}}$$ (4.24)

with HAL Horizontal Alarm Limit

$\delta HDOP_{i\ max}$ Increase in HDOP after exclusion of 'worst-case' satellite 'i'.

Finally the Threshold T can be eliminated by inserting equation 4.17 into 4.18:

$$P_{MD} = P\left[Q^{-1}(P_{FA}|r)|r,\lambda\right]$$ (4.25)

For a given set of parameters n, σ, HAL, P_{MD} and P_{FA}, this equation can be solved for $\delta HDOP_{i\ max}$.

4.2.2.1 RAIM Requirements

The Required Navigation Performance which had been established in Chapter 3 can be converted into RAIM requirements in terms of σ, HAL, P_{MD} and P_{FA} (**Table 5**) as required to solve equation 4.25 for $\delta HDOP_{i\ max}$ which is the key to predict whether RAIM is available. $\delta HDOP_{i\ max}$ determines the maximum allowable increase of the

	Departure	En-route	Terminal	Initial Approach	NPA
False Alarm Rate [h⁻¹]	10^{-5}	10^{-5}	10^{-5}	10^{-5}	10^{-5}
Probability of Missed Detection	$1 \cdot 10^{-3}$	$1 \cdot 10^{-3}$	$1 \cdot 10^{-3}$	$1 \cdot 10^{-3}$	$1 \cdot 10^{-3}$
Horizontal Alert Limit [m]	555	1850	1850	555	555
σ of Pseudorange Noise [m]	33.3	33.3	33.3	33.3	33.3

Table 5: RAIM Requirements

4. Theory of Autonomous Integrity Monitoring

HDOP after exclusion of the 'worst-case' satellite 'i'.

Figure 9 displays the $\delta HDOP_{i\ max}$ values as a function of the number of visible satellites and the RAIM requirements given in Table 5 for the different phases of flight.

4.2.2.2 *Availability of Failure Detection (FD)*

To predict whether it is possible to perform RAIM Failure Detection, the maximum value for $\delta HDOP_i$ needs to be determined for the actual satellite constellation by applying equation 4.9. If the calculated value is less than the $\delta HDOP_{i\ max}$ given in **Figure 9**, it can be predicted that RAIM Failure Detection is available.

4.2.2.3 *Availability of Failure Identification (FI)*

Following the confirmation that RAIM Failure Detection is available, the satellite constellation at hand needs to be checked whether the geometry is of sufficient quality to support the Failure Identification procedure. This is done in applying the procedure of verifying the availability of RAIM FD against the sub-set constellations. The $\delta HDOP_{i,j}$ values obtained again have to be less than the $\delta HDOP_{i\ max}$ given in Figure 9 to ensure the availability of RAIM FI.
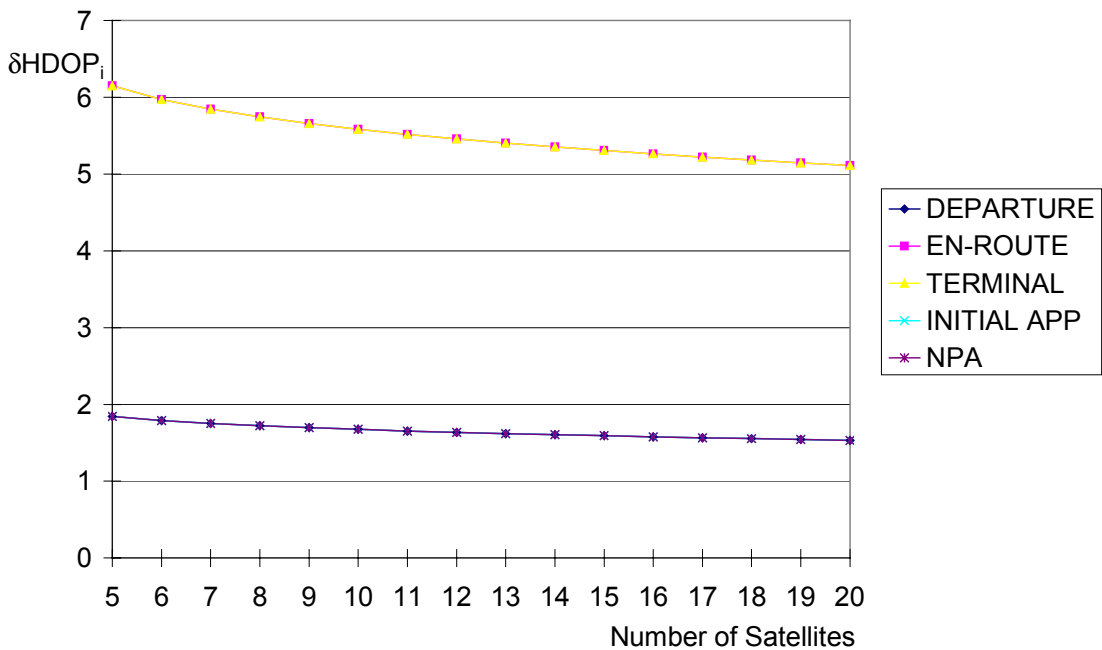
Figure 9: Geometrical Requirements for RAIM Availability (χ^2-Distribution)

4.2.2.4 *Failure Detection*

Equation 4.7 describes the linear transformation which projects the range measurement error vector $\underline{\varepsilon}$ into the resulting residual measurement error $\underline{\bar{z}}$. Assuming that the elements of $\underline{\varepsilon}$ are independent zero-mean Gaussian random variables with the same variance, then the sum of the squares of the elements of $\underline{\bar{z}}$ has an un-normalised χ^2-Distribution with n-4 degrees of freedom. The sum of squares is subsequently used as the Decision Variable for the test statistics (Section 4.2.1):

$$D = \underline{\bar{z}}^T \, \underline{\bar{z}} \tag{4.26}$$

   with   D   Decision Variable.

The decision variable can also directly be formulated through the linearised measurements:

$$D = \underline{z}^T \cdot \left[\underline{\underline{I}} - \underline{\underline{H}}\left(\underline{\underline{H}}^T \underline{\underline{H}} \right)^{-1} \underline{\underline{H}}^T \right] \cdot \underline{z} \tag{4.27}$$

Having formulated the Decision Variable, the RAIM algorithm can be implemented in two ways, either providing a constant false-alarm-rate (CFAR) or ensuring a constant probability of detection (CPOD) to check whether the Decision Variable exceeds the threshold and a fault has to be declared.

4.2.2.5 *Constant-False-Alarm-Rate (CFAR) Implementation*

By applying equation 4.17 the threshold T can be set to provide a constant probability of false alarm. This results in a probability of missed detection which varies with the geometry of the satellite constellation. The instantaneous probability of missed detection needs to be monitored to ensure that its requirement is met.

4.2.2.6 *Constant-Probability-Of-Detection (CPOD) Implementation*

For this implementation of the RAIM algorithms equation 4.18 can be inverted to provide for the calculation of the threshold T:

$$T = \sigma^2 P^{-1}\left(P_{MD}\middle| r, \lambda\right) \tag{4.28}$$

Therefore, T is calculated as a function of the satellite geometry providing a constant probability of missed detection and resulting in the probability of missed detection varying with the geometry.

4.2.2.7 *Failure Identification*

A maximum likelihood fault identification technique is described in [STURZA, 1991]. However, the Failure Identification function can also be implemented by applying the Failure Detection function to the sub-set constellations (see Section 4.2.2.4). The sub-set constellation, which does not lead to a detection of a failure does not include the faulty satellite and, therefore, the error source is identified.

4.2.3   Constant-Detection-Rate/Variable-Protection-Level Method

A different approach to determine the Decision Variable has been proposed by [BRENNER, 1990]. This algorithm is based on the parity space concept and uses orthogonal transformations to optimise the visibility of the error contributed by the individual satellite. These orthogonal transformations will preserve Gaussian properties of the test statistics. This simplifies the calculation of critical parameters such as thresholds, false alarm rates and detection probabilities and, therefore, avoids any χ^2-distributed functions.

In the observation function (4.3) all noise components are assumed to be normally distributed and mutually uncorrelated with zero mean. The equation contains redundant information that is disregarded in the formation of the least-square estimate. This information can be extracted by performing an orthogonal transformation of the observation equation (4.3). An (n x n) orthogonal matrix Q is characterised by the following property:

$$\underline{\underline{Q}} \cdot \underline{\underline{Q}}^T = \underline{\underline{Q}}^T \cdot \underline{\underline{Q}} = \underline{\underline{I}}_n \tag{4.29}$$

with Q n x n orthogonal matrix

         I_n n x n unity matrix.

The orthogonal matrix Q is used to transform the (n x 4) measurement matrix H to a matrix H_{TR} that contains zeros in rows 5 to n and an upper triangular (4 x 4) matrix H_{UTR} in rows 1 to 4. Equations 4.3 can be transformed into:

$$\begin{aligned} \underline{\underline{Q}} \cdot \underline{z} &= \underline{\underline{Q}} \cdot \underline{\underline{H}} \cdot \underline{x} + \underline{\underline{Q}} \cdot \underline{\varepsilon} \\ &= \underline{\underline{H}}_{TR} \cdot \underline{x} + \underline{\underline{Q}} \cdot \underline{\varepsilon} \end{aligned} .$$

(4.30)

and Q can be partitioned into a (4 x n) matrix Q_1 and a ((n-4) x n) matrix Q_2:

$$\begin{pmatrix} \underline{\underline{Q}}_1 \\ \underline{\underline{Q}}_2 \end{pmatrix} \cdot \underline{z} = \begin{pmatrix} \underline{\underline{H}}_{UTR} \\ \underline{\underline{0}} \end{pmatrix} \cdot \underline{x} + \begin{pmatrix} \underline{\underline{Q}}_1 \\ \underline{\underline{Q}}_2 \end{pmatrix} \cdot \underline{\varepsilon} .$$

(4.31)

This equation can be split horizontally into two parts, whereby the lower part yields:

$$\underline{\underline{Q}}_2 \cdot \underline{z} = \underline{\underline{Q}}_2 \cdot \underline{\varepsilon} .$$

(4.32)

The Decision Variable is defined through the following equation:

$$D = \underline{\underline{Q}}_2 \cdot \underline{\varepsilon} = \underline{\underline{Q}}_2 \cdot \left(\underline{v} + \underline{\varepsilon}_k \right)$$

(4.33)

with $\underline{v}$ n x 1 vector of measurement noise

       $\underline{\varepsilon}_k$ n x 1 vector of bias due to failure.

Since all the row vectors in Q are orthogonal unit vectors this must also be true for Q_2. The matrix Q_2 contains all available information concerning the redundancy of the residuals. In the case of only five (n=5) visible satellites Q_2 consists of a single row vector:

$$\underline{q}^T = \begin{pmatrix} \underline{\underline{Q}}_{2_{11}} & \underline{\underline{Q}}_{2_{12}} & \cdots \underline{\underline{Q}}_{2_{1n}} \end{pmatrix} .$$

(4.34)

The Decision Variable can be expressed as:

$$D = \underline{q}^T \cdot \underline{v} + \underline{q}^T \cdot \underline{\varepsilon}_k = \xi + q_k \cdot \varepsilon_k$$

(4.35)

with $\underline{\varepsilon}_k = \begin{pmatrix} 0 \\ \vdots \\ \varepsilon_k \\ \vdots \\ 0 \end{pmatrix}$ bias due to failure in satellite k

(4.36)

and ξ scalar containing the normally-distributed, zero-mean measurement noise.

When there are more than 5 satellites visible, the parity space will have a dimension greater than one and the matrix Q_2 will contain (n-4) orthogonal unit vectors similar to q. Only one unit vector is needed with a maximised coefficient for the satellite which is being monitored. A column vector of Q_2 defines the impact of a satellite error, which will have components in all (n-4) dimensions of the parity space. It is possible to choose a co-ordinate system in the parity space by orthogonal transformation in order that the initial column vector and, therefore the impact of the error, is along one axis only. This transformation will not influence the noise variance and will consequently amplify the visibility of the error.

The failure detection is again based on testing the Decision Variable against a threshold T, the criterion for a failure being:

$$|D| > T .$$
(4.37)

If no faulty satellite is received (Null-Hypothesis), equation 4.35 can be simplified to:

$$D = \xi$$
(4.38)

The Threshold T, which corresponds to a specified Probability of False Alarm, can be determined for a Gaussian-distributed decision variable by (see also equation 4.13):

$$\begin{aligned}
P_{FA} = P(|\xi| > T) &= \frac{2}{\sqrt{2\pi}\sigma} \int_{T}^{\infty} e^{-\frac{x^2}{2\sigma^2}} dx \\
&= \frac{2}{\sqrt{2\pi}} \int_{\frac{T}{\sigma}}^{\infty} e^{-\frac{y^2}{2}} dy
\end{aligned}$$
(4.39)

The Alternate-Hypothesis is valid if an error occurs in the kth satellite. The coefficient q_k determines how large the bias ε_k needs to be for the detection to occur, in this case the Detection Variable is again normally distributed but with the mean value $q_k\varepsilon_k$. The Probability of Missed Detection for a given error ε_k corresponds to those cases where D is brought below T by the noise:

$$\begin{aligned}
P_{MD} = P(|D| \leq T) &= \frac{1}{\sqrt{2\pi}\sigma} \int_{-\infty}^{T} e^{-\frac{(x-q_k\cdot\varepsilon_k)^2}{2\sigma^2}} dx \\
&= \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\frac{T-q_k\cdot\varepsilon_k}{\sigma}} e^{-\frac{y^2}{2}} dy
\end{aligned}$$
(4.40)

4.2.3.1 *RAIM Requirements*

The performance requirements established in Table 5 are applicable.

4.2.3.2 *Availability of Failure Detection (FD)*

The geometrical constraints for a satellite constellation to allow for RAIM FD can be calculated following a similar approach to that followed in Section 4.2.2. For a given set of parameters n, σ, HAL, P_{MD} and P_{FA} the equations (4.39) and (4.40) can be solved for $\delta HDOP_{i\,max}$ with:

$$q_k \cdot \varepsilon_k = \frac{HAL}{\delta HDOP_{i\,max}} \qquad (4.41)$$

Figure 10 shows the geometrical requirements in terms of $\delta HDOP_{i\,max}$ as a function of the number of visible satellites.

4.2.3.3 *Availability of Failure Identification (FI)*

The same procedure as explained in Section 4.2.2.3 needs to be applied to verify the
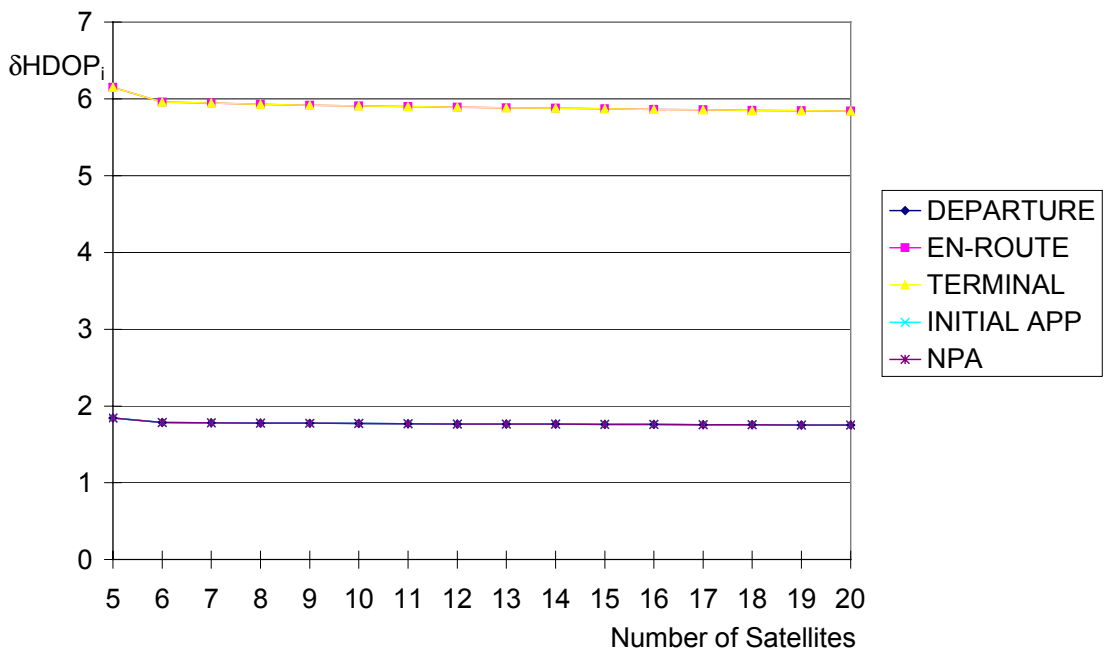
Figure 10: Geometrical Requirements for RAIM Availability (Normal-Distribution)

availability of RAIM FD in the sub-set constellations. The $\delta HDOP_{i,j}$ values obtained have again to be again less than the $\delta HDOP_{i\,max}$ given in Figure 10 to ensure the availability of RAIM FI.

4.2.3.4 *Failure Detection*

The RAIM algorithm proposed by [BRENNER, 1990] is implemented according to the Constant-False-Alarm-Rate (CFAR) method. Equation 4.39 needs to be inverted to calculate the Threshold T. If the Decision Variable D is larger than the Threshold T a failure has been detected. Subsequently, the Probability of Missed Detection P_{MD} can be calculated with equation 4.40 and checked against the requirements (Table 5) to confirm if the test has been carried out reliably.

4.2.3.5 *Failure Identification*

[BRENNER, 1990] implements the Failure Identification function by applying the Failure Detection function to the sub-set constellations (see Section 4.2.3.4). The sub-set constellation, which does not lead to a detection of a failure, does not include the faulty satellite and, therefore, the error source is identified.

4.3   AIDING BY BAROMETRIC MEASUREMENTS (BARO-AIDING)

In Section 4.2 it has been outlined that the performance of autonomous integrity monitoring is dependent on the degree of freedom provided by the number of measurements. In order to increase the degree of freedom, additional measurements are required. One possible source is the barometric altimeter. It provides altitude information derived from a barometric pressure measurement. This measurement can be considered as an additional range measurement, which originates from the centre of the Earth.

In [TSO-C129A, 1996] it is described how the measurement matrix $\underline{H}$ needs to be modified for baro-aiding and how the barometric altitude is required to be calibrated to ensure compatibility with range measurements from the satellites. [TSO-C129A, 1996] requires that calibration is only carried out when the maximum subset $VDOP_i$ is better or equal to 5; and calibrated altitude data shall only be utilised when RAIM cannot be provided by satellite range measurements alone as described in Section 4.2.

5.   FLIGHT TRIALS ONBOARD COMMERCIAL AIRLINERS

To serve the purposes of the required data evaluation activities, a data recording programme had been set up onboard of commercial airliners. A mix of different aircraft types had been selected to satisfy requirements of different operational scenarios and different onboard equipment.

To introduce a common data recording format an Interface Control Document [EUROCONTROL/

Figure 11: LUFTHANSA Airbus A340-300

ICD1, 1996] was established (see also Annex D). It describes in detail the raw measurements and computed data which have to be recorded from the satellite navigation sensors and the inertial sensors. Additional data from various other sensors are included to provide a comprehensive description of the aircraft status vector. It was decided, in view of future EGNOS activities, to include readings from available satellite communication (SatCom) equipment which would deliver indications about the reception conditions of geostationary satellites onboard these aircraft as additional sources for range measurements.

LUFTHANSA was identified as the initial partner to record data, because the German airline was taking delivery of some of the first commercial aircraft - Airbus A340's and A321's - to have GPS receivers already included in their standard avionics fit. The regular data recording onboard the LH A340-300 (**Figure 11**) commenced in April 1997. BRITISH AIRWAYS have subsequently equipped one of their Boeing B747-400 for data recording which entered operational status in September 1998.

Figure 12 presents the hardware set-up onboard the A340. All systems providing the required sensor data are connected to a dedicated Data Management Unit (DMU) via ARINC 429 data busses; the DMU then forwards the data to an Optical Quick Access Recorder (OQAR) via an ARINC 573 data bus. Data are obtained from the GPS Sensor Unit (GPSSU), the Inertial Reference System (IR), the Air Data Reference System (ADR), hybrid GPS/IRS (GPIRS), SatCom and diverse sensors (through the Data Monitoring Computer (DMC) and the Aircraft Condition Monitoring System (ACMS)).

A similar system configuration has been installed onboard the B747-400 which delivers data according to the same format [EUROCONTROL/ICD1, 1996] as that onboard the Airbus aircraft.
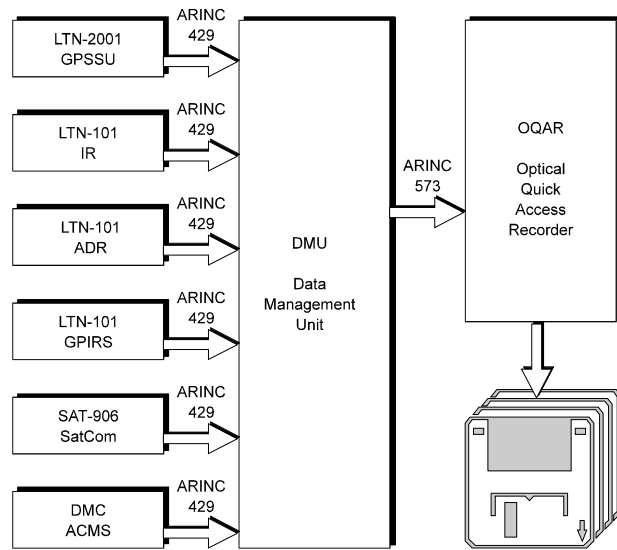
Figure 12: Aircraft Installation (A340/321)

6.   SOFTWARE DEVELOPMENT AND QUALITY ASSURANCE

It is evident that software which produces results for Safety Regulation purposes has to be of 'high quality'. The first section of this chapter defines what 'high quality' is, how quality requirements can be specified and which processes can be implemented to achieve them.

The second section explains how particular parts of this general approach have been applied to provide the evidence that the quality required of the developed data evaluation system has been successfully implemented. This is of vital importance because the results (Chapter 8) produced by the data evaluation system are intended to contribute to the approval of satellite navigation for use in civil aviation (Chapter 9).

6.1   GENERAL

6.1.1   'High Quality' Software

The results which will be presented in Chapter 8 and which will lead, subsequently, to the development of a Safety Argument in Chapter 9 have to be produced with tools of 'high quality' to be acceptable for Safety Regulation in order to approve safety-critical applications of Satellite Navigation. Therefore, it has to be established when these tools can be expected to be of 'high quality'.

Consequently, quality requirements have to be specified and evidence provided that the required level of quality has been met. [DEUTSCH & WILLIS, 1988] conclude that a software is of 'high quality' when it can be demonstrated that the relevant quality requirements have been achieved.

6.1.2   Specification of Quality Requirements

This section introduces a software quality model [DEUTSCH & WILLIS, 1988] which has been used as the basis for the development of the data evaluation system. This model is based on the fact that the user of the evaluation system and its data evaluation results will express his quality requirements clearly, for example in terms of 'Correctness', 'Reliability' and 'Verifiability'. However, the software engineer will encounter problems when relating these quality requirements from the user's point of view to the design and implementation of the data evaluation system. Therefore, the user is expected to express his quality requirements further, in terms of 'Quality

Factors' (Section 6.1.2.1) which have to be translated into 'Quality Criteria' (Section 6.1.2.2) to be understood from the software engineering point of view.

6.1.2.1 *Quality Factors*

The quality model requires the user to specify his quality requirements using the following Quality Factors:

1. *Correctness:*   extent to which the software design and implementation conform to the stated requirements;
2. *Efficiency:*   resources needed to provide the required functionality;
3. *Expandability:*   suitability of modifications (perfective aspects) during software maintenance;
4. *Flexibility:*   adaptive aspects of software maintenance;
5. *Integrity:*   security against either overt or covert access to programs and database;
6. *Interoperability:*   software is easy to be interfaced and produces or uses results that comply with agreed standards;
7. *Maintainability:*   suitability of issuing new software releases due to errors;
8. *Manageability:*   administrative aspects of modifications to the software;
9. *Portability:*   use on different operating systems and computers;
10. *Reliability:*   rate of failures in the software that render it unusable;
11. *Reusability:*   use of portions of the software for other applications;
12. *Safety:*   absence of unsafe software conditions, trust to be placed in the software;
13. *Survivability:*   continuity of reliable software execution with degraded functionality in presence of system failures;
14. *Usability:*   effort required to learn and the recurring effort to use the functionality of the software;
15. *Verifiability:*   suitability to verify that the software is working correctly.

6.1.2.2 *Quality Criteria*

The quality requirements, expressed as Quality Factors by the user, have to be transformed into the engineerable Quality Criteria for the design and implementation

of the data evaluation system to ensure that the user's requirements related to quality are met:

1. *Accuracy:*   achieving required precision in calculation and outputs.
2. *Anomaly Management:*   non-disruptive failure recovery;
3. *Augmentability:*   ease of expansion in functionality and data;
4. *Autonomy:*   degree of decoupling from execution environment;
5. *Commonality:*   use of standards to achieve interoperability;
6. *Completeness:*   all software is necessary and sufficient;
7. *Consistency:*   use of standards to achieve uniformity;
8. *Distributivity:*   geographical separation of functions and data;
9. *Document Quality:*   access to complete understandable information;
10. *Efficiency of Communications:* economic use of communication resources;
11. *Efficiency of Processing:* economic use of processing resources;
12. *Efficiency of Storage:* economic use of storage resources;
13. *Functional Scope:* range of applicability of a function;
14. *Generality:* range of applicability of a unit;
15. *Independence:* degree of decoupling from support environment;
16. *Modularity:* orderliness of design and implementation;
17. *Operability:* ease of operating the software;
18. *Safety Management:* software design to avoid hazards;
19. *Self-Descriptiveness:* understandability of design and source code;
20. *Simplicity:* straightforward implementation of functions;
21. *Support:* functionality supporting the management of changes;
22. *System Accessibility:* controlled access to software and data;
23. *System Compatibility:* ability of two or more systems to work in harmony;
24. *Traceability:* ease of relating code to requirements and vice versa;
25. *Training:* provisions to learn how to use the software;
26. *Virtuality:* logical implementation to represent physical components;
27. *Visibility:* insight into validity and progress of development.

Such a quality model allows the user to express and specify his requirements concerning the desired quality of the data evaluation system. **Table 6** displays the mapping between the user's Quality Factors and the engineerable Quality Criteria.

QUALITY FACTORS / QUALITY CRITERIA	Correctness	Efficiency	Expandability	Flexibility	Integrity	Interoperability	Maintainability	Manageability	Portability	Reliability	Reusability	Safety	Survivability	Usability	Verifiability
Accuracy										•		•			
Anomaly Management										•		•	•		
Augmentability			•												
Autonomy														•	
Commonality						•									
Completeness	•						•								
Consistency	•						•								
Distributivity												•	•		
Quality of Documentation								•			•				
Efficiency of Communication		•													
Efficiency of Processing		•													
Efficiency of Storage		•													
Functional Scope						•					•				
Generality			•	•							•				
Independence						•			•		•				
Modularity			•	•		•	•			•	•				•
Operability														•	
Safety Management												•			
Self-Descriptiveness			•	•			•		•		•				•
Simplicity			•	•			•			•	•				•
Support							•	•			•				•
System Accessibility					•										
System Compatibility						•									
Traceability	•						•								•
Training														•	
Virtuality			•												
Visibility							•								•

Table 6: Quality Factors and Criteria

6.1.3 Software Quality Engineering and Assurance

Once the quality requirements have been specified an approach needs to be implemented to ensure that the desired software quality is met. Today a number of techniques exist:

- independent verification and validation,

- audits,
- quality metrics,
- development methodologies,
- software quality evaluation tools,
- software quality standards,
- design and code inspections.

Software quality engineering is the combination of these different techniques and the decision-making to select the right mixture thereof with the aim to review-out defects and test-out errors. This is accompanied by software quality assurance, which is the monitoring process to ensure that all the software quality requirements are accomplished.

6.1.4   Software Development and Life-Cycle

To achieve the objectives of software quality engineering and quality assurance the software development is carried out following a life-cycle. The main purpose of a life-cycle is to provide a structure for the software development process [EUROCONTROL, 1992].

Figure 13 displays such a life-cycle, in this case a V-cycle, which includes Quality Assurance and Prototyping. The different phases, the associated documents and their purpose are the subject of the explanations in the following sections.
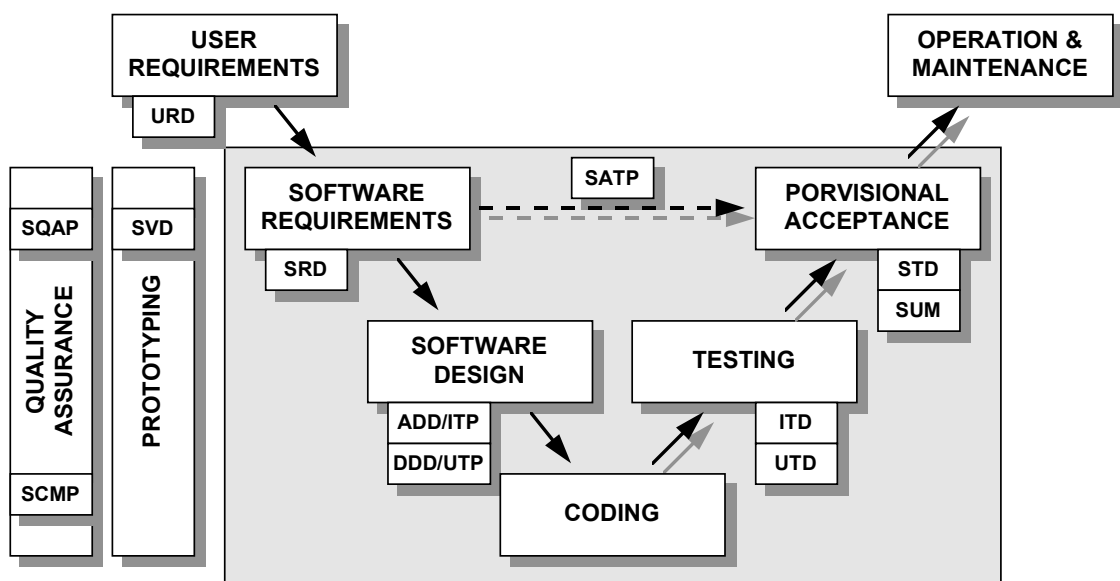
Figure 13: Software Life-Cycle

6.1.4.1 *User Requirements*

During this phase the future user of the system defines the functional and the quality (non-functional) requirements (Section 6.1.2) of the software. The main activities during this phase are:

- capture of user requirements,
- determination of operational environment,
- classification of degree of necessity,
- identification of relevant constraints,
- definition of acceptable performance and accuracy,
- description of Human-Computer Interaction (HCI) and
- feasibility studies.

The result of this phase is a User Requirements Document (URD), which should be written in the 'language' of the user to ensure that its contents can be verified and finally agreed by the user.

6.1.4.2 *Software Quality Assurance Plan*

All work done during the software development phase should be done in conformity with the Software Quality Assurance Plan (SQAP) to ensure that the quality requirements are fulfilled as stated in the User Requirements Document. The SQAP covers and describes, in particular:

- the choice of tools and methods for software development and quality assurance,
- the choice of the programming languages,
- the relevant coding standards,
- the quality metrics,
- the inspection and check of software code and documentation,
- the production of a Software Configuration Management Plan (SCMP).

The SQAP describes the means whereby evidence is provided that the software quality attributes required of the software to be developed will be successfully implemented.

6.1.4.3 *Prototyping*

In order to ensure that the data evaluation software will meet the user requirements the software development is accompanied by prototyping activities. The objective of prototyping is the implementation of core modules to prove the general system concept and to carry out early validation and verification of the system. These developments will provide the basis to refine unstable user requirements before the formal process of transformation into software requirements is concluded. This process is documented in a System Validation Document (SVD).

6.1.4.4 *Software Development*

Software Requirements Definition

The primary activity of this phase is to specify the software requirements including the construction of a logical model of the system. A software engineering tool may be chosen to provide a method for the communication between the user and the software developer to translate the User Requirements Document into the Software Requirements Document (SRD). The contents of the SRD should cover the following essential points:

- capability requirements,
- performance requirements,
- interface requirements,
- operational requirements,
- resource requirements,
- quality requirements.

The secondary activity of this phase is the production of the first issue of the Software Acceptance Test Plan (SATP), which will be the major input for the Provisional Acceptance phase.

Software Architectural Design

The aim of the Architectural Design Phase is to define the software architecture of the system down to the design entities. During this phase the transition is established from the requirements domain to the solution domain by performing the following activities:

- construction of the physical model,

- specifying the architectural design,
- reviewing the design,
- defining the integration test techniques to be used.

Major outputs of this phase are the Architectural Design Document (ADD), a traceability matrix, showing how the software requirements are achieved, and the Integration Test Plan (ITP).

Software Detailed Design

During the Detailed Design Phase the algorithms should be described which are to be used for each major operation of the previously described design entities. This phase is structured along the following activities:

- refining the design,
- detailing the description of the processing logic and the data structures,
- preparing the design for implementation,
- reviewing the detailed design,
- defining the unit test strategy,
- detailing the software acceptance test activities.

The major outputs of this phase are the Detailed Design Document (DDD), the Unit Test Plan (UTP) and the second issue of the SATP.

Coding

When the design of each design entity is complete, reviewed and approved, the entities can be coded. Output of this phase is the commented code which has been established following the coding standards as defined in the SQAP. From the coding phase onwards the code it is recommended that the code always be placed always under the version control as documented in the SCMP.

Unit Testing

This phase consists of the execution of the test procedures described in the UTP and the evaluation of the test results. Testing at this level is to assess the correct internal operation of the entities. The results should be documented in the Unit Test Document (UTD). This document together with the unit tested code are the output of this phase.

Integration Testing

The integration tests defined in the ITP should be executed during this phase, their results evaluated and documented in the Integration Test Document (ITD). Testing at this level should demonstrate that the design entities interface correctly after having been integrated into the complete system. The ITD, the internally tested code, the Software User Manual (SUM) and the final issue of the SATP are the deliverables of this phase. After successful completion of this phase the code should be considered

S/W Life-Cycle Phase	Major Inputs	Major Activities	Major Outputs (Deliverables)	Major Milestones
User Requirements Definition		Identification of user requirements	URD	URD approved
Software Requirements Definition	URD	Identification of software requirements. Construction of a logical model.	SRD SATP (I)	SRD approved SATP (I) approved
Prototyping	URD Test data	Proof of system concept. Early system validation.	SVD Verified algorithms. Experimental system prototype. Data evaluation results.	SVD approved
Architectural Design	SRD SVD	Design of software architecture. Construction of a physical model.	ADD ITP	ADD approved
Hardware Specification	URD SRD ADD	Development of hardware specifications for operational system.	HSD	Hardware procurement
Software Detailed Design	ADD	Module design.	DDD UTP SATP (II)	SATP (II) approved
Coding	ADD DDD	Coding.	Code	Code approved
Unit Testing	SUTP Untested code	Unit testing.	UTD Unit tested code	
Integration Testing	SITP Unit tested code	Integration of units and testing.	ITD SUM SATP(III) 'Internally tested code'	SUM delivered SATP delivered
Provisional Acceptance	SUM SATP (III) Internally tested code	Provisional acceptance tests.	STD Provisionally accepted software.	STD delivered. Software provisionally accepted. SUM approved.
System Preparation for Operation	SUM STD Provisionally accepted software SATP (III)	Period of operational use. Final acceptance test.	Complete software system including documentation.	Final acceptance

Table 7: Software Life-Cycle

ready for Provisional Acceptance.

<u>Provisional Acceptance</u>

In this phase the software is tested for acceptance and checked for correspondence with the User Requirements Document (URD) and the Software Requirements Document (SRD). The tests which have to be performed are laid down in the Software Acceptance Test Document (SATP). When all acceptance tests have been successfully completed, the software can be provisionally accepted. An additional activity during this phase is the evaluation of the Software User Manual (SUM). The output from this phase is the Software Transfer Document which records the results of the acceptance test and defines the remaining actions to be concluded before the software can finally be accepted.

The major inputs, activities, outputs and milestones of the different phases of the software life-cycle are summarised in **Table 7**.

6.2   DEVELOPMENT OF THE DATA EVALUATION TOOL

The life-cycle process which has been developed in Section 6.1 provides the basis for the development process of the data evaluation tool from the software engineering point-of-view. The initial step is the definition of the functional requirements from the user's point-of-view which leads to the establishment of the User Requirements Document (URD) described in Section 6.2.1. The non-functional requirements result in the definition of the Quality Model (Section 6.2.2) which includes the transformation of the users' quality requirements (factors) into engineerable quality attributes (criteria). Subsequently, quality metrics are defined (Section 6.2.3) to demonstrate that the quality requirements have been achieved.

6.2.1   Development of the User Requirements

The functional requirements for the data evaluation tool are defined in the User Requirements Document [EUROCONTROL/URD, 1997]. This document is structured along the data flow through the subsequent processing steps, the database organisation and the data evaluation. Its basic ideas were discussed at an early stage with a number of European Civil Aviation Authorities and Safety Regulators to ensure the acceptability of the results when available. The detailed data evaluation process is explained in Chapter 7.

6.2.2 Development of the Quality Model

The non-functional requirements are formulated through the implementation of the Quality Model as described in Section 6.1.2. **Table 8** displays the weighting ('+' = high, '±' = medium, '−' = low) of importance which has been assigned to the Quality Criteria in context of the Quality Factors.

The Quality Factors and Criteria allow a separation of non-functional requirements

QUALITY FACTORS / QUALITY CRITERIA	Correctness	Efficiency	Expandability	Flexibility	Integrity	Interoperability	Maintainability	Manageability	Portability	Reliability	Reusability	Safety	Survivability	Usability	Verifiability
Accuracy										+	⊕				
Anomaly Management										−	−	−			
Augmentability			+												
Autonomy													−		
Commonality						±									
Completeness	+						+								
Consistency	+						+								
Distributivity												−	−		
Quality of Documentation							+				±				
Efficiency of Communication		−													
Efficiency of Processing		+													
Efficiency of Storage		±													
Functional Scope						−					±				
Generality			−	−							±				
Independence						−			−		±				
Modularity			+	−		−	+	−			±				⊕
Operability														⊕	
Safety Management												−			
Self-Descriptiveness			+	−			+	−			±				⊕
Simplicity			+	−			+			⊕	±				⊕
Support								+	−		±				+
System Accessibility					+										
System Compatibility						±									
Traceability	⊕						+!								⊕
Training														±	
Virtuality			−												
Visibility							+								+

Table 8: Ranking of Quality Factors and Criteria for Data Evaluation Software

describing the system operation from those describing the derivation of the data evaluation results. The following paragraphs concentrate on a sub-set of the latter non-functional requirements, which have been weighted to be of high importance ('⊕'), because of their importance in the development of the Safety Argument.

The URD formulates functional requirements which are defined to ensure that the data evaluation process in support of the Safety Argument can be established. It is required that the software design and implementation conforms with the stated functional requirements (*Correctness*). Therefore, it is important that the code is traceable (*Traceability*) to the requirements and vice versa.

This requirement has to be seen in conjunction with the required *Reliability* of the software in terms of *Simplicity*, defining the straightforward implementation of functions.

The next important Quality Factor is *Safety* which requires the absence of unsafe failure conditions and leads to trust being placed in the software. In this context *Accuracy* is the important Quality Criterion to ensure that calculations and outputs are achieved with the required precision.

The description of the functionality of the data evaluation tool in Chapter 7 reveals the high number of parameters and different conditions which define and influence the scenarios under which the individual results are produced. To exclude or at least to minimise operator errors it is required that the system is easy to use (*Usability*), described by the ease of operating the software (*Operability*).

The most important non-functional requirement is expressed by the Quality Factor *Verifiability*, which expresses how easy it is to verify that the software is working correctly. In the frame of the Safety Argument the orderliness of the design and implementation (*Modularity*) together with the understandability of design and source code (*Self-Descriptiveness*) will play an important role to justify that the results have been produced by correctly working software. To support this argument the Quality Criteria *Simplicity* and *Traceability* will again be of importance.

The non-functional requirements together with the Software Quality Assurance Plan (SQAP) have been presented to a number of European Safety Regulators who endorsed the proposed implementation of the Quality Model as pre-condition for any successful Safety Regulatory activity.

6.2.3 Definition of Quality Metrics

The Quality Model for the data evaluation software has been developed in the preceding section by transforming the important non-functional user requirements (Quality Factors) into engineerable Quality Criteria.

The Quality Criteria which are identified as being of importance to the development of the data evaluation software are:

1. *Accuracy*,
2. *Modularity*,
3. *Operability*,
4. *Self-Descriptiveness*,
5. *Simplicity*,
6. *Traceability*.

The following sections explain which techniques (Section 6.1.3) are applied to provide evidence about the successful achievement of the Quality Criteria.

Accuracy

Independently developed programs are used to verify the calculation results at different stages of the data evaluation process. All tests are defined and executed independently from the software development. In all cases where no cross-check with existing software is possible, test results are calculated 'by hand' for verification. In addition plausibility checks are carried out between different parameters. These activities are supported during design and testing by using prototype installations of individual functions to conduct Unit Testing before Integration Testing (Section 6.1.4.4).

Modularity

The achievement of this requirement is ensured during the design by the consequent application of the development standards defined by the software life-cycle (Section 6.1.4.4). The main objective in this context is the decomposition of the system into components during the architectural and detailed design.

As part of the Unit Test activities a commercial analysis tool LOGISCOPE™ is used which is widely recognised in industry for the development of safety-critical software. The tool analyses the source code *inter alia* with respect to:

- the number of GOTO-statements (*UNCOND_JUMP*), which is an indicator for the program's testability,
- the number of entries into a function (*N_IN*) and return statements (*N_OUT*), the applied software coding standards recommend that a function should only have one entry and one exit point and
- the number of auxiliary exits (*P_NODES*), which is again an indicator of the program's testability.

Operability

This requirement is addressed by the design of the human-machine interfaces, which is implemented in window technology, intuitive menus and sub-menus, the display of all relevant information and automated summary print-outs of control parameters. During testing all functions are checked for successful rejection of wrong inputs. The development of a detailed and unambiguous User Manual is a contributing factor to achieve user-friendliness and prevent the user from introducing errors through operation of the data evaluation program.

Self-Descriptiveness

To ensure that this requirement is achieved, rigorous code inspections are carried out. During an independent process the functions, in particular those described in Chapter 4, are transformed into block- or flow-diagrams. These diagrams are checked for their correct translation and implementation in the code. In addition the tool LOGISCOPE™ is used to analyse:

- the number of statements in a function (*N_STMTS*),
- the number of blocks of comments (*N_COM*) to calculate the frequency of comments and
- the number of blocks of comments per statement (*COM_R = N_COM / N_STMTS*). This is used as an indicator of the effort undertaken by the developer to describe the implemented function.

Simplicity

This requirement is addressed during the design by consequent application of the development standards (Section 6.1.4.4). As with *Modularity*, the decomposition of the system into components during the architectural and detailed design is of importance. The achievement is checked by inspection of the source code. In addition LOGISCOPE™ is used to identify:

- the number of independent paths in a connected graph - based on graph theory - in order to quantify the complexity of a resulting control structure,
- the number of GOTO-statements (*UNCOND_JUMP*),
- the number of control structures nesting in a function (*MAX_LVLS*) to calculate the maximum number of nested levels and
- the number of non-cyclic execution paths (*N_PATHS*), this metric indicating the number of test cases required to fully test the function.

As explained above the metrics defined for *Modularity*, *Self-Descriptiveness* and *Simplicity* are calculated by LOGISCOPE™. Ranges of acceptable values (thresholds) are defined for the individual metrics. The calculated values and the acceptable ranges are provided numerically and graphically for every measured module and in summary for all measured modules. The results are finally classified as follows:

1. Perfect: module fulfils the concerned Quality Criterion perfectly,
2. Accepted: module can be accepted,
3. Reconstruct: module must be corrected,
4. Rewrite: module must be rewritten.

Traceability

The achievements in terms of *Maintainability* and *Simplicity* contribute considerably to fulfil the requirement that code should be easily related to requirements and *vice versa*. The Software Acceptance Test activities are defined in such a way that the program is tested against every individual User Requirement to ensure their complete implementation and full traceability through the system until presentation of the evaluation results.

6.2.4 Implementation of the Software Life-Cycle

Following the definition of the User Requirements and the development of the Quality Model together with the associated quality metrics, the software life-cycle is implemented as displayed in Figure 13 and summarised in Table 7 to provide the structure for the software development process.

Particular use is made of prototypes, which are used in this case for early validation to ensure that the data recording processes onboard the airliners are correctly implemented. Individual functions of the data evaluation procedures are implemented to deliver evidence of their correct functioning as part of the Unit Test activities. The

major objective of these prototypes is to generate confidence in the system development and the subsequent data evaluation results from an early stage.

The data evaluation system was provisionally accepted after successful conclusion of all test activities and the demonstration that all functional and non-functional requirements were achieved.

7.   DATA EVALUATION

7.1   GENERAL

This chapter describes in detail the data evaluation tool, which was developed to achieve the objectives of the data analyses (Section 1.3).

The processing core of this tool was developed around an ORACLE™ database system that contains the RNP values and recorded data specified in Chapters 3 and 5, respectively. The software life-cycle and quality assurance procedures described in Chapter 6 were applied in order to provide a tool in which the required level of confidence could be placed in its results.

The actual processing core of the tool allows a user to access the data contained in the database for evaluation purposes; the core also comprises the implementation of the theory of autonomous integrity monitoring as described in Chapter 4.

7.2   DESCRIPTION OF DATA EVALUATION TOOL

7.2.1   Database System

The data recorded onto the optical discs onboard the aircraft were prepared for loading into the ORACLE™ database system by a series of steps comprising conversion into engineering units, formatting and quality control. Following this preparation, the data were loaded into the relevant tables of the database. Using the standard set of RNP values (Table 5) the data evaluation process was started at the end of which the evaluation results were translated into statistics for each flight. Subsequently, individual flight statistics were combined to derive global statistics based on all flights.

The following sections introduce the process, which has been developed to evaluate the system performance in three different satellite visibility scenarios. It is explained in detail how Accuracy, Integrity, Availability and Continuity of Service Qualifiers have been defined, how they have been realised by implementing the theory described in Chapter 4 and how the results are presented.

7.2.2 Visibility Scenarios

The Accuracy, Integrity, Availability and Continuity of Service Qualifiers describing the performance of the satellite navigation system are dependent on the relative geometry between the aircraft antenna and the satellite constellation as described by (i) the aircraft position and attitude and (ii) the satellite elevations and azimuths. In this context it is understood that Availability is given if, and only if, the Accuracy and Integrity Qualifiers both meet their relevant requirements.

The Qualifiers are determined for three visibility scenarios:

1. <u>Theoretical visibility:</u> All selected GPS satellites are taken into consideration, in order to establish whether or not they would be theoretically visible from the aircraft's position (which is considered to be a point in space).

2. <u>Theoretical dynamic visibility:</u> The same information as above is generated, but an aircraft and antenna model and the measured aircraft attitude are taken into consideration to determine theoretical signal reception.

3. <u>Measured visibility:</u> Satellites are only considered visible when related status bits or available range measurements indicate the successful signal reception in the airborne environment.

The satellite navigation system performance within these three visibility scenarios has been investigated in order to obtain information about the combined influence of aircraft dynamics and the real operational environment on the quality of reception of satellite navigation signals.

The database was used to assess whether these qualifiers met the required navigation performance for Accuracy, Integrity and Availability for different phases of flight. Availability performance along continuous flight tracks was checked to establish whether this Qualifier met the Continuity of Service requirement.

7.2.3 Aircraft and Antenna Model

The evaluation of the influence of the dynamics of the aircraft on the overall system performance - using the second 'theoretical dynamic' visibility scenario - requires the development of a reception model. This model has been derived from the geometry of the aircraft structure, the installation position and the reception diagram of the GPS
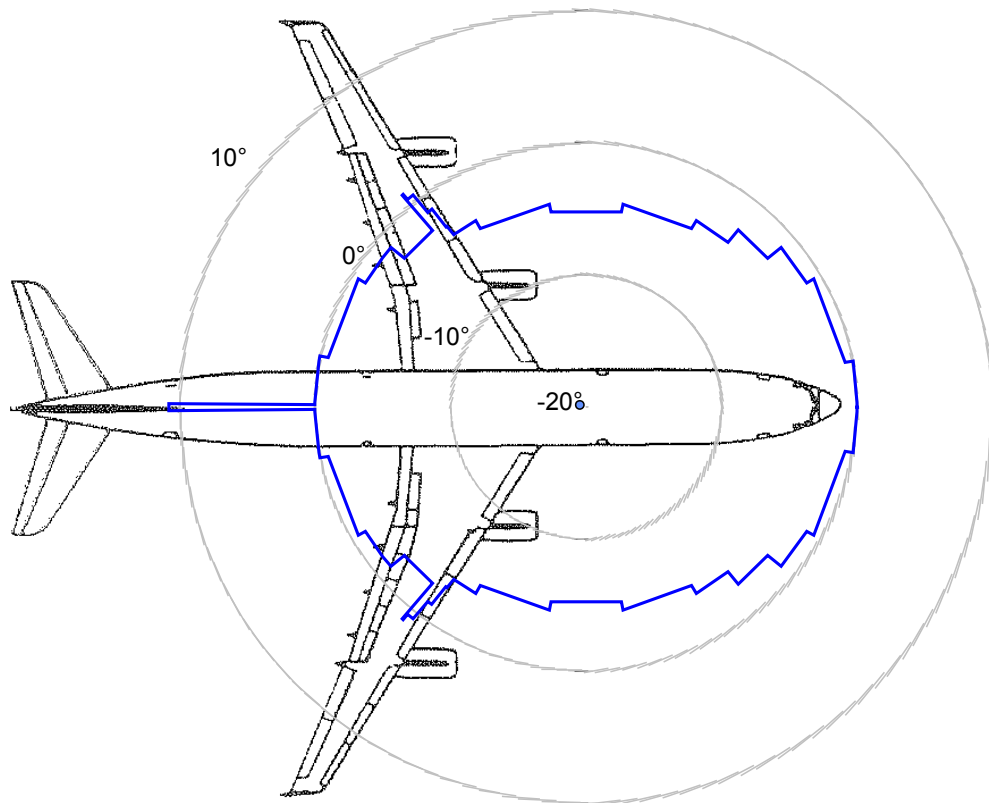
Figure 14: Geometric Aircraft and Antenna Reception Diagram for the Airbus A340-300

antenna. **Figure 14** displays the geometric mask angles for a 360° panoramic view centred over the GPS antenna position on the top of the aircraft fuselage. Obstruction by the fuselage, winglets and the vertical stabiliser can clearly be identified. The minimum elevation angle of –5° is the result of the reception diagram of the antenna. However, extensive investigations of the recorded measurements revealed that satellites were received below the masking area displayed in Figure 14 [LIPP, ET.AL., 1999].

7.2.4   Phases of Flight

In order to apply the RNP requirements for different phases of flight, all flights - when loaded into the database - were automatically split into phases of flight using the rules summarised in **Table 9**. The right-hand column of this table indicates how many samples with a sampling rate of 1 Hz are included in the database (representing a total of almost 900 flight hours).

A total of 330 samples have been excluded from the data evaluation due to recording problems identified by the quality control procedures carried out before loading the data into the database. These procedures apply plausibility checks to the raw data

Phase of Flight	Rule		Number of Samples
Ground	Groundspeed	< 100 Kn.	not investigated
Departure	Groundspeed Altitude	> 100 Kn. < 11.000 ft	48 168
En Route	Altitude	> 11.000 ft	2 865 522
Terminal	Altitude Distance to Airport	< 11.000 ft > 4.000 ft > 28.000 m	47 627
Initial Approach	Altitude Distance to Airport	> 2.500 ft < 28.000 m > 14.000 m	14 341
Final Approach (NPA)	Altitude Distance to Airport Groundspeed	< 2.500 m < 14.000 m > 100 Kn.	18 442

Table 9: Definition of Phases of Flight

concerning their possible physical range and change versus time, their resolution and the consistency between measurements of different sensors. Those data samples that had been identified by the quality control procedures as being erroneous were manually checked and subsequently marked in the database. The data remain in the database for traceability but they are not included in the statistical evaluation. This manual part of the procedure ensures that data are only excluded for known reasons related to the recording equipment and not related to failures of the measurement equipment.

7.2.5   Flights included in the Database

The database used for the data evaluation herein comprises 100 intercontinental flights of a LUFTHANSA Airbus A340-300 aircraft representing a total of almost 900 flight hours collected from 14th April 1997 to 12th June 1997. This represents the data

Number of Flights	Between
6	Frankfurt / FRA - Atlanta / ATL
4	Frankfurt / FRA - Bangkok / BKK
15	Frankfurt / FRA - Boston / BOS
8	Frankfurt / FRA - Dallas/Ft. Worth / DFW
8	Frankfurt / FRA - Madras / MAA
25	Frankfurt / FRA - New York / JFK
10	Frankfurt / FRA - Osaka / KIX
2	Frankfurt / FRA - Rio de Janeiro / GIG
8	Frankfurt / FRA - Sao Paolo / GRU
1	Frankfurt / FRA - Düsseldorf / DUS
2	Dallas/Ft. Worth / DFW - New York / JFK
4	Dallas/Ft. Worth / DFW - Houston / IAH
2	Dallas/Ft. Worth / DFW - New Orleans / MSY
5	Düsseldorf / DUS - New York / JFK

Table 10: Itineraries of Flights in the Database
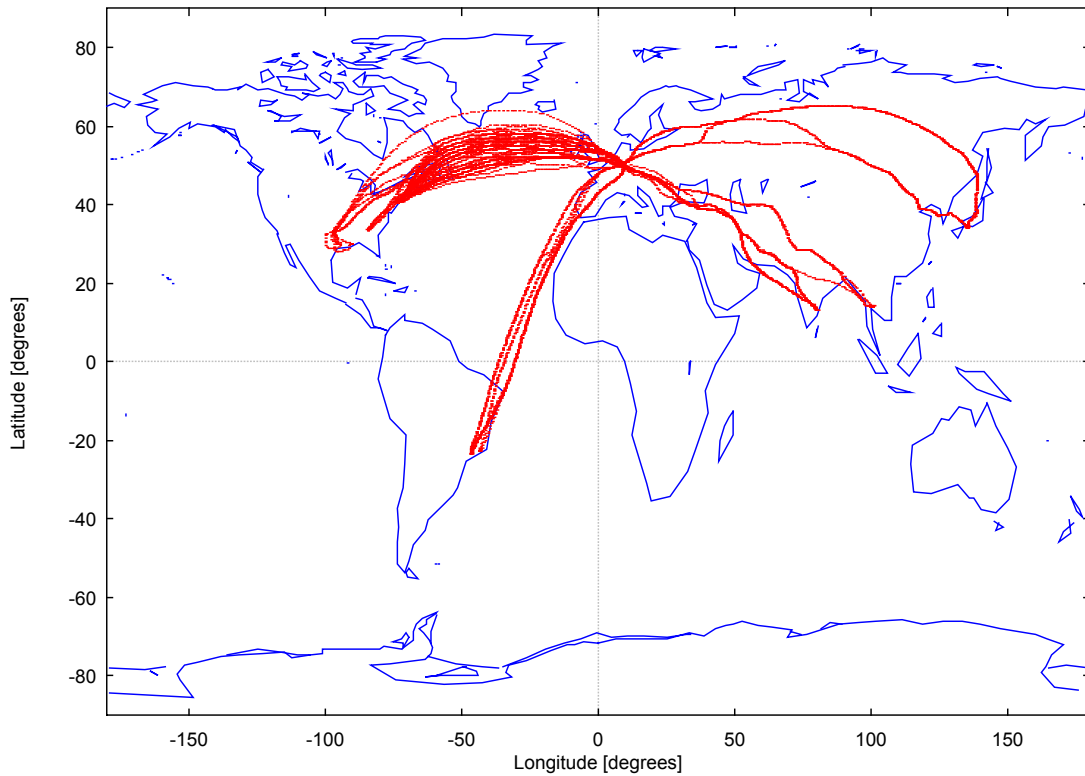
Figure 15: Trajectories of Flights in the Database

collected during the first two month of operational data recording onboard the A340. **Figure 15** displays the trajectories of these flights and **Table 10** summarises their itineraries.

7.2.6 Accuracy

To define the Accuracy Qualifier a concept was adopted which had been proposed in [STURZA/BROWN, 1990]. The maximum horizontal and vertical position errors are estimated from the expected measurement noise (Table 5) and the geometry of the current satellite constellation defined in equation 4.8.

$$ACC_{hor} = 2 \cdot \sigma \cdot HDOP \tag{7.1}$$

       with ACC_{hor} estimated horizontal position error.

These estimated position errors are compared against the requirements defined in Section 3.2.1 in order to decide if the required system performance can be achieved. These calculations are solely dependent on the combined influence of the geometry of the local constellation and the range error and can be derived either from an empirical model or using actual measurement data.
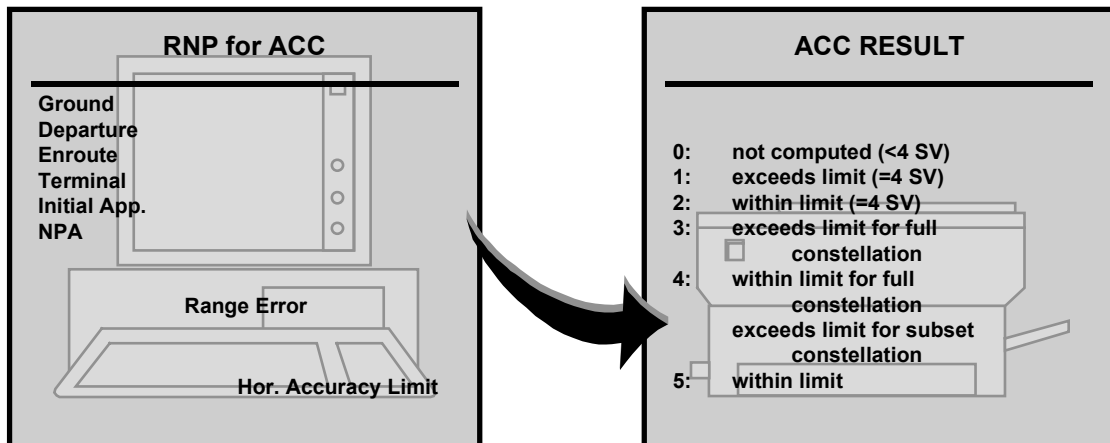
Figure 16: Accuracy Evaluation

On the left hand-side of **Figure 16** the input parameters which describe the Required Navigation Performance for the different phases of flight related to Accuracy are shown. The results of the evaluation are classified into six different result classes as given in Figure 16.

The accuracy requirements are considered as being fulfilled – at least without redundancy - if the result is within classes 2, 4 or 5. If, in the case of a detected faulty satellite, the requirements have still to be fulfilled by a remaining sub-set of satellites, only a result in class 5 fulfils the requirements.

7.2.7   Availability of RAIM Failure Detection and Identification

The initial step to evaluate the performance of the RAIM algorithms is to decide whether RAIM Failure Detection and Identification can be carried out depending on the geometric constellation of the visible satellites.

The RAIM Detection and Identification procedure requires - as introduced in Sections 4.2.2.2, 4.2.2.3, 4.2.3.2 and 4.2.3.3 - sufficiently performant sub-sets of satellites. The performance of the resulting sub-sets has been described by the decrease in quality of the satellite constellations' Horizontal Dilutions of Precision $\delta HDOP_i$ and $\delta HDOP_{i,j}$, as one and two satellites at a time are sequentially excluded from the set of visible satellites. The maximum allowable limit of this geometric deterioration - that is, when the 'worst case' satellite or pair of satellites is excluded - is calculated from the mathematical formulation in Section 4.2 and applying the requirements summarised in Table 5.

Figure 17 describes how the RAIM FDI Availability results are presented. Six result classes have been defined for the RAIM Availability Qualifier, class (2) representing the case where the current geometry of the satellite constellation is sufficient to start
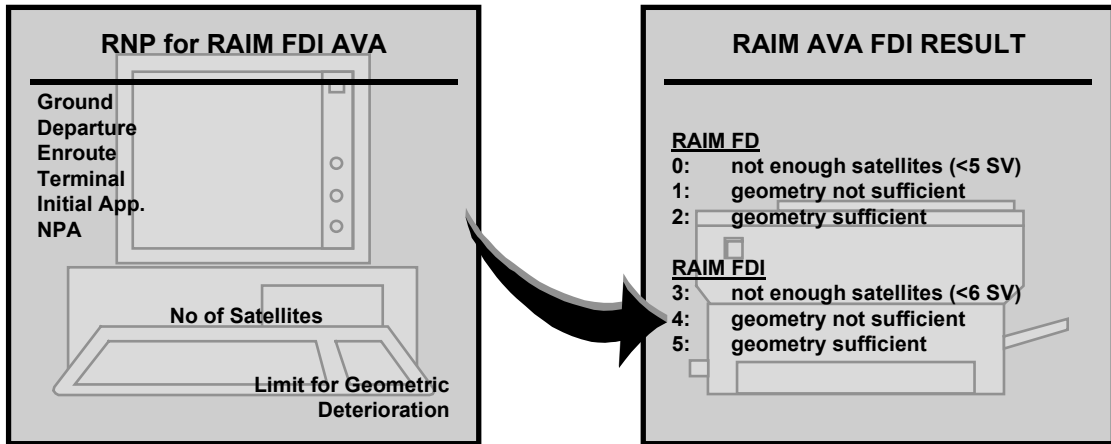
Figure 17: RAIM FDI Availability

a reliable RAIM Detection procedure. In other words, all necessary pre-conditions have been met for the RAIM algorithm to detect that a single satellite has failed. If the evaluation result falls into class (5), then the geometry is still sufficient for identifying which satellite is erroneous.

By applying an assumption to the range error, the calculation of the Accuracy and RAIM FDI Availability Qualifiers can be carried out based on the relative constellation of visible satellites with respect to the aircraft. This process is comparable to a pre-flight prediction of the positioning performance.

7.2.8 RAIM Failure Detection and Identification Algorithms

After RAIM Availability has been declared valid using the measured data, the performance of the RAIM algorithms can be investigated.

The Required Navigation Performance with respect to RAIM FDI is described by those input parameters given in **Figure 18**, which were discussed in Chapter 3 and
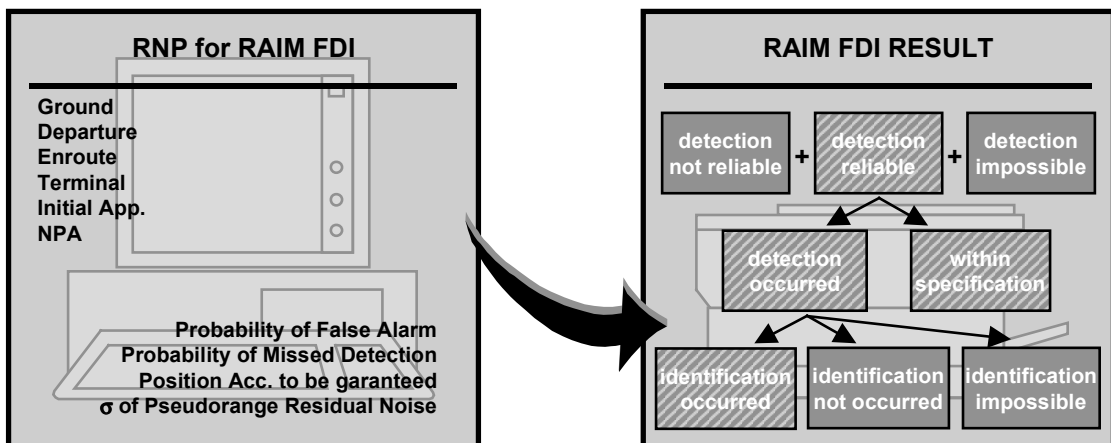
Figure 18: RAIM Detection and Identification

were summarised in Table 5.

Results for RAIM FDI have been classified in accordance with the scheme depicted in Figure 18. The three main result classes are:

- detection of a faulty satellite not reliable (0),
- detection reliable (1), and
- detection impossible (2).

Class (1) is split into:

- detection occurred (3) and
- everything within specification (4).

If detection occurred in the case of class (3) the evaluation continues with the identification process, which tries to identify which satellite is faulty. There are three possible results:

- identification of the faulty satellite occurred (5),
- identification not occurred (6) and
- identification impossible (7).

The navigation performance requirements for RAIM Detection are fulfilled in the case of class (1) - detection reliable. Requirements are met for RAIM Detection and Identification for the combination of class (1) and class (5) - identification of the faulty satellite successfully occurred.

7.2.9 Baro-Aiding

In cases where RAIM FDI was declared as unavailable (Section 7.2.7) or unreliable (Section 7.2.8) baro-aiding has been added as described in Section 4.3 in order to establish whether the additional measurement would improve the RAIM performance.

7.2.10 Availability

The Availability of the navigation service is assessed against the definition in Section 3.2.3. In practical terms Availability will be declared when the Accuracy requirement is fulfilled (Accuracy available) and when RAIM Failure Detection is set to available.

7.2.11 Continuity of Service

In order to describe the Continuity of Service all outages of the Availability of the navigation service will be checked, in order to determine whether the total amount of time that outage occurred exceeds the Total Outage Duration as described in Section 3.3.

7.2.12 GNSS Error Simulator

To validate the correct functioning of the FDI algorithms and to investigate their performance a GNSS error simulator is used. This simulator allows the creation of specific fault scenarios by modelling errors onto the measured receiver raw data as recorded onboard of the aircraft. This is of particular interest to test the Identification function, because satellite errors are not known *a priori* and a reference is required against which the algorithms' behaviour can be judged.

The simulator, which has been developed for these purposes, allows the specification of different types of errors (peaks, ramps and steps) for the pseudorange measurement. It also features the possibility of modelling the correlated errors for the other receiver raw measurements such as range-rate and delta-range (see ANNEX D - Onboard Data Recording- Table 21).

8. RESULTS

8.1 SYSTEM PERFORMANCE

8.1.1 Availability of Accuracy

Table 11 presents the availability of the GPS position accuracy for the three visibility scenarios and the different phases of flight. The results are based on the accuracy qualifier definition presented in Section 7.2.6. For all visibility scenarios and during all phases of flight down to Non-Precision Approach the required accuracy (Table 3) is available.

Accuracy Measured (min elev. >0°)	Departure	En Route	Terminal	Initial App.	Final App. (NPA)
Number of Samples (in sec)	48183	2866663	47849	14349	18371
Available	100	100	100	100	100
Available with redundancy	98.59701554	99.98608138	99.96656147	99.72820406	99.98911328
Not computed (<4SV)	0	0	0	0	0
Exceeds limits (=4SV)	0	0	0	0	0
Within limits (=4SV)	0	0	0	0	0
Exceeds limits (full const.)	0	0	0	0	0
Within limit (full const.) & Exceeds limits (subset)	1.40298446	0.01391862	0.03343853	0.27179594	0.01088672
Accuracy Theoretical Dynamic (>0°)	**Departure**	**En Route**	**Terminal**	**Initial App.**	**Final App. (NPA)**
Available	100	100	100	100	100
Available with redundancy	99.41888218	100	99.92476332	99.86061746	100
Not computed (<4SV)	0	0	0	0	0
Exceeds limits (=4SV)	0	0	0	0	0
Within limits (=4SV)	0	0	0	0	0
Exceeds limits (full const.)	0	0	0	0	0
Within limit (full const.) & Exceeds limits (subset)	0.58111782	0	0.07523668	0.13938254	0
Accuracy Theoretical (min elev. >0°)	**Departure**	**En Route**	**Terminal**	**Initial App.**	**Final App. (NPA)**
Available	100	100	100	100	100
Available with redundancy	100	100	100	100	100
Not computed (<4SV)	0	0	0	0	0
Exceeds limits (=4SV)	0	0	0	0	0
Within limits (=4SV)	0	0	0	0	0
Exceeds limits (full const.)	0	0	0	0	0
Within limit (full const.) & Exceeds limits (subset)	0	0	0	0	0

Table 11: Availability of Accuracy (Percentage of Time)[4]

---

[4] Results are given with a maximum number of decimal places, subsequent discussions consider the most significant numbers.

In addition, results are derived to describe when accuracy is still available although the worst-case satellite - whose exclusion would have the worst impact on the results - is excluded from the constellation. No effect can be observed for the theoretical scenario. Therefore, if the information transmitted by the worst case satellite would have been identified as faulty and excluded from the available measurement sources the required accuracy could still be provided by the remaining satellites. Slight decreases of performance can be observed for the theoretical dynamic and measured visibility scenarios due to the combined effect of manoeuvring of the aircraft coupled with the limitation of the onboard receiver to 8 reception channels. These occurrences are subject to further investigations in Section 8.1.4. In that section, outages with respect to the availability of RAIM Detection are analysed and it can be assumed that availability outages of accuracy and RAIM Detection outages are caused by similar effects.

The main observation, that the required accuracy is available for all visibility scenarios and during all phases of flight, reduces the need to investigate the Availability of the navigation service (7.2.10) and therefore concentrate on examining the availability of the integrity function.

8.1.2 Predicted Availability of RAIM Detection & Identification

Table 12 presents the results for the predicted availability of RAIM Detection and Identification during the 900 flight hours loaded into the database. The main observations are:

- No situation occurred where RAIM Detection was not available due to the fact that less than five satellites were predicted to be visible.
- Predicted RAIM Detection was always available during the Departure, En-route and Terminal phases of flight in the theoretical visibility scenario. Outages occur during the Initial and Final Approach phases, when requirements are most stringent.
- Outages in RAIM Detection availability occur for the scenarios of measured and theoretical dynamic visibility. These outages are further analysed in Section 8.1.4. In the theoretical dynamic visibility scenario outages are mainly caused by the receiver losing sight of satellites during aircraft manoeuvres. The performance degrades form the theoretical dynamic to the measured scenario because of the receiver being limited to eight reception channels, whereas the theoretical dynamic scenario considers an all-in-view receiver.
- The availability of the RAIM Detection and Identification capability is dramatically less than for RAIM Detection only, because now a minimum of six satellites

(instead of five for Detection) is required and the geometric constellations of the sub-sets of five satellites have each to fulfil the Detection requirements. This decrease in performance is particularly evident for Departure, Initial and Final Approach, where the requirements are most stringent.

- A high degree of correlation can be observed between the results for two types of algorithms. This, on one hand, validates that their behaviour and performance is highly comparable; on the other hand, it verifies the correct implementation of the algorithms.

RAIM Availability Measured (min elev. >0°)	Departure	En Route	Terminal	Initial App.	Final App. (NPA)
Number of Samples (in sec)	48183	2866663	47849	14349	18371
Detection					
Sturza-Brown					
Available	93.06186829	99.88341846	99.89968442	95.90215346	97.48516684
Not possible (<5SV)	0	0	0	0	0
Not possible (geometry)	6.93813171	0.11658154	0.10031558	4.09784654	2.51483316
Brenner					
Available	93.18431812	99.88861614	99.89968442	96.02062861	97.60492080
Not possible (<5SV)	0	0	0	0	0
Not possible (geometry)	6.81568188	0.11138386	0.10031558	3.97937139	2.39507920
Detection and Identification					
Sturza-Brown					
Available	14.33700683	95.13612169	95.30397709	25.20733152	23.79293452
Not possible (<6SV)	0.08716767	0.01179071	0.03343853	0	0
Not possible (geometry)	85.57582550	4.85208760	4.66258438	74.79266848	76.20706548
Brenner					
Available	16.83581346	95.21349388	95.26008903	27.65349502	29.04033531
Not possible (<6SV)	0.08716767	0.01179071	0.03343852	0	0
Not possible (geometry)	83.07701887	4.77471541	4.70647245	72.34650498	70.95966469

RAIM Availability Theoretical Dynamic (>0°)	Departure	En Route	Terminal	Initial App.	Final App. (NPA)
Detection					
Sturza-Brown					
Available	93.64506154	99.99856977	99.86833581	97.97198411	98.25812422
Not possible (<5SV)	0	0	0	0	0
Not possible (geometry)	6.35493846	0.00143023	0.13166419	2.02801589	1.74187578
Brenner					
Available	93.85675446	99.99856977	99.86624590	98.09742839	98.25812422
Not possible (<5SV)	0	0	0	0	0
Not possible (geometry)	6.14324554	0.00143023	0.13375410	1.90257161	1.74187578
Detection and Identification					
Sturza-Brown					
Available	45.82944192	99.14656868	98.03339673	55.19548401	61.09629307
Not possible (<6SV)	0.04358384	0.00174419	0.10658530	0	0
Not possible (geometry)	54.12697424	0.85168713	1.86001797	44.80451599	38.90370693
Brenner					
Available	47.93806944	99.16261521	98.02921691	57.13290125	65.30945512
Not possible (<6SV)	0.04358384	0.00174419	0.10658530	0	0
Not possible (geometry)	52.01834672	0.83564060	1.86419779	42.86709875	34.69054488

RAIM Availability Theoretical (min elev. >0°)	Departure	En Route	Terminal	Initial App.	Final App. (NPA)
Detection					
Sturza-Brown					
Available	100	100	100	99.75608056	99.03108160
Not possible (<5SV)	0	0	0	0	0
Not possible (geometry)	0	0	0	0.24391944	0.96891840
Brenner					
Available	100	100	100	99.75608056	99.03108160
Not possible (<5SV)	0	0	0	0	0
Not possible (geometry)	0	0	0	0.24391944	0.96891840
Detection and Identification					
Sturza-Brown					
Available	71.42353112	99.59356925	100	65.88612447	65.71770726
Not possible (<6SV)	0	0	0	0	0
Not possible (geometry)	28.57646888	0.40643075	0	34.11387553	34.28229274
Brenner					
Available	72.84934520	99.60288321	100	67.32873371	69.17968537
Not possible (<6SV)	0	0	0	0	0
Not possible (geometry)	27.15065480	0.39711679	0	32.67126629	30.82031463

Table 12: Predicted Availability of RAIM FDI (Percentage of Time)

8. Results

Baro-aided RAIM Availability Measured (min elev. >0°)	Departure	En Route	Terminal	Initial App.	Final App. (NPA)
Number of Samples (in sec)	48183	2866663	47849	14349	18371
Detection					
Sturza-Brown					
Available	98.15910176	99.99323255	100	98.68980417	98.99842143
Not possible (<5SV)	0	0	0	0	0
Not possible (geometry)	1.84089824	0.00676745	0	1.31019583	1.00157857
Brenner					
Available	98.44135899	99.99323255	100	98.68980417	98.99842143
Not possible (<5SV)	0	0	0	0	0
Not possible (geometry)	1.55864101	0.00676745	0	1.31019583	1.00157857
Detection and Identification					
Sturza-Brown					
Available	56.62578088	99.51406915	98.49108654	66.03944526	71.12296554
Not possible (<6SV)	0	0	0	0	0
Not possible (geometry)	43.37421912	0.48593085	1.50891346	33.96055474	28.87703446
Brenner					
Available	59.48363531	99.54455756	98.49108654	69.08495366	74.90610201
Not possible (<6SV)	0	0	0	0	0
Not possible (geometry)	40.51636469	0.45544244	1.50891346	30.91504634	25.09389799

Baro-aided RAIM Availability Theoretical Dynamic (>0°)	Departure	En Route	Terminal	Initial App.	Final App. (NPA)
Detection					
Sturza-Brown					
Available	99.11794616	100	99.98119083	99.86758659	100
Not possible (<5SV)	0	0	0	0	0
Not possible (geometry)	0.88205384	0	0.01880917	0.13241341	0
Brenner					
Available	99.30680946	100	99.98119083	99.87455572	100
Not possible (<5SV)	0	0	0	0	0
Not possible (geometry)	0.69319054	0	0.01880917	0.12544428	0
Detection and Identification					
Sturza-Brown					
Available	75.06589461	99.94031388	99.50887166	84.33340302	91.70431659
Not possible (<6SV)	0	0	0	0	0
Not possible (geometry)	24.93410539	0.05968612	0.49112834	15.66659698	8.29568341
Brenner					
Available	76.99811137	99.94149993	99.50887166	86.86319604	94.45321431
Not possible (<6SV)	0	0	0	0	0
Not possible (geometry)	23.00188863	0.05850007	0.49112834	13.13680396	5.54678569

Baro-aided RAIM Availability Theoretical (min elev. >0°)	Departure	En Route	Terminal	Initial App.	Final App. (NPA)
Detection					
Sturza-Brown					
Available	100	100	100	100	100
Not possible (<5SV)	0	0	0	0	0
Not possible (geometry)	0	0	0	0	0
Brenner					
Available	100	100	100	100	100
Not possible (<5SV)	0	0	0	0	0
Not possible (geometry)	0	0	0	0	0
Detection and Identification					
Sturza-Brown					
Available	92.58037067	99.99309301	100	94.67558715	93.76190735
Not possible (<6SV)	0	0	0	0	0
Not possible (geometry)	7.41962933	0.00690699	0	5.32441285	6.23809265
Brenner					
Available	94.28429114	99.99309301	100	96.10425814	96.54346524
Not possible (<6SV)	0	0	0	0	0
Not possible (geometry)	5.71570886	0.00690699	0	3.89574186	3.45653476

Table 13: Predicted Availability of Baro-aided RAIM FDI (Percentage of Time)

75

Table 13 presents the results for the predicted availability of RAIM Detection and Identification when aiding by barometric measurements is introduced as described in Sections 4.3 and 7.2.9. The main observations are:

- RAIM Detection is always available during all phases of flight in the theoretical visibility scenario. No outages occur any more during the Initial and Final Approach phases.
- Outages in RAIM Detection availability are reduced but still occur for the scenarios of measured and theoretical dynamic visibility caused by the same reasons as described above. However, for the theoretical dynamic scenario RAIM Detection availability reaches almost 100% during all phases of flight.
- During the terminal phase of flight (theoretical dynamic scenario) RAIM Detection is not available for 9 seconds out of 47849, while 100% RAIM Detection availability is achieved for the measured scenario. This particular case can be explained by differences between the modelled and real signal reception conditions (see Section 7.2.3).
- The availability of the RAIM Detection and Identification capability is considerably improved by baro-aiding. However, performance is still limited for Departure, Initial and Final Approach, where the requirements are more stringent.
- Again a high degree of correlation can be observed between the two types of algorithms.

8.1.3   RAIM FDI Algorithms

Table 14 summarises the performance of the RAIM algorithms using the real measurement data with respect to the availability of reliable detection capabilities.

The most important observation resulting from these investigations is that when detection was declared reliable detection did never occur and no faulty satellite signal was identified. To validate the correct implementation of the algorithms and to ensure the correctness of the statement that at no time during the 900 flight hours a satellite error occurred, the GNSS error simulator (see Section 7.2.12) has been used and the relevant results are described in Section 8.1.6.

The actual performance of the algorithms correlates very well with what was predicted. The performance of the baro-aided algorithms remains, in general, somewhat lower than predicted. This is due to unavailability of the baro-aiding during particular flight periods when calibration of the barometric sensor output is carried out at the same time as RAIM Detection becomes unreliable.

RAIM Algorithm Results	Departure	En Route	Terminal	Initial App.	Final App. (NPA)
Number of Samples (in sec)	48168	2865522	47627	14341	18442
Sturza-Brown					
Detection reliable	93.16973925	99.90752121	99.93071157	95.91381354	97.54365036
Everything within spec.	93.16973925	99.90752121	99.93071157	95.91381354	97.54365036
Detection occurred	0	0	0	0	0
Detection not reliable	6.83026075	0.09247879	0.06928843	4.08618646	2.45634964
Detection impossible	0	0	0	0	0
Brenner					
Detection reliable	93.50813818	99.91101098	99.92651227	96.12300397	97.60329682
Everything within spec.	93.50813818	99.91101098	99.92651227	96.12300397	97.60329682
Detection occurred	0	0	0	0	0
Detection not reliable	6.49186182	0.08898902	0.07348773	3.87699603	2.39670318
Detection impossible	0	0	0	0	0
*Sturza-Brown +**Baro***					
Detection reliable	97.72047833	99.99605656	100	97.82441950	97.99371001
Everything within spec.	97.72047833	99.99605656	100	97.82441950	97.99371001
Detection occurred	0	0	0	0	0
Detection not reliable	2.27952167	0.00394344	0	2.17558050	2.00628999
Detection impossible	0	0	0	0	0
*Brenner + **Baro***					
Detection reliable	97.90940043	99.99713839	100	98.96799386	97.99371001
Everything within spec.	97.90940043	99.99713839	100	97.81047347	97.99371001
Detection occurred	0	0	0	0	0
Detection not reliable	2.09059957	0.00467629	0	2.18952653	2.00628999
Detection impossible	0	0	0	0	0

Table 14: Availability of reliable RAIM Detection (Percentage of Time)

8.1.4 Analyses of Outages

The detailed analyses of those occurrences where Detection capabilities of the RAIM Algorithms were unreliable revealed that they can be classified into three different categories:

A. <u>RAIM Detection unreliable due to the receiver being limited to 8 reception-channels:</u> In this category, RAIM Detection has been identified as being unreliable due to the fact that the LH A340-300 onboard receiver hardware is limited to 8 reception channels. The receiver-dependent choice of 8 satellites out of potentially more than 8 visible satellites is not optimal for RAIM Detection purposes since the receiver was designed for supplemental means only, according to TSO C-129 C3. Furthermore, a satellite may become unusable due to shadowing, which limits the receiver - at least for several tens of seconds - to 7 or less satellites, although there may still be satellites visible which the receiver is not able to track. The effects of this category on RAIM Detection unavailability are therefore rather a design issue of onboard receivers than one of GPS limitations. Cases belonging to this class are no longer expected to occur for an all-in-view receiver architecture.

| Phase of Flight | total / shortest / longest outage in sec / Number of outages | | Outage Category Sturza/Brown / Brenner in sec | | |
	Sturza/Brown CFAR	Brenner CFAR	A	B	C
Unaided RAIM					
Departure	3290 / 1 / 523 / 46	3127 / 1 / 495 / 47	2824/2607	156/156	310/364
En route	2650 / 3 / 376 / 43	2550 / 3 / 380 / 47	1070/1045	376/380	1204/1125
Terminal	33 / 14 / 19 / 2	36 / 17 / 19 / 2	33/36	0/0	0/0
Initial App.	586 / 1 / 97 / 19	609 / 1 / 97 / 18	336/336	143/167	107/106
Final App.(NPA)	453 / 4 / 179 / 14	442 / 4 / 179 / 13	348/348	0/0	105/94
Total	**7012**	**6764**	**4611/4372**	**675/703**	**1726/1689**
Baro-aided RAIM					
Departure	1098 / 2 / 523 / 13	1007 / 2 / 495 / 12	1055/964	23/23	20/20
En route	113 / 21 / 40 / 4	134 / 21 / 40 / 5	43/43	0/0	70/91
Terminal	0 / - / - / -	0 / - / - / -	0/0	0/0	0/0
Initial App.	312 / 4 / 97 / 7	368 / 4 / 97 / 8	131/163	113/137	68/68
Final App.(NPA)	370 / 78 / 168 / 3	370 / 68 / 178 / 3	302/302	0/0	68/68
Total	**1893**	**1879**	**1531/1472**	**136/160**	**226/247**

Table 15: Outage Duration in RAIM Detection Reliability and Outage Categories

B. <u>RAIM Detection unreliable due to insufficient geometry of the satellite constellation</u>: The receiver uses all available satellites but loses lock on a signal due to manoeuvring of the aircraft, or the requirements during a particular phase of flight cannot be met by the geometry of the satellite constellation. RAIM Detection reliability cannot, therefore, be maintained. These cases would also occur with an all-in-view receiver architecture.

C. <u>Other Cases:</u>
Intermittent loss of satellite tracking: This failure condition appears only in data from 1997 and parts of 1998 before the receiver manufacturer upgraded the existing software to solve what was identified to be a receiver problem.

Table 15 summarises the total outage times, and the shortest and longest outage durations for the different algorithms, and the percentage of the outages belonging to the three different outage classes.

8.1.5 Result Compensation

If the presented statistics are compensated for Outage Category C (expected not to occur anymore for recordings from late 1998 onwards) and assuming that the receiver could be exchanged for an all-in-view receiver (eliminate Outage Category A), the results of the data analysis would be as shown in **Table 16**.

RAIM Detection would be declared reliable for 100% during Terminal and Final Approach for the 100 flights. Detection would also be reliable with 99.67613%,

RAIM Algorithm Results (Detection reliable)	Departure	En Route	Terminal	Initial App.	Final App. (NPA)
Sturza-Brown	99.67613353	99.98687848	100	99.00285894	100
Brenner	99.67613353	99.98673889	100	98.83550659	100
*Sturza-Brown +**Baro***	99.95225046	100	100	99.21204937	100
*Brenner + **Baro***	99.95225046	100	100	99.04469702	100

Table 16: Availability of reliable RAIM Detection (Percentage of Time) - Compensated

99.98674% and 98.83551% for Departure, En-route and Initial Approach, respectively (Sturza/Brown).

The reliability for baro-aided RAIM Detection would lead to the following improvements: 100% during En-route and 99.95225% and 99.04470% for Departure and Initial Approach.

8.1.6   Availability and Continuity of Service

The main observation made in Section 8.1 was that the required accuracy is available for all visibility scenarios and during all phases of flight. This reduces the need to investigate the Availability of the navigation service (7.2.10) in favour of the Availability of the Integrity (RAIM Failure Detection) function. All outages were evaluated whether they exceeded the maximum allowable outage duration as defined in Table 4. In total, nine outages for Sturza/Brown and eight for Brenner were identified, of which 8 and 7 respectively are due to the receiver being limited to eight reception channels. Only one case exists where the total allowable outage duration of 300 seconds is exceeded during an en route phase of flight. This occurs when seven satellites are visible but with insufficient geometric distribution to allow for RAIM Failure Detection. This problem is immediately solved when using the algorithms in their baro-aided implementation.

8.1.7   Results of GNSS Error Simulations

The results of Section 8.1.3 clearly show that during the 900 flight hours under investigation no detection of any satellite fault has been indicated by the algorithms. This leads to the question: were the algorithms capable of detecting any fault if it had occurred? This question cannot be answered based on the information contained in the recorded data because there is no reference available to identify any satellite faults *a priori*.
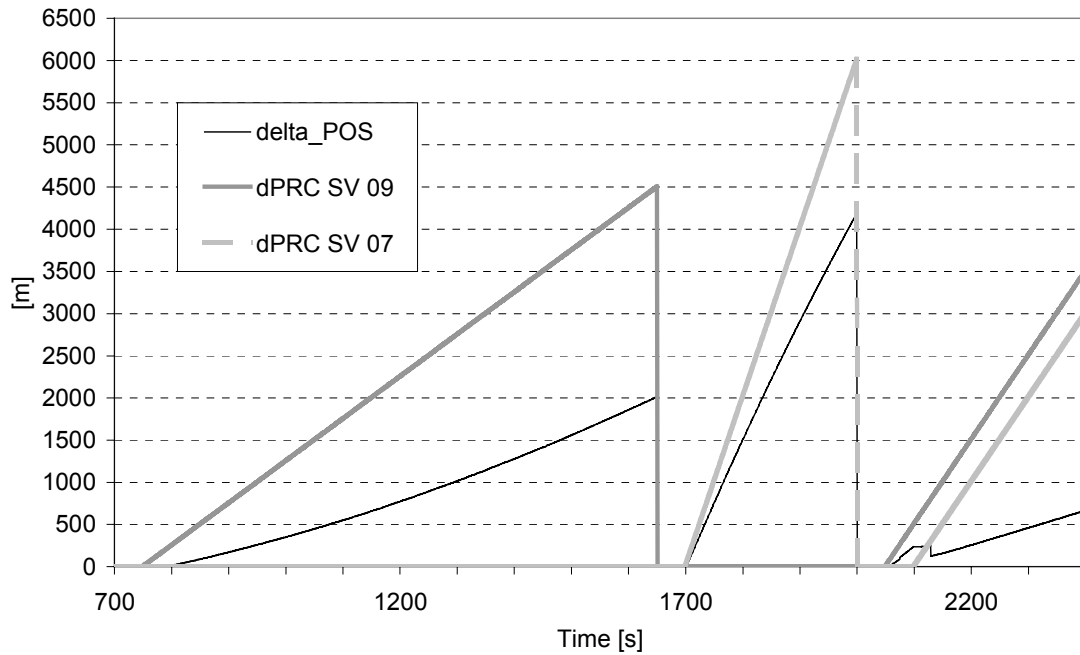
Figure 19: Simulated Pseudorange Errors and Resulting Position Error

Therefore, the GNSS error simulator described in Section 7.2.12 is used to simulate a number of error scenarios and to investigate the behaviour of the two algorithms.

Data from a short flight during the en-route and terminal phases of flight have been selected for this error simulation. **Figure 19** displays the three error scenarios:

1. A ramp is simulated on the pseudorange of one satellite (SV 09) with a gradient of 5 ms^{-1} during 900 s.

2. A ramp of 20 ms^{-1} is added to the measurement of another satellite (SV 07) during 300s.

3. The third scenario consists of ramps of 10 ms^{-1} modelled on both satellites' measurements in parallel, one ramp (SV 07) starting 50s later than the ramp for the second satellite (SV 09). This scenario was created to investigate what would happen in the unlikely event of a double satellite error.

Figure 19 shows the simulated ramps and the resulting position error (delta_POS), which occurs if the faulty information is included in the positioning calculation.

Figure 20 displays the results obtained for the Sturza-Brown algorithm:
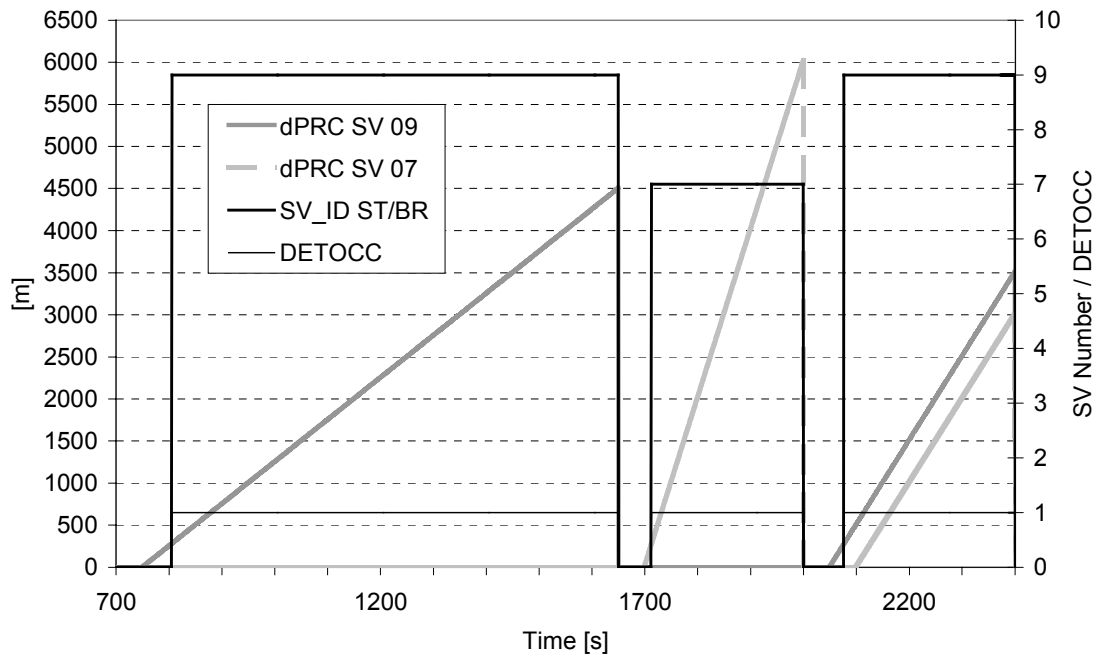
Figure 20: Failure Detection and Satellite Identification (Sturza-Brown)

1. In the first scenario it requires 56 s until detection occurs (DETOCC = 1). The position error has increased to 20.75 m by then. The 'faulty' satellite SV 09 is identified instantaneously.

2. In the second scenario it takes only 13 s until detection occurs and the 'faulty' satellite is correctly identified. At this time the position error amounts to 179.28 m.

3. The third scenario requires 27 s until detection occurs and SV 09 is identified as being faulty. The position error is 116.60 m at this time. The satellite is identified before the ramp of the second satellite starts. SV 09 remains identified throughout the error simulation.

Figure 21 describes the performance of Brenner's algorithm when exposed to the simulated faults. In each case, detection occurs earlier than when using Sturza-Brown. In the first scenario, detection occurs three seconds before Sturza-Brown and in the second and third scenarios, one second earlier. However, identification does not take place immediately:

1. In the first scenario it takes 91 s from the start of the ramp until the correct 'faulty' satellite is identified (38 s after detection); the position error is 73.74 m.
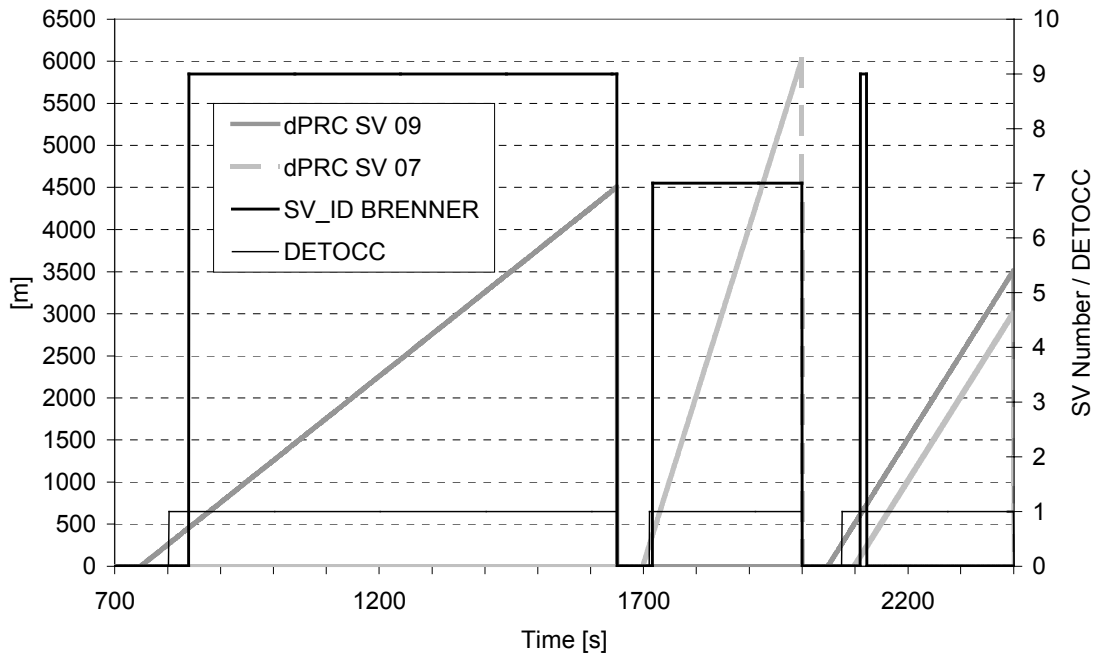
Figure 21: Failure Detection and Satellite Identification (Brenner)

2. In the second scenario identification occurs 18 s into the fault (6 s after detection). The position error at this time is 256.88 m.

3. For the third scenario detection occurs 26 s after the ramp commenced (position error 110.53 m). Detection remains signalled throughout the simulated double satellite error. Identification of the first satellite requires 61 s which is already 11 s into the ramp simulated on the second satellite. However, 12 s later the algorithm is no longer capable of deciding whether it can identify the fault or not and sets the flag identification to 'impossible'.

The 'early warning' capabilities of the algorithms demonstrate that the Horizontal Alert Limit is never exceeded and, therefore, any alarm would be raised within the specified Time-to-Alarm (Table 4).

The results obtained in this section using the GNSS error simulator provide the evidence for the correct functioning of the algorithm when errors may occur onboard the satellites leading subsequently to erroneous range measurements in the satellite receiver. It has even been demonstrated that the algorithms can handle double satellite errors, although with different results.

8.1.8   Representative Data and Saturation of Statistical Results

This section discusses in how far the data recorded during the almost 900 flight hours (Section 7.2.5) can be assumed as being representative to provide a basis for a fundamental set for the statistical results.

Figure 22 displays the HDOP averaged over 24 hours of one day during the flight trial period. The calculations were done for one-minute time increments and a resolution of one degree in latitude and longitude. The altitude was fixed to the Earth's surface (0 meters) and a two degree mask angle was applied.

The white lines represent the flight trajectories as already presented in Figure 15.

It can be seen that the included flights cover the entire spectrum of the HDOP distribution over the Earth. However, most of the data were collected during flights crossing the North Atlantic region, where the average HDOP appears to be higher compared to other regions of the Earth. Consequently, the obtained results can be judged as being conservative and, therefore, on the safe side.

Another aspect to be looked at is the influence caused by the fact that during the
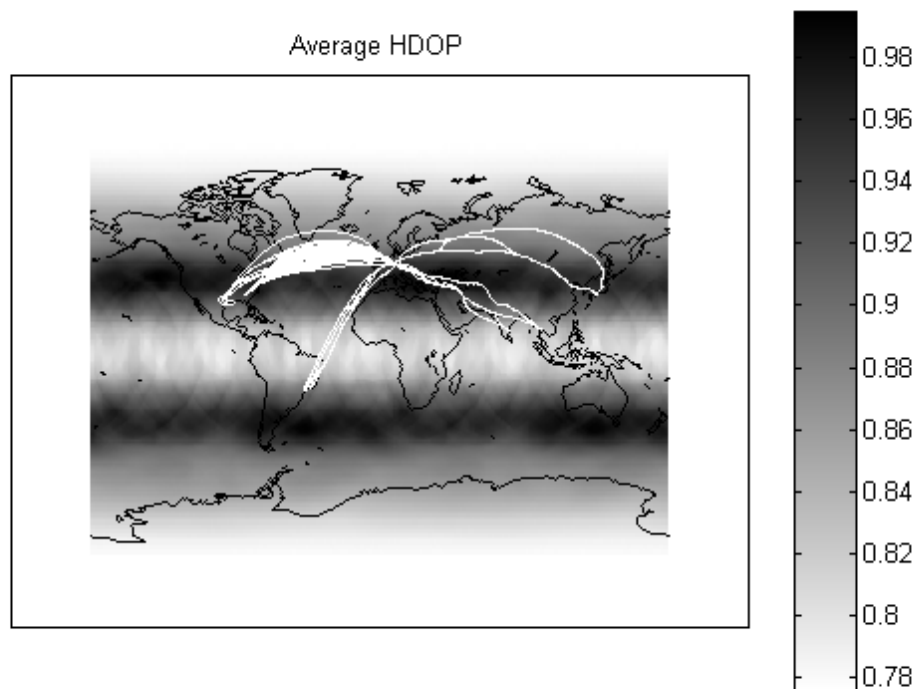
Figure 22: Average HDOP during Flight Trials

flight trials a 26-satellite constellation was operational instead of the nominal 24-satellite constellation.

Figure 23 displays the difference between the average HDOP for the real 26-satellite constellation and the nominal 24-satellite constellation. The dark areas represent those regions where the two additional satellites bring an advantage over the nominal satellite constellation. This improvement influences in particular the flights over the East Coast of the United States. However, most of the data where collected in regions not being affected too much by the improvement of the geometrical quality of the constellation caused by the two additional satellites. In addition in can be stated that is unlikely that GPS will ever be operated in a nominal constellation only, because the current replacement strategy for the satellites will always lead to more than the nominal 24 satellites being in orbit.

From Figure 22 and Figure 23 and the associated considerations it can be concluded that the areas of the Earth covered by the flight trials and therefore the collected data are representative, if not even leading to more conservative results in particular over the North Atlantic Region.

This answers the question about the recorded data being representative with respect
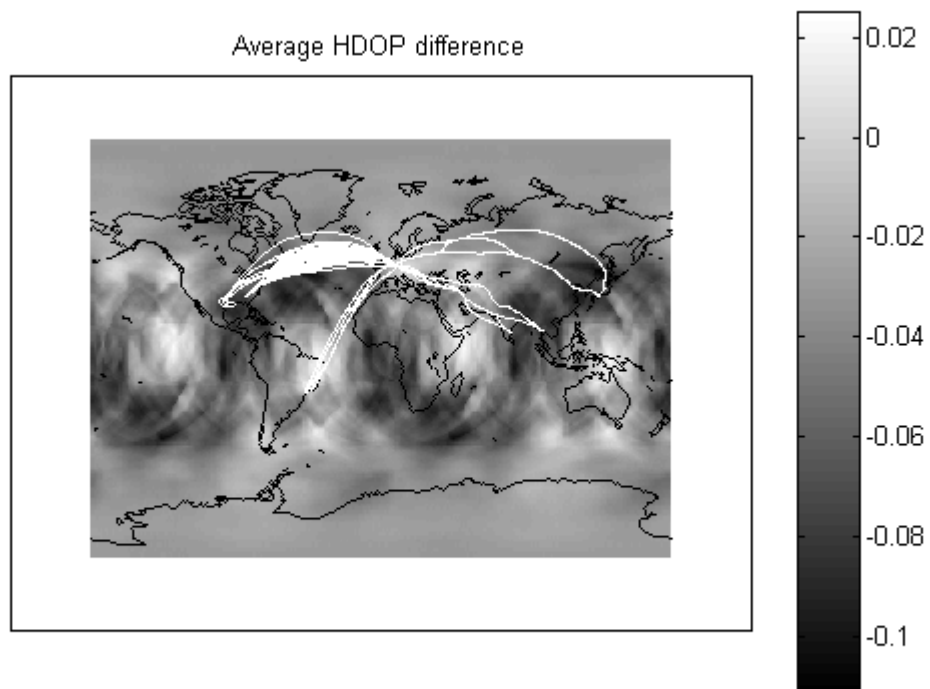
Figure 23: Average HDOP Difference to nominal 24-Satellite Constellation
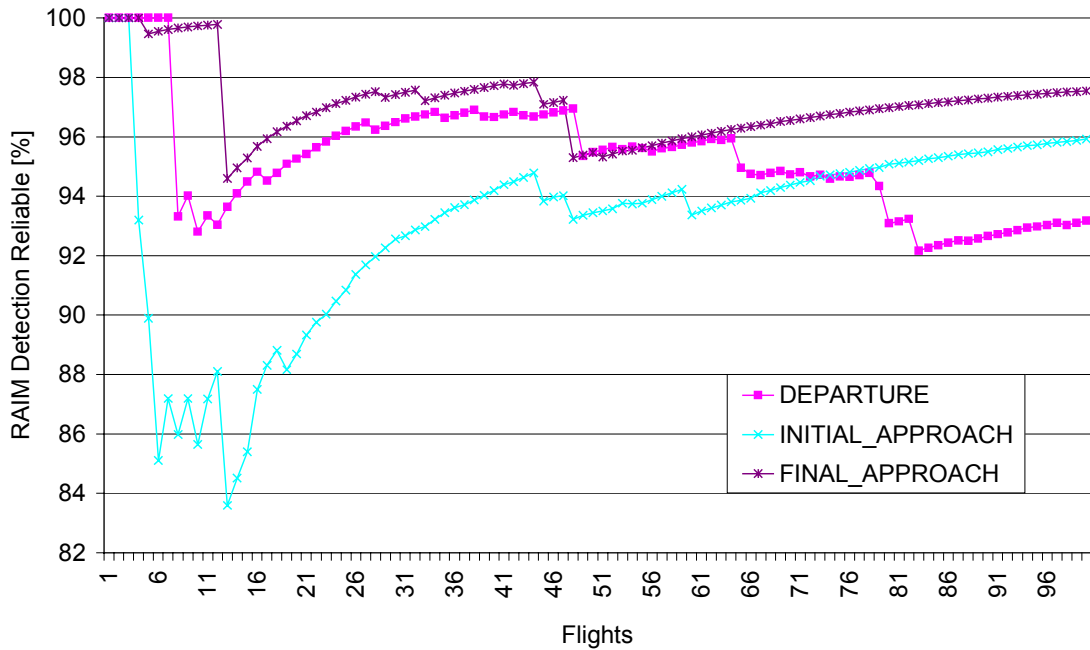
Figure 24: Accumulated Statistics for Sturza-Brown FD Reliability (I)

to the geographical distribution of the flight trajectories and the distribution of the geometrical quality of the satellite constellation over the Earth's surface. The second question to be looked at is the amount of data being recorded and being sufficient to form a fundamental set for the results to be statistically representative.

Figure 24 and **Figure 25** show the accumulation of the statistical results for reliable RAIM Detection (Sturza-Brown algorithm) as the number of flights included in the fundamental set for the statistics grows.

These graphs are intended to give a general impression of the dependence between the occurrence of outages, their duration and the size of the fundamental set of data considered for the statistics. The graphs for Departure, Initial and Final Approach (Figure 24) appear to show an asymptotic behaviour which may be expected from such a graph. However, the Availability of RAIM Detection decreases quite considerably after the first flights and this has a strong influence on the remainder of the curve.

Figure 25 contains the graphs for En-Route and Terminal phases of flight. The curves do not necessarily follow the expected asymptotic pattern. However, it needs to be outlined that the scale of the y-axes only covers 0.12% of the total of 100%. The results presented here are based on the data recorded from the onboard receiver, and it is appropriate to recall that these data contain numerous outages caused by outage classes which were receiver-specific and would not necessarily appear with a different receiver. Therefore, another receiver based on an all-in-view
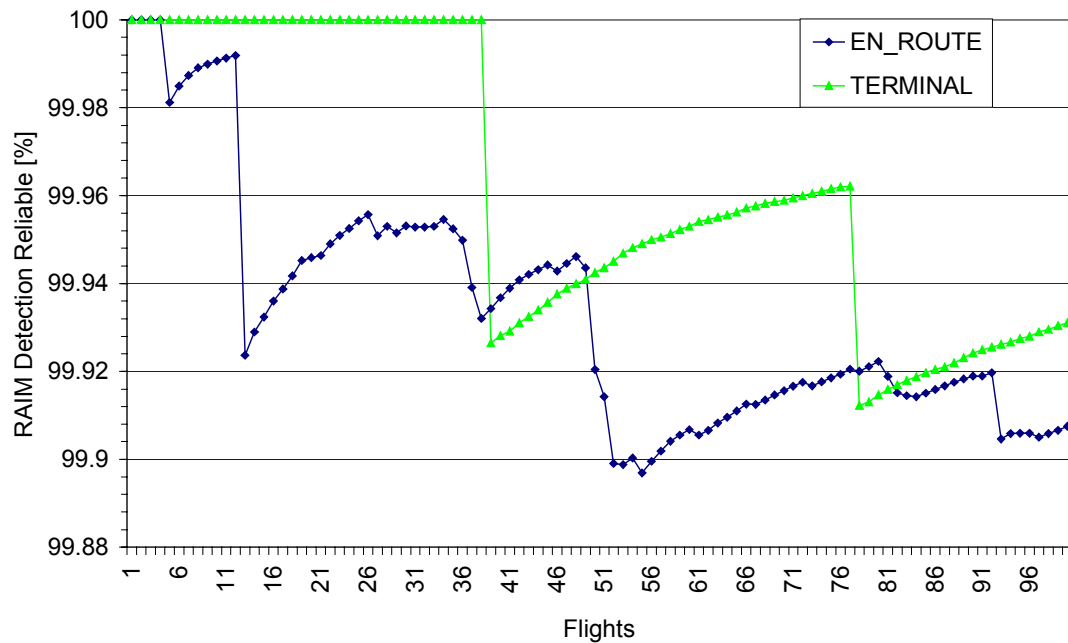
Figure 25: Accumulated Statistics for Sturza-Brown FD Reliability (II)

technology would be expected to provide results which would be closer to the expectation of the asymptotic behaviour.

The presented results are restricted to the flight trial data referred to in Section 7.2.5. The above saturation graphs show that an increasing amount of data would improve the confidence level be placed on the results. However, these graphs present a tool which could be used during a continuous data evaluation process to help determining the size of the fundamental set of data which can be considered as being sufficient to establish statistically representative results.

8.2   VERIFICATION OF RNP PARAMETERS

The results of the data evaluation in the preceding sections are based on the requirements laid out in Table 4. It shall now be established in how far these results meet the FD and FDI Availability requirements summarised in the same table.

In order to facilitate this comparison and to increase the fundamental set for the statistical results, the values for Departure, Initial and Final Approach, and the values for En-route and Terminal, respectively, are combined, since the requirements for these two groups of flight phases are the same.

Table 17 summarises the results concerning detection declared reliable by the RAIM algorithms based on the results in Table 16. The values given in bold are those which

RAIM Algorithm Results (Detection reliable)	Departure + Initial + Final App. (NPA)	En Route + Terminal
Sturza-Brown	99.63064076	**99.98709300**
Brenner	99.60099319	**99.98695570**
Sturza-Brown +Baro	**99.83199714**	**100**
Brenner + Baro	**99.80234957**	**100**

Table 17: Availability of reliable RAIM Detection (in bold: requirements achieved)

meet the requirement for FD Availability (99.80% - 99.90%). These results are limited to Failure Detection because the algorithms were not required to switch into their Identification mode (see Section 8.1.3).

The following conclusion can be drawn from these results: Without baro-aiding the FD Availability requirement can be met for the En-route and Terminal phases of flight, but it requires baro-aiding to fulfil the requirement during all phases of flight down to final approach.

Table 18 contains the relevant results for the predicted Availability of RAIM FDI derived from Table 12 and Table 13. The results for the theoretical and theoretical dynamic visibility scenarios are given. The measured scenario has not been considered due to the restrictions induced on the results by the limitation of using an 8-channel receiver (see Sections 8.1.2 and 8.1.4).

The following conclusions can be drawn: (i) During En-route and Terminal phases of flight the FD Availability (99.80-99.90%) and the FDI Availability (94.55-98.20%) requirements can be met by un-aided RAIM, (ii) the introduction of baro-aiding allows the requirements to be met during the more demanding phases of flight for the theoretical visibility scenario. It is evident that the dynamic environment during Departure, Initial and Final Approach has a major effect, in particular, on the RAIM FDI Availability.

Predicted RAIM Availability	Departure + Initial + Final App. (NPA)	En Route + Terminal
Theoretical Dynamic		
FD Sturza-Brown	95.45999531	**99.99643165**
FD Brenner	95.60832108	**99.99639734**
FDI Sturza-Brown	50.95731926	**99.12829318**
FDI Brenner	53.51346674	**99.14400764**
Theoretical		
FD Sturza-Brown	99.73672175	**100.00000000**
FD Brenner	99.73672175	**100.00000000**
FDI Sturza-Brown	69.14576715	**99.60024183**
FDI Brenner	71.03692075	**99.60940287**
Predicted Baro-aided RAIM Availability	**Departure + Initial + Final App. (NPA)**	**En Route + Terminal**
Theoretical Dynamic		
FD Sturza-Brown	99.45119464	**99.99969120**
FD Brenner	99.56491107	**99.99969120**
FDI Sturza-Brown	80.48774458	**99.93323068**
FDI Brenner	82.71139513	**99.93439726**
Theoretical		
FD Sturza-Brown	**100.00000000**	**100.00000000**
FD Brenner	**100.00000000**	**100.00000000**
FDI Sturza-Brown	93.22027613	**99.99320641**
FDI Brenner	**95.12008207**	**99.99320641**

Table 18: Predicted Availability of RAIM FDI (in bold: requirements achieved)

9. **SAFETY CASE DEVELOPMENT**

9.1   INTRODUCTION

This chapter introduces the fundamentals of the Safety Case concept. The history of this concept and the ALARP ("As Low As Reasonably Practical") principle – which is paramount for the Safety Case development - are briefly summarised in order to demonstrate the origin of the concept and the level of acceptance it has gained for non-aviation applications. Recent activities show that the civil aviation community - after its introduction to the Safety Case concept – is seriously considering adopting it for the safety regulation of satellite navigation services.

This chapter shows how a high level safety standard in form of a Target Level of Safety (TLS) can be formulated to serve as the basis for a risk model. This risk model is, subsequently, developed to demonstrate how the results obtained in Chapter 8 can be used by an Air Traffic Service provider to achieve a conclusive Safety Argument or Case in favour of the use of satellite navigation onboard of commercial airliners**.**

9.1.1   Safety Case Concept

The term "Safety Case" is one which has become widely used in the UK - and more recently in other regions of the world such as South East Asia - to refer to a particular approach to safety assurance which has been gaining ground over the last 20-30 years [TIEMEYER, 1997]. The Safety Case is contained in a document, which presents the safety rationale, evidence and findings of a service provider (Dutyholder) to a regulator or approval body. The document is prepared in such a way as to represent the Dutyholder's argument for why he considers the service to be safe. He presents his 'case for safety' to a regulator who will then either accept or reject it. Responsibility for the case and for the safety of the service itself are never given up by the Dutyholder.

The Dutyholder must justify to himself that the service is safe and the Case represents his plans, designs, arrangements and, where applicable, his arguments which will convince the regulator to accept his justification for safety. The same basic approach has also been adopted in parts of mainland Europe, though the term "Safety Case" is not generally used.

In a Safety Case regime, the Dutyholder himself sets the goals for safety performance and describes how he proposes to meet the goals at a detailed technical level. This contrasts with a prescriptive regulatory approach, where a specific approach is mandated. The Dutyholder, who is responsible for the service, is free to choose the most effective approach that meets these safety requirements. The Dutyholder must demonstrate to the regulator that his chosen approach is safe in concept, design and operation, taking into account both technical and human factors. In particular, the Dutyholder is obliged to demonstrate that all risks have been reduced to "As Low As Reasonably Practicable" (ALARP).

The Safety Case is a 'living' document, which evolves over the lifetime of a service. Submission for approval at the following lifecycle stages is recommended:

i) design;
ii) detailed design;
iii) pre-operation;
iv) operational (ongoing).

The Safety Case approach may also prove that the system is 'unsafe'. The Safety Case helps determine this fact.

The Safety Case philosophy is aimed at those bodies (the designers, operators and providers) who are in the best place to provide safety analysis and to address the consequences of the analysis in a timely and effective manner. At the same time, the Safety Case aims to ensure that the Dutyholder has satisfied himself that the system is safe and that this issue is not left open to a regulator to determine. With prescriptive regulation this process is reversed, implying that the regulator must establish the system safety targets and prescribe requirements to the Dutyholder for achieving safety. The clear distinction is, therefore, that the Safety Case recognises that the regulator is perhaps in the weakest position to ensure that all matters affecting the safety of design and operation have been identified and that these risks have been effectively managed.

Indeed, a more important factor may be that prescriptive regulation requires the full system hazard analysis to be completed before the requirements can be set, and thus the design will be delayed while this occurs. Equally, the analysis requires there to be a design (and defined operational regime) on which to base the analysis. The Safety Case regime, in contrast, specifies only the high level target and thereafter allows the designer to evolve the design detail and the risk analysis in parallel. This clearly reduces project lead times.

9.1.2 History

During the 1960's it was recognised within the UK that the law which governed the health and safety of people at work needed a complete rethink. Not only was the law at the time fragmented but it was not dealing with the problems posed by advancing technology. Lord Robens was appointed to investigate the rise in accidents in the modern workplace and to publish these findings [ROBENS, 1972]. The central philosophy which the report questioned was the practice of controlling safety by the process of detailed prescriptive regulation and he concluded that the process was no longer appropriate to modern technology and that self regulation by industry itself, exercising a more open ended duty of care would prove more satisfactory.

In the UK, following the Robens Report the move to the goal-setting approach to safety legislation across industry began with a major overhaul of the UK Health and Safety Legislation that took place in the mid-1970's. This trend continued in the late 1980's with the development and adoption of a European Council Framework Directive addressing health and safety at work; this was implemented in the UK as the Management of Health and Safety at Work Regulations (1992), which introduced the requirement for a risk assessment by all employers.

In parallel with these developments in general health and safety legislation, the use of risk assessments and Safety Cases extended across the industries dealing with potentially major hazards. The UK nuclear power industry was already producing Safety Cases in the early 1970's. For the chemical industry the Seveso Directive [CEC, 1982] introduced similar requirements. In the offshore sector, the Piper Alpha accident in 1988 [CULLEN, 1990] ultimately led to the introduction of the Offshore Installation (Safety Case) Regulations in 1992. The other North Sea Shelf States, most notably Norway, have adopted an essentially similar approach. The privatisation of the UK Railway industry was preceded by the introduction of a Safety Case regime, enacted in 1994 [HSE, 1990].

On the international scene, a number of countries in the Asia Pacific region have adopted Safety Case regimes for both their on and offshore oil and gas, chemical and petrochemical, and transport industries, based broadly on the UK/EC models. In the shipping industry, the last 4-5 years have seen a developing interest on the part of the International Maritime Organisation (IMO) in the use of an element of risk assessment alongside its existing, largely prescriptive, regime. In the specific field of control systems and electronics, the International Electro-technical Commission (IEC) is developing a standard for the functional safety of safety related systems using a risk-based approach.

9.1.3 The ALARP Principle

The ALARP principle introduced in Section 9.1 can be used to judge whether an acceptable standard of safety has been achieved. The aim of a safety management system is to reduce risks to "As Low As Reasonably Practicable" (ALARP). The ALARP principle recognises that no activity is entirely free from risk, but predicates that the level of risk should be minimised. The Dutyholder is considered to have discharged his responsibility if he can show:

- that the level of risk is tolerable, and;
- there would be a gross disproportion between the cost of additional preventive or protective measures, and the reduction in level of risk that would be achieved.

The ALARP triangle (**Figure 26**) indicates three specific areas within the diverging lines that represent an increasing level of risk. There will always be a point at which the level of risk is deemed to be unacceptably high. If the level of risk cannot be reduced below that level the system in question is considered to be too hazardous. The criteria for acceptance of risk vary from one industry to another; they are based on how the individuals exposed to the hazards perceive the level of risk, and the degree to which they believe they have control over their exposure. The threshold below which the level of risk is considered to be negligible may be judged by
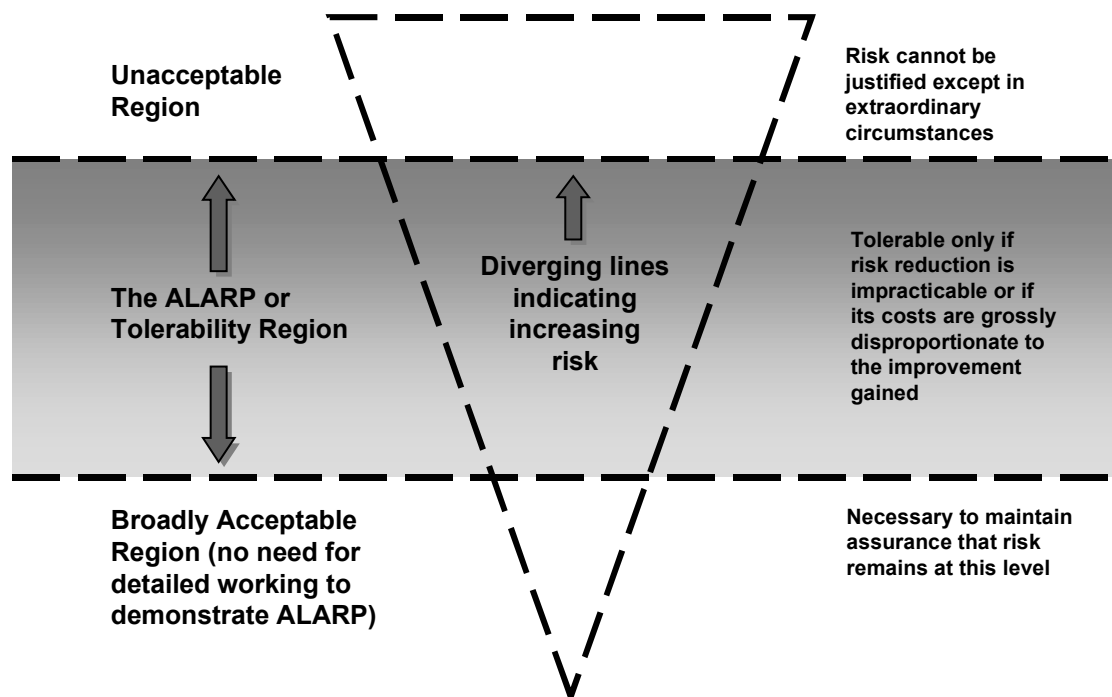
Figure 26: The ALARP Principle

comparison with the exposed individuals' short term risk of death from natural causes.

Where the level of risk is below but close to the intolerable level, a high burden of proof is placed on the Dutyholder to attempt to reduce the risk further, and to show that all reasonably practicable precautions have been taken. Where the risk is less, there is still a continuing duty on the Dutyholder to take all reasonably practicable steps to ensure that accidents either do not occur, or that if they do, their effects are mitigated. The financial trade-off between cost and level of risk becomes progressively of more importance as the level of risk decreases. Eventually, a point is reached where the risks are sufficiently negligible that further risk assessment, and consideration of additional precautions, is unnecessary. These points are represented by the horizontal lines on the diagram.

9.2 SAFETY STANDARD

Any Safety Case requires the derivation of a fundamental safety standard against which it will be judged whether the service proposed by the service provider (Dutyholder) will be safe. This safety standard can be derived from the concept of the Target Level of Safety (TLS) developed by ICAO [ICAO/AWOP, 1994]. The TLS is a global target for all hazards associated with civil aviation. The TLS can be expressed as the acceptable frequency of accidents attributable to all causes. The safety standard to be applied to satellite navigation is a fraction of this global TLS.

ICAO derives in [ICAO/AWOP, 1994] - based on historic data for jet propelled aircraft - a global TLS value of 1.0×10^{-7} fatal accidents per flight hour. Based on an approximate number of flight hours of 1.0×10^7 within the ECAC airspace during the year 1998, the global TLS would correspond to one fatal accident per year over ECAC.

A more rigorous determination of the TLS value based on historic accident data in the ECAC region has been undertaken in [TIEMEYER, ET AL., 2000]. Here, aircraft types have been included which establish a more complete representation of the commercial air traffic in Europe. Based on available accident data and statistics of the annual numbers of aircraft movements collected by EUROCONTROL over the period 1993 to 1998, the accident rate is calculated as 1.39×10^{-6} hull loss accidents per mission. Considering the total number of flights recorded under Instrument Flight Rules for 1998 yields approximately 10 hull loss accidents per year.

This number can be defined as the global, publicly acceptable overall safety standard (TLS) which comprises all causes of accidents. Examinations of air accident statistics reveal that navigation systems do not contribute significantly as the primary causes of accidents, however, a dominant cause labelled 'cockpit crew' presumably includes a number of accidents caused by inappropriate actions taken following failures of navigation systems. In addition it needs to be recognised that causes and their contribution leading to accidents vary with the phase of flight during which they occur.

For the purpose of developing the risk model in Section 9.3 and in the absence of any firm data, the fraction of the TLS attributable to satellite navigation shall be assumed to be 1%. This figure is consistent with the precedent of 0.8% of the accident rate which was used in calculating the safety standard for Instrument Landing Systems. Based on 1998-numbers describing the air traffic in the ECAC region, this would result in one hull loss accident per ten years as the maximum tolerable risk contributed to the global TLS by satellite navigation.

Remark: It shall be underlined, that the fraction of the global TLS attributable to satellite navigation as 1% is an assumption to facilitate the future development of the risk model. Air Traffic Service providers need to revise this number dependent on circumstances particular to the airspace they are responsible for and the type of operations for which they plan to obtain approval.

9.3   PROPOSED RISK MODEL

The risk model that connects the possible failures of the satellite navigation system through to the Target Level of Safety is developed in this section. It forms the basis for the Air Traffic Service Providers to translate results obtained in Chapter 8 into a conclusive Safety Argument or Case in favour of the use of satellite navigation onboard of commercial airliners.

Starting on the left hand-side of **Figure 27** a list of all possible GNSS failures and their frequencies needs to be established. Basic input for this list is provided by the results of Chapter 8.

The flow diagram (rotated) contains the following labelled boxes and annotations:

- GNSS Failure
- Dutyholder's Mitigation Measures
- Hazard Frequency
- ATS Provider's Mitigation Measures
- Overall Hazard Frequency
- Consequence C=1 (CFIT) C=2 (Midair)
- Contribution to Level of Risk from Hazard
- Σ
- Total Level of Risk from all Hazards attributable to GNSS
- Compare with Fraction of the TLS assigned to GNSS
- Assess separately for each State, then combine for the whole of ECAC
- Contractual Interface between the GNSS Dutyholder and the States' ATS Providers
- Δ ATS
- GNSS SAFETY CASE
- ATS SAFETY CASE

Figure 27: Safety Case - Risk Model

Maybe not for GPS, because of a lack of direct control and influence, but for any future satellite navigation system it can be considered that the Dutyholder could put further measures in place to mitigate the remaining GNSS failures. However, these mitigation measures can be assumed to fail with a certain probability, which leads to the hazard frequency within the GNSS. The system performance together with the hazard frequency forms the basis for the GNSS Safety Case, which has to be established by the GNSS Dutyholder. Here he demonstrates that he has taken all reasonably practical steps - using the ALARP principle (Section 9.1.3) - to ensure that the system achieves its performance and safety requirements. At this stage in the process the contractual interface between the GNSS Dutyholder and the Air Traffic Service provider can be established.

From this point onwards it is the responsibility of the ATS provider to define the operational service he intends to provide using GNSS. If the GNSS performance and the associated GNSS hazard frequency do not satisfy the operational requirements, the ATS provider has to foresee appropriate mitigation measures such as back-up navigation means for en-route operations or alternate airports for precision approaches. The probability that these mitigation measures will fail leads towards the overall hazard frequency. By using the ALARP principle again (Section 9.1.3), the ATS provider has then to demonstrate that he has taken all reasonably practical steps to ensure that the service he intends to offer is safe. The overall hazard frequencies, which can be experienced in the national airspaces have to be combined for the whole of the ECAC area and then be multiplied by their possible consequences such as controlled flight into terrain (CFIT), mid-air collision or simply loss of separation to obtain the level of risk resulting from the hazards. Subsequently, all risks have to be combined to determine the total level of risk from all hazards attributable to GNSS.

It has to be shown that the total level of risk finally obtained is less than the fraction of the Target Level of Safety, which had been assigned to GNSS in Section 9.2.

The ATS Safety Case is completed through the combination of the GNSS Safety Case and the work carried out by the ATS Service Provider.

9.4   RECENT DEVELOPMENTS – REGULATORY MECHANISM

The Safety Case concept, which has been introduced in the preceding sections, was recently proposed to the European civil aviation community as a means to regulate future satellite navigation services. This proposal led to the initial agreement between a number of European Air Traffic Service providers to commence with the

development of the Design Safety Case (see Section 9.1) for the European Geostationary Navigation Overlay Service (EGNOS) [TIEMEYER, 1999].

In [TIEMEYER, 1997] was identified that the introduction of space systems to civil aviation radionavigation service provision requires unprecedented co-operation on safety regulation at both regional and international levels, reflecting the international nature of satellite systems themselves. Satellite navigation systems will deliver signals over a large portion of the Earth's surface. Ideally, this should be reflected in the approach to their safety regulation and it was considered that the Safety Case philosophy could provide an efficient means of achieving such an objective.

The functional relationship between participating organisations as displayed in **Figure 28** serves as the basis for (i) explaining the regulation philosophy and (ii) identifying those issues to be dealt with nationally and those to be carried out on an international level.

The Global Navigation Satellite System (GNSS) Safety Case (SC) will need to be provided by the 'GNSS Dutyholder' to the State Air Traffic Service Providers. The individual State ATS Providers will incorporate this GNSS Safety Case into their Safety Case (or alternative approval process) for the provision of air traffic services. Today, system and service provision occurs within the boundaries of individual States. This will not be the case when satellite navigation systems are used because of their multi-national nature.
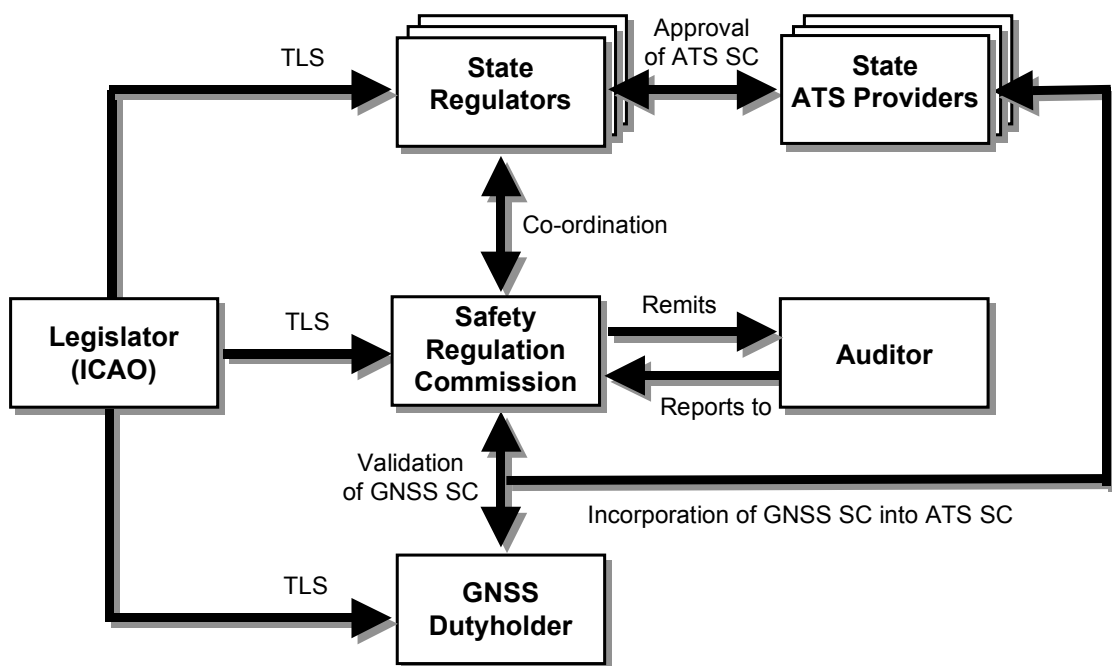
Figure 28: Proposed Regulatory Mechanism

The key feature of the mechanism is that it provides a basis for consensus between the States and serves as a focus for achieving the system safety assurance objectives. As a result of EUROCONTROL's Revised Convention (signed on 26th June 1997) the EUROCONTROL Safety Regulation Commission (SRC) was established in 1998 to ensure European co-ordination between national safety regulators from an early stage *inter alia* related to satellite navigation. Such a mechanism would address the primary functions of the

- Legislator (ICAO);
- Safety Regulation Commission (SRC);
- GNSS Dutyholder;
- Auditor;
- State Regulators and
- State Air Traffic Service Providers

as depicted in Figure 28. The following sections provide guidance as to how the proposed regulatory mechanism operates as well as explaining the functions and their interactions.

9.4.1   The Legislator (ICAO)

A Legislator – here the International Civil Aviation Organisation (ICAO) – should define the Target Level of Safety for the future use of all GNSS services across all regions. The Legislator has to ensure consistency in safety matters and inter-operability issues.

9.4.2   The Safety Regulation Commission (SRC)

The implementation of the Safety Case Regime requires the centralisation of certain of the State Regulators' activities. The SRC – as a body composed of States' representatives – would collectively agree whether the Dutyholder had developed an acceptable case for safety. The SRC comprises representatives of all the State Regulators such that extra- and inter-State problems can be resolved in this forum.

One of the responsibilities of the SRC will be to satisfy itself that the provisions described in the Safety Case are in place and operating effectively. This is termed validation of the Safety Case.

The remit of SRC as far as GNSS is concerned is to:

- ensure the sharing of State experiences;
- provide the means to co-ordinate and harmonise the activities of the State Regulators;
- establish an open forum for international discussion regarding the regulation of GNSS;
- minimise the overall cost and time-scales of the GNSS approval stages, and
- provide confidence in GNSS as an approved system for world-wide application.

9.4.3 The GNSS Dutyholder

The function of the Dutyholder is to ensure the safety of the overall design and operation of GNSS. He would review and determine the adequacy of the case for safety and initiate changes as a result of these reviews. The Dutyholder would act as the single point of contact for all Safety Case material presented to the SRC.

9.4.4 The Auditor

The SRC may, during the design and operational phase of the system, raise queries regarding the system design, operation and integration. The SRC could appoint an Auditor to assist in the resolution of queries and to undertake the continuous validation of the Safety Case, in particular, the Safety Management Systems, Practices, Plans and in-house monitoring guidelines. It is this activity which will provide continuous evidence to the SRC that the system is safe, and will continue to be safe. The Auditor would operate solely as the agent of the SRC and be fully independent of the GNSS Dutyholder and the State ATS Providers.

9.4.5 The State Regulators

The State Regulators already regulate the activities of the ATS providers within the State boundary and this process will continue unchanged. The State Regulator will be responsible for accepting the ATS Safety Case with guidance from the Legislator and perhaps the SRC. Further assistance, if requested from the SRC, in form of an Independent Advisor may also be available. The State Regulator will provide input and feedback to the SRC with the SRC overseeing the consistency of local regulation for these services.

9.4.6 The State Air Traffic Service Providers

The Air Traffic Service (ATS) providers and airspace users within each State should construct an Air Traffic Service Safety Case covering all aspects of CNS/ATM. Part of that Safety Case would comprise the GNSS Safety Case. This should be carried out with appropriate guidance from the Legislator, SRC and State Regulator. The ATS Safety Case will then be submitted to the State Regulator within each State.

The ATS providers will require an interface with the State Regulator, although these bodies will remain completely independent of each other. This should ensure that the Regulator is able to have full visibility of the service provision and its associated activities.

The ATS providers must have the authority to implement changes necessary to ensure that the safety targets are met, and that operational safety is maintained in accordance with the terms of the ATS Safety Case.

9.5 APPLICATION OF THE RISK MODEL

This section introduces how the processes described in Chapter 6 and the results obtained in Chapter 8 can be used as the basic input into the risk model developed in Section 9.3.

For the result of any risk modelling activity to be acceptable to the Dutyholder and, subsequently, to the Regulator, it is necessary to provide evidence that the data fed into the model are correct. This evidence is provided through two independent activities.

First, all tools used to deliver any safety-relevant data have to be developed following the rules for producing 'High Quality' Software (Section 6.1.1). By applying and enforcing the defined standards for software development and quality assurance the Dutyholder demonstrates that he has done everything which is 'reasonably practicable' to ensure himself and the Regulator about the correctness of his findings.

Second, at least two different data analysis algorithms have to be independently tested and implemented. They should deliver throughout the data evaluation process similar results, thereby justifying that the obtained results can be considered as having a very high level of confidence.

In this particular case, in order to relate the results describing the Availability of the Accuracy and Integrity functions to the risk model of the GNSS Safety Case (Figure 27) an identification of the potential hazards and their frequencies, given rise by the GNSS failures, needs to be carried out to populate the box 'Hazard Frequency'. It is assumed that the relevant hazards resulting from any GNSS failure are erroneous position calculations. In order to determine the frequency of potential hazards occurring (here: position errors) a hazard identification tree needs to be developed.

9.5.1 Failure Identification Tree

Figure 29 proposes a model of such a hazard identification tree to be applied to satellite navigation. Fundamental input to this tree are the Required Navigation Performance and the performance level of the availability of Accuracy, Failure Detection, and Failure Detection and Identification.

The potential hazard, which can be attributed to Accuracy, is the loss of accuracy, due to an insufficient geometry of correctly operating satellites. May this potential
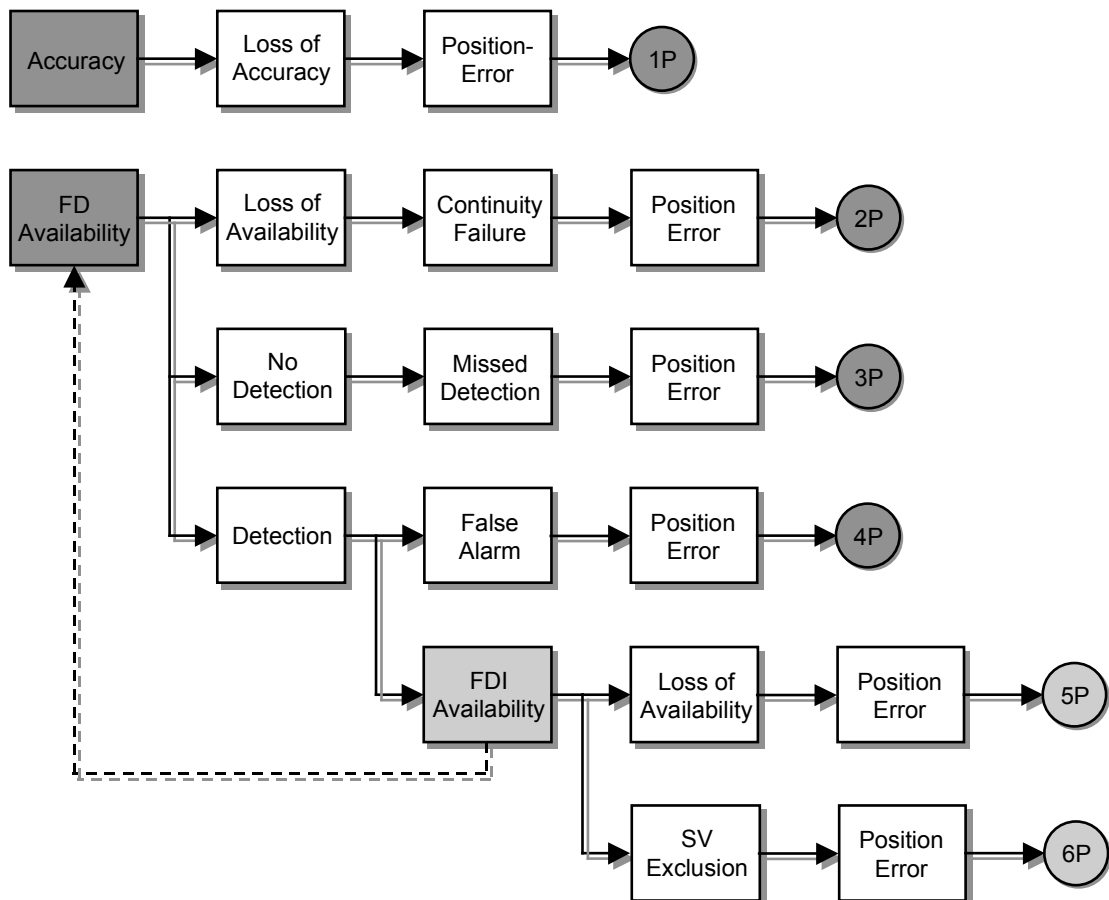
Figure 29: Model of a Hazard Identification Tree

hazard occur it can yield to a position error (hazard '1P').

The second failure mode relevant to the hazard identification tree is the availability of the RAIM Failure Detection function. Loss of availability can lead to a Continuity of Service failure after the maximum allowable outage time is exceeded. This loss of continuity could result in a position error (hazard '2P').

In case of Failure Detection being available, the most likely outcome is no detection occurring. Missed detection remains as the potential hazard, which could subsequently lead to a position error (hazard '3P'). Does the system detected faulty information coming from one of the satellites, this could be due to one of two reasons, either a false alarm (concluding in hazard '4P') has occurred, or a correct detection. In either case the Failure Identification process would be initiated, which means restarting the Failure Detection process on the sub-sets of the satellite constellation. This restart would allow to identify that sub-set, which does not lead to Detection and, therefore, does not include the satellite transmitting the faulty information. Whether the satellite is identifiable or not, the probability of a position error still remains leading into hazards '5P' or '6P'.

The next step to be taken is the assessment of the individual hazards identified in the tree and the evaluation of their associated frequencies. This concludes the establishment of the information required describing the box 'Hazard Frequency' of the GNSS Safety Case in Figure 27.

9.5.2   Hazard Assessment

In order to conduct the hazard assessment it is required to analyse the branches of the Hazard Identification Tree. **Table 19** summarises the results of such a hazard assessment.

The potential hazards given rise by the GNSS Failures are transferred from Figure 29. The Required Navigation Performance describing the requirements related to each of these potential hazards are listed in Table 3 and Table 4 in Chapter 8. The question is addressed whether these requirements are met, considering mitigation measures, where appropriate. Are the relevant requirements met, the potential hazard may remain with a certain frequency of occurrence. Then the probability of a relevant position error resulting from the potential hazard has to be determined. Subsequently, the frequency of occurrence of the potential hazard multiplied by the probability of a position error resulting from the potential hazard yields the hazard frequency for the hazard to give rise to a relevant position error.

GNSS Failure	Potential Hazard	RNP	Mitigation	RNP met?	Freq. of Occurrence of pot. hazard	Probability of Position Error from pot. hazard	Hazard (Figure 29)	Hazard Frequency
Accuracy	Loss of Accuracy due to insufficient geometry of correctly operating satellites	→Table 3 Accuracy	—	yes, at all times →Section 8.1.1	0	—	1P	does not occur
Integrity	Loss of Failure Detection Availability	→Table 4 FD Availability	Baro-aiding	yes, but does not lead to a hazard in its own right →Section 8.2	—	—	—	—
	Loss of Continuity of Service due to insufficient geometry of correctly operating satellites (Failure Detection)	→Table 4 Continuity of Service	Baro-aiding	yes, allowable outage duration never exceeded with mitigation →Section 8.1.6	0	—	2P	does not occur
	Missed Failure Detection	→Table 4 Integrity Risk	Baro-aiding	yes, constraint parameter for RAIM algorithm →Section 8.2	10^{-7}/h	0.1 – 1.0 *Position reference required*	3P	10^{-7} - 10^{-8}/h
	Failure Detection False Alarm	→Table 4 False Alarm Rate	Baro-aiding	yes, constraint parameter for RAIM algorithm →Section 8.2	10^{-5}/h	0.1 – 1.0 *Position reference required*	4P	10^{-5} - 10^{-6}/h
	Loss of FDI Availability	→Table 4 FDI Availability	Baro-aiding	yes for terminal and en-route, does not lead to a hazard in its own right →Section 8.2	—	—	5P	—
	Satellite exclusion following Failure Detection	—	—	does not lead to a hazard in its own right	—	—	6P	—

Table 19: Hazard Assessment

Accuracy

The potential hazard to be attributed to Accuracy, is the loss of accuracy due to an insufficient geometry of correctly operating satellites. Section 8.1.1 reveals that Accuracy is available at any time. Therefore, it can be concluded that the frequency of occurrence of this potential hazard equals '0' and that hazard '1P' is unlikely to appear and not being of any relevance. It may become relevant if a faulty satellite were identified and excluded from the navigation solution and the Accuracy shall still be achieved with the reduced number of satellites. In Section 8.1.1 it is shown that in this case Accuracy may not always be available. However, this leads not to a hazard in its own right, because at this stage it is already known to the system that a fault

has occurred and appropriate mitigation measures external to the satellite navigation system can become effective.

<u>Integrity</u>

The loss of availability of the Failure Detection function is the first potential hazard of the group of hazards given rise by GNSS failing on Integrity. Section 8.1.2 provides the evidence that the requirements from Table 4 are achieved. Scenarios exist which require baro-aiding being used as a mitigation measure. However, loss of FD Availability can be assessed as not being a hazard in its own right as further mitigation measures external to GNSS could be thought of to cover periods of determined FD unavailability.

The potential hazard of loss of availability – as described above – can lead to a Continuity of Service failure after the maximum allowable outage time is exceeded. This loss of continuity could result in a position error (hazard '2P'). The results in Section 8.1.6 have shown that it is possible to avoid any such failure in continuity when using baro-aided RAIM. Therefore, this hazard does not occur assuming that baro-aided RAIM is used.

In the case of Failure Detection being available, the most likely outcome is that no detection occurs. In fact, the results in Chapter 8 show that during the analysed 900 flight hours at no time a detection did occur. However, one potential hazard remains: missed detection. The frequency of this happening is 10^{-7}/h, which was a constraint parameter for the RAIM algorithms. Needed is the probability of such a missed detection leading to a position error resulting in hazard '3P'. To conclude the assessment of this hazard at this stage it is assumed that a missed detection during the more demanding phases of flight would ultimately lead into a position error (probability 1.0 / worst case assumption). For the lesser demanding phases of flight it shall be assumed that only one out of ten missed detections would result in a position error due to the length of time to recover until the position error increases in excess of the given accuracy limits (probability 0.1). However, these assumptions need to be validated through intensive investigations using positioning reference systems. In the current absence of such reference data, it is only possible to proceed with the hazard assessment based on these assumptions.

If the system has detected faulty information coming from one of the satellites, this could be either a false alarm (concluding in hazard '4P') or a correct detection. The False Alarm Rate was predefined with a maximum of 10^{-5}/h, as one constraint parameter for the RAIM algorithms to give rise to this potential hazard. Again it shall be assumed that a false alarm during the more demanding phases of flight would

ultimately lead into a position error (probability 1.0 / worst case assumption). For the remaining phases of flight one out of ten (probability 0.1) false alarms could potentially result in a position error for the same reason as above. To validate the determination of the probability of this hazard to result in a relevant position error, positioning reference data would equally be required.

Following a Failure Detection the Failure Identification process would be initiated which means restarting the Failure Detection process on the sub-sets of the satellite constellation. This restart would allow to identify that sub-set, which does not lead to Detection and, therefore, does not include the satellite transmitting the faulty information. One potential hazard (→hazard '5P') is the unavailability of the FDI function for which a general availability requirement exists (Table 4). Again – using baro-aiding – this requirement can be fulfilled at least during terminal and en-route phases of flight.

Having FDI available the possibility of a position error still remains whether the satellite is identifiable or not, leading into hazard '6P'.

However, the latter two potential hazards can be assessed as being not hazards in their own right because at this stage (following detection) it is already known to the system that a fault has occurred and appropriate mitigation measures external to the satellite navigation system could come into force.

The Hazard Identification Tree and the hazard assessment scheme describe the basic GNSS failures, determine the relevance of the potential hazards and with what frequency they may give rise to the hazard categories '1P' to '6P'. Subsequently, the hazards are propagated through the Air Traffic Service environment by describing the escalation path that may lead to a fatal accident. Figure 27 and Table 19 identify that either mitigation measures can be engineered into the GNSS application or procedural measures (e.g. conditions for operational approval) could be put in place to prevent a failure that has occurred from escalating into a fatal accident. These may be thought of as a series of barriers to prevent such a thing from happening. Their effectiveness may be characterised as the probability that they succeed in arresting the propagation of the accident sequence when demanded. The intent of these mitigation measures is to ensure that the contribution of the navigation system does not exceed the fraction of the Target Level of Safety as assigned to it in Section 9.2.

10. __MULTI-MODAL APPLICABILITY__

10.1 __GENERAL__

This chapter discusses the applicability of the achieved results and the Safety Case concept in the context of multi-modal transport. It examines how the maritime and land-mobile community could directly draw benefits from these developments.

Recent investigations led by the European Commission and the European GNSS Secretariat have identified how the maritime community is organised through the International Maritime Organisation (IMO) to deal with aspects such as safety. At the same time it became clear that for land-mobile users such international organisations for co-ordination do not yet exist (see also Section 3.4).

The following considerations will, therefore, mainly concentrate on the maritime area. However, it can be assumed that, in general, parallels can be drawn between the applications for maritime and land-mobile users.

10.2 __MARITIME TRANSPORT__

The International Maritime Organisation (IMO) promotes the use of a Formal Safety Assessment (FSA) [PEACHEY, 1998]. The objective of this assessment is to provide reliable information to support the decision making process at IMO related to the development of improved regulations. The FSA is formally structured into five steps:

1. The identification of hazards;
2. The assessment of risks associated with those hazards;
3. Options for reducing the risks identified;
4. Cost benefit assessment of the options identified in 3;
5. Decisions on which options to select.

The first three of these five steps can easily be related to the Safety Case concept presented in Chapter 9 and in particular to the risk model displayed in Figure 27. Hazard identification is proposed to be carried out for civil aviation applications at the level of the provision of the navigation service and the air traffic service, followed by an assessment of the associated risks. This allows the determination of the total level of risk, which needs to be achieved in order to meet the Target Level of Safety. If the process in its first iteration reveal that the target cannot be met, options for reducing

the risk have to be identified. At this stage the FSA of the IMO goes a step further by introducing a cost benefit assessment before the decision making process. This differs from the aviation approach where the complexity and ultimate priority of safety-related issues introduces severe difficulties in many cases to carry out comprehensive and meaningful cost benefit analyses. However, until this step, a high level of similarity can be identified between the Safety Case concept proposed for aviation and the IMO FSA.

This consequently leads to the conclusion that the presented results and the proposed Safety Case approach could be encompassed by existing procedures already adopted by the maritime community. In particular the identification of hazards which are exclusively related to satellite navigation are relevant to both modes of transport. The risk reduction or mitigation measures which will be implemented for different operational applications will differ, but they can all be based on the initial hazard identification. This would therefore be the stage at which the Safety Cases would start to differ. However, the same concept for their development could be followed.

The maritime community has recently been presented informally with the current activities of the aviation sector and felt that the approach covers, in general, their needs. However, the requirements which are placed on aviation for safety regulation appeared as a whole as being too stringent for maritime applications. This would lead to the conclusion that what has been proposed herein for aviation covers more than what is required for maritime applications and could easily be re-used for the maritime sector.

10.3   LAND TRANSPORT

The requirements that the terrestrial transport sector would have towards information about GNSS failures and the associated hazard identification as input into a regulatory regime are difficult - if not impossible - to identify. This may be due to the fact that currently no operations directly concerning the safety of life are critically dependent on satellite navigation.

This transport sector is highly dispersed and no central organisation exists which represents it. This is, *inter alia*, due to the fact that regulation is very much handled within each individual State; and it was only recently that co-ordination across borders started on a larger scale for rail applications, for example. However, evidence exists that for rail applications in the UK concepts similar to the proposed Safety Case are applied   [HSE, 1996]. If rail transport were to introduce operations where satellite

navigation would be a safety critical contributor, it can consequently be assumed that the results generated for civil aviation in combination with the Safety Case concept can be applied.

These results and concepts developed herein are also available to the road transport community for consideration. Closer links to the developments for the other modes of transport may be sought as and when satellite navigation was included in safety-critical services, and in which the issue of liability arises and regulation is required.

11. <u>CONCLUSIONS</u>

In order to contribute to resolving the problem of restricted approvals of satellite navigation for operational use in civil aviation, a unique attempt was made to exhaustively evaluate and describe satellite navigation performance in the operational environment of commercial airliners through a scientific-technical approach. A total system concept was developed in order to progress the operational approval of satellite navigation applications in civil aviation. For the first time, parameters describing the Required Navigation Performance (RNP) were combined with those describing the performance of satellite navigation. The developed set of parameters established the basis for an exhaustive system evaluation comprising a unique flight trial programme – involving a wide-body airliner –, the development of a world-wide unique database and the subsequent data evaluation process. The overall aim was to demonstrate with a high level of confidence to what extend GPS RAIM could satisfy the developed set of requirements. With the proposal of a Safety Case concept, a methodology was developed and provided which would allow to demonstrate that operations based on satellite navigation can be approved as safe for the operational use in civil aviation.

The following sections summarise the major conclusions which can be drawn from the findings of the performance evaluation of satellite navigation and the Safety Case Development.

11.1 PERFORMANCE EVALUATION

A set of parameters describing the Required Navigation Performance was established. They provide a consistent input into the performance evaluation process.

1. Qualifiers have been developed to describe in practical terms Accuracy, Integrity, Availability and Continuity of Service for the implementation into the data evaluation tools.

2. The required Accuracy was available for all visibility scenarios and during all phases of flight. This reduced the need to investigate the Availability of the navigation service in favour of the Availability of the Integrity function.

3. No situation occurred where RAIM Detection was not available due to the fact that less than five satellites were predicted to be visible.

4.   When detection was declared reliable for the RAIM algorithms, detection did never occur and no faulty satellite signal was identified.

5.   The prediction of the system performance showed that FD Availability and the FDI Availability were met by un-aided RAIM only during En-route and Terminal phases of flight. Baro-aiding allowed to meet the requirements during the more demanding phases of flight for the theoretical visibility scenario. The dynamic environment during Departure, Initial and Final Approach showed a major impact, in particular, on the RAIM FDI Availability.

6.   This predicted performance was confirmed by the results achieved through two independent RAIM algorithms. The FD Availability requirement was met for the En-route and Terminal phases of flight without baro-aiding, but it required baro-aiding to fulfil the requirement during the more demanding phases of flight. These algorithm results were limited to Failure Detection, because the algorithms were never required to switch into Identification mode.

7.   A high degree of correlation can be observed between the results for two types of RAIM algorithms. This, on one hand, validates that their behaviour and performance is highly comparable; on the other hand, it verifies the correct implementation of the algorithms.

8.   Only one case existed where the maximum allowable outage duration of 300 seconds was exceeded during an en-route phase of flight. This problem was immediately solved when using the algorithms in their baro-aided implementation.

9.   The results obtained using the GNSS error simulator provided the evidence for the correct functioning of the algorithm when errors occur onboard the satellites. It was also demonstrated that the algorithms could handle double satellite errors.

10.   The 'early warning' capabilities of the algorithms demonstrated that the Horizontal Alert Limit was never exceeded and, therefore, any alarm was raised within the specified Time-to-Alarm.

11.2   SAFETY CASE DEVELOPMENT

1.   The concept of the Safety Case was developed as a means to facilitate the approval of operations based on GNSS in civil aviation.

2.   A Risk Model is proposed which propagates potential GNSS failures along an escalation path until they may lead to a fatal accident. It is shown how mitigation measures - as a series of barriers preventing a system failure escalating into a fatal accident - can ensure that the application of GNSS does not exceed the fraction of the Target Level of Safety which was assigned to it.

3.   A model of a hazard identification tree has been developed together with the associated hazard assessment in order to demonstrate the practical application of the Risk Model to the GNSS.

4.   All tools used to deliver any safety-relevant data have been developed following rules for producing 'High Quality' Software. Applying these standards for software development and quality assurance allows the Dutyholder to demonstrate that he has done everything which is 'reasonably practicable' to ensure himself and the Regulator about the correctness of his findings.

5.   Two different RAIM algorithms have been independently tested and implemented. They deliver throughout the data evaluation process similar results, which justifies that the obtained results can be considered as having a very high level of confidence.

6.   Investigations into the multi-modal applicability of the proposed Safety Case concept revealed that the concept would exceed the requirements that maritime users may have for their applications. It was felt that the concept would also be of benefit for terrestrial users, as and when they would start looking into safety-critical operations being dependent on GNSS.

11.3   SUMMARY

In summary, evidence is provided that satellite navigation can be approved as safe for operational use in civil aviation, considering that an augmentation such as baro-aiding may be at least required during the more demanding phases of flight. Two independent RAIM algorithms were implemented to confirm the results and a GNSS error simulator was used to provide additional evidence about the correct behaviour of the algorithms. It was argued that the areas of the Earth covered by the flight trials provided geographically representative data. However, saturation graphs showed that an increasing amount of data would improve the confidence level to be placed on the results. The following final chapter derives a number of recommendations from the obtained results.

12. **RECOMMENDATIONS**

This chapter lists a number of recommendations which are drawn from the results presented in Chapter 8, the Safety Case Development in Chapter 9 and the conclusions drawn in Chapter 11.

1. On frequent occasions it became evident that the GPS receiver-dependent choice of eight satellites out of potentially more than the 8 visible satellites was not optimal for RAIM. However, this particular receiver was designed for supplemental means according to TSO C-129 C3. Any future data recording campaign should use all-in-view receivers.

2. The results reveal that baro-aiding may not be a sufficient augmentation to achieve the required RAIM FD and FDI performance in the dynamic environment of an aircraft during the more demanding phases of flight (Departure, Initial and Final Approach). This statement is based on simulations which used a very conservative model for the aircraft and antenna reception pattern. In reality it was observed that satellites were regularly received until -20° in elevation in the body-fixed co-ordinate system. It can be expected that RAIM FDI may turn out to perform better under these conditions. In order to obtain an improved correlation between practice and theory it is recommended to improve on the aircraft antenna reception model implemented in this study. However, at the same time a study should be carried out to investigate the quality of signals which are received form such low elevation angles since it is suspected that they have travelled along the aircraft's skin.

3. The fact that the required RAIM performance during the more demanding phases of flight could not clearly be achieved, highlights the need to extend performance prediction and data evaluation to further potential augmentation systems such as Inertial Reference Systems and EGNOS. This would also be an opportunity to define appropriate requirements for the constellation of Galileo satellites.

4. The findings concerning the saturation of the statistical results and the required fundamental set of data demonstrated that, for Departure, Initial and Final Approach phases of flight in particular, more data are required, while the results for En-route and Terminal showed a reasonably small bandwidth in their variations. It would be desirable to increase the scope of information

contained in the database by obtaining data from short-haul aircraft. This would considerably increase the amount of available data during the more demanding phases of flight.

5.   In order to determine the probability of position errors resulting from the different branches of the hazard identification tree, thorough investigations using a positioning reference system need to be carried out. This would result in the hazard identification tree being sufficiently well populated with the relevant probabilities and frequencies.

6.   Such a positioning reference system could also support an investigation to check whether errors did, in fact, occur even though the RAIM algorithms had declared everything as being within specifications. Assuming that this work progressed towards Precision Approach applications, the reference system could also be used to determine the contribution of the Navigation System Error and the Flight Technical Error to the Total System Error as an input into operational procedure design and auto-pilot layout.

7.   Once the GNSS hazard identification tree has been fully established so that it describes all potential hazards and their frequencies, it would be the task of the ATS providers to base their ATS Safety Case on this input. They could then establish any procedural or mitigation measures (e.g. conditions for operational approval) necessary to achieve the Target Level of Safety which is required from the overall ATS provision.

8.   During the Safety Case development for aviation applications contact should be sought with other modes of transport to involve them from an early stage and to facilitate their process of re-using elements of the Safety Case to their own purposes.

REFERENCES

[1]   BRENNER, M.: *Implementation of a RAIM Monitor in a GPS Receiver and an Integrated GPS/IRS*; ION GPS-90, Colorado Springs, September 1990

[2]   BRENNER, M.: *An Integrity Monitoring Scheme for Precision Approach Applications*; ION GPS-96, Kansas City, September 1996

[3]   BRENNER, M.: *Integrated GPS/Inertial Fault Detection Availability*; Navigation, Vol. 43, No. 2, Summer 1996, pp. 111-130

[4]   BREEUWER, E.; FARNWORTH, R.; TIEMEYER, B.; WATT, A.: *GNSS-1 Performance Specification and Validation for Civil Aviation*; ION GPS-98, Nashville, September 1998

[5]   BROWN, A.: *A Multi-Sensor Approach to Assuring GPS Integrity*; Radio Technical Commission for Aeronautics, 1989 Annual Assembly Meeting, Washington, December 1989

[6]   BROWN, A.: *Receiver Autonomous Integrity Monitoring Using A 24-Satellite GPS Constellation*; ION National Technical Meeting, January 1990

[7]   BROWN, A.; STURZA, M.: *The Effect of Geometry on Integrity Monitoring Performance*; Institute of Navigation Annual Meeting, June 1990

[8]   BROWN, A.; KING, J.; SPALDING, J.: *Differential GPS Autonomous Failure Detection*; ION GPS-91, Albuquerque, September 1991

[9]   BROWN, R.A.; HALL, R.O.; ROMRELL, G.K.; WAID J.D.: *RAIM Availability for CAT IIIb Operation*; Institute of Navigation 51st Annual Meeting, Colorado Springs, CO, June 1995

[10]   BROWN, R.G.; Chin, G.Y.; Kraemer, J.H.: *Update on GPS Integrity Requirements of the RTCA MOPS*; ION GPS-91, Albuquerque, NM, September 1991

[11]   BROWN, R.G.: *A Baseline RAIM Scheme and a Note on the Equivalence of Three RAIM Methods*; ION National Technical Meeting, San Diego, California, January 1992

[12] BROWN, R.G.: *Receiver Autonomous Integrity Monitoring*; Global Positioning System: Theory and Applications, American Institute of Aeronautics and Astronautics, Vol. II, 1993, pp. 142-165

[13] BROWN, R.G.; KRAEMER, J.H.; NIM G.C.: *Comparison of FDE and FDI RAIM algorithms for GPS*; ION National Technical Meeting, San Diego, California, January 1994

[14] BROWN, R.G.; KRAEMER, J.H.; NIM G.C.*: A Partial Identification Algorithm for GPS Sole Means Navigation*; ION GPS-94, Salt Lake City, September 1994

[15] BROWN, R.G.: *GPS RAIM: Calculation of Thresholds and Protection Radius Using Chi-Square Methods - A Geometric Approach*; RTCA Paper No. 491-94/SC159-584, November 1994

[16] Chin, G.Y.; Kraemer, J.H.; BROWN, R.G.: *GPS RAIM: Screening out Bad Geometries under Worst-Case Bias Conditions*; Institute of Navigation 48th Annual Meeting, Washington, D.C., June 1992

[17] CONLEY, R.; WILFONG, A.: *The Design and Application of a GPS Integrity Model*; ION GPS-91, Albuquerque, NM, September 1991

[18] CULLEN: *The Public Inquiry into the Piper Alpha Disaster*; The Hon Lord Cullen, Vol. 1 & 2, Department of Energy, ISBN 0 10 113102, 1990

[19] DALY, P.; MISRA, P.N.: *GPS and Global Navigation Satellite System (GLONASS)*; Global Positioning System: Theory and Applications, American Institute of Aeronautics and Astronautics, Vol. II, 1995, pp. 243-272

[20] DEUTSCH, M.S.; WILLIS, R.R.: *Software Quality Engineering*; Prentice-Hall Inc., 1988

[21] FERNOW, J.; LEE, Y.C.: *Analyses Supporting FAA Decisions Made During The Development of Supplemental GPS Avionics Requirements*; Navigation, Vol. 41, No. 4, 1994-95, pp. 463-477*

[22] HEIN, G.W.; EISFELLER, B.; PIELMEIER, J.F.X.: *GPS RAIM Availability in ECAC Airspace - Study Report*; IfEN University FAF Munich, July 1997

[23] HINSON, D.R.: Letter from the Administrator, United States Federal Aviation Administration, to Dr. Assad Kotaite, President of the ICAO Council, Washington DC, 14 September 1994

[24] KELLY, R.J.; DAVIS, J.M.: *Required Navigation Performance (RNP) for Precision Approach and Landing with GNSS Applications*; Navigation, Vol. 41, No 1, Spring 1994

[25] KELLY, R.J.: *Derivation of the RAIM Algorithm from First Principles with Performance Comparisons between Published Algorithms*; ION National Technical Meeting, Santa Monica, January 1996

[26] KOTAITE, A.: Address by the President of the ICAO Council to GLOBAL NAVCOM '96, Singapore, 4 June 1996

[27] LEE, Y.C.: *Analyses of Use of Receiver Autonomous Integrity Monitoring (RAIM) Capability for Sole-Means GPS Navigation in the Oceanic Phase of Flight*; IEEE AES Magazine, May 1992, pp. 29-36

[28] LEE, Y.C.: *Analyses of RAIM Function Availability of GPS Augmented with Barometric Altimeter Aiding and Clock Coasting*; ION GPS-92, September 1992

[29] LEE, Y.C.: *Analyses of Use of Receiver Autonomous Integrity Monitoring (RAIM) in a GPS Wide-Area Augmentation System (WAAS)*; ION National Technical Meeting, San Diego, California, January 1994

[30] LEE, Y.C.: *Receiver Autonomous Integrity Monitoring Availability for GPS Augmented with Barometric Altimeter Aiding and Clock Coasting*; Global Positioning System: Theory and Applications, American Institute of Aeronautics and Astronautics, Vol. II, 1994, pp. 221-242

[31] LEE, Y.C.: *New Techniques Relating Fault Detection and Exclusion Performance to GPS Primary Means Integrity Requirements*; ION GPS-95, September 1995

[32] LEE, Y.C., ET AL.: *Summary of the RTCA SC-159 GPS Integrity Working Group Activities*; ION National Technical Meeting, Santa Monica, California, January 1996 & Navigation, Vol. 43, No. 3, 1996, pp. 307-338

[33] LIPP, A.; BONDARENCO, N.; TIEMEYER, B.; DOLCETTI, A.; AVANZI, G.: *Satellite Navigation Antenna Performance on Transport Aircraft*, GNSS'99, Third European Symposium on Global Navigation Satellite Systems, 5-8 October 1999, Genoa, Italy

[34] MCDAVID, T.; MURPHY, T.; SOTOLONGO, G.: *GPS/IRS/FMS Integration for RNP Airspace Operations*; ION National Technical Meeting, Anaheim, CA, January 1995

[35] PARKINSON, B.W.; AXELRAD, P.: *Autonomous GPS Integrity Monitoring Using the Pseudorange Residual*; Navigation, Vol. 35, No. 2, 1988, pp. 255-274

[36] PARKINSON, B.W.; STANSELL, T.; BEARD, R.; GROMOV, K.: *A History of Satellite Navigation*; Navigation, Vol. 42, No. 1, Special Issue, 1995, pp. 109-164

[37] PEACHEY, J.H.: *FSA Methodology*; Special Presentation on Formal Safety Assessment, IMO, London, November 1998

[38] ROBENS: *Safety and Health at Work*, Report of the Committee 1970-72, Lord Robens Chairman, Cmnd 5034

[39] SHARKEY, S.; JOHANNESSEN, R.: *Reliability Performance in GPS Receivers, the Nature of Their Failures and Planning to Live with Realistic Failure Rates in Satellite Navigaion System Receivers*; NAV 96, London, November 1996

[40] SHIENOK, N.N.: *GLONASS Status and Prospects for Development and International Application*; Co-ordinational Scientific Information Center Russian Space Forces, 1997

[41] SOLAT, N.: *Information provided to the author by the FAA representative in Europe on the probability of two GPS outages*; May 1996

[42] STRACHAN, V.F.: *The Global Positioning System as a Sole Means of Navigation*; Civil Avionics '97 Conference, January 1997

[43] STURZA, M.A.: *Navigation System Integrity Monitoring Using Redundant Measurements*; Navigation, Vol. 35, No. 4, 1988-89, pp. 483-501

[44] STURZA, M.A.; BROWN A.K.: *Comparison of Fixed and Variable Threshold RAIM Algorithms*; ION GPS-90, Colorado Springs, September 1990

[45] STURZA, M.A.: *Fault Detection and Isolation (FDI) Techniques for Guidance and Control Systems*; AGARDOGRAPH No. 314, AGARD, NATO, 1991

[46] TIEMEYER, B; WATT, A.; BONDARENCO, N.: *SAPPHIRE - How does GNSS perform onboard Commercial Airliners? -* ; ION GPS-96, Kansas City, Missouri, U.S.A., September 1996

[47] TIEMEYER, B.; WATT, A.; FARNWORTH, R.: *Can GNSS be certified for Civil Aviation?*, ION GPS-96, Kansas City, Missouri, U.S.A., September 1996

[48] TIEMEYER, B.; WATT, A.; FLETCHER, P.; COTTAM, M.: *GNSS Space System Safety Case - Results of an Impact Study*, GNSS '97, 22-25 April 1997, Munich, Germany

[49] TIEMEYER, B.; WATT, A.; BONDARENCO, N; DENSKAT, U.; HENZLER, J.: *SAPPHIRE or how to evaluate GNSS Performance Onboard of Commercial Airliners*, GNSS '97, 22-25 April 1997, Munich, Germany

[50] TIEMEYER, B.; FARNWORTH, R.; JOHNSTONE, A.; BRENNAN, G.: *Development of the EGNOS Safety Case*, ESREL '99, European Safety and Reliability Conference, September 1999, Munich, Germany

[51] TIEMEYER, B.; FARNWORTH, R.; JOHNSTONE, A.; GILMARTIN, B.: *The EGNOS Safety Case – Setting the Safety Standard & Current Status*, ESREL 2000, European Safety and Reliability Conference, 15-17 May 2000, Edinburgh, UK

[52] VAN DYKE, K.L.: *RAIM Availability for Supplemental GPS Navigation*; Navigation, Vol. 39, No. 4, 1992-93, pp. 429-443

[53] VAN DYKE, K.L.: *Fault Detection and Exclusion Performance Using GPS and GLONASS*; Navigation, Vol. 42, No. 4, 1995, pp. 581-595

[54] VAN GRAAS, F.; FARRELL, J.L.: *Receiver Autonomous Integrity Monitoring (RAIM): Techniques, Performance and Potential*; Institute of Navigation 47th Annual Meeting, Williamsburg, VA, June 1991

[55] VAN GRAAS, F.: *Signals Integrity*; NATO/AGARD, Lecture Series No. 207, System Applications and Innovative Application of Satellite Navigation, July 1996

[56] WATT, A.; STOREY, J.: *The Technical Implementation of a Common European Programme for Satellite Navigation*; ION National Technical Meeting, Anaheim, January 1995

[57] WATT, A.: *The Impact of Satellite Navigation on the Airline Industry*; MPhil Thesis, College of Aeronautics, Cranfied University, December 1996

[58] – CEC: *CEC Directive*; 82/501/EEC (Seveso), amended 1987/1988

[59] – EGS/EUROPEAN GNSS SECRETARIAT: *Applications and User Requirements*; Report of the European GNSS Maritime Advisory Forum, MARFOR/WP4/V1.0, 1999

[60] – EUROCONTROL: *EEC Standard for a Software Life-Cycle and its Documentation*; EEC/SEU/ST/0003, Issue 1.0, 1992

[61] – EUROCONTROL: *Area Navigation Equipment - Operational Requirements and Functional Requirements*; EUROCONTROL DOC-003/93, Version 1.0, 1993

[62] – EUROCONTROL: *GNSS Safety Regulation Guidelines*, OCR/DP/053, Issue 5.1, 24 April 1996

[63] – EUROCONTROL: *EEC SAPPHIRE DUAU Interface Control Document 1 - Aircraft Interfaces*; DUAU-TN-2472-003, Issue B, 29 November 1996

[64] - EUROCONTROL: *EEC SAPPHIRE DUAU User Requirements Document*; DUAU-RS-2450-001, Issue K, 1997

[65] – EUROCONTROL: *Future ATM Profile - Capacity Shortfalls in Europe (1996 - 2006)*; EEC Task R13, Draft 1.0, 08 March 1997

[66] – EUROCONTROL: *Civil Aviation Requirements for EGNOS*; Discussion Paper OCR/DP/157, SNA Group / OCR Task Force, July 1998

[67] – EUROPEAN COMMISSION: *Galileo – Global Satellite Navigation Services for Europe*; Brochure, 1999

[68] – FANS(II)/4: *FANS Phase II Report*; ICAO Document 9623, Montreal, September 1993

[69] – ICAO/AWOP: *Report of the 15th Meeting*, All Weather Operations Panel, ICAO, 1994

[70] – ICAO: *Manual on Required Navigation Performance (RNP)*, Doc 9613-AN/937, First Edition, ICAO, 1994

[71] – ICAO: *Report on Proposed Required Navigation Performance (RNP) Concept for Approach, Landing and Departure Operations*, Special Communications/Operations Divisional Meeting, WP11, ICAO, 1995

[72] – ICAO/AWOP: *Report of the 16th Meeting*, All Weather Operations Panel, ICAO, 1997

[73] – ICAO/GNSS: *ICAO Circular - Guidelines for the Introduction and Operational Use of the Global Navigation Satellite System (GNSS)*; Circular 267-AN/159, 1996

[74] – ICAO/GNSSP/WGA/NUMBERS SUB-GROUP: *Draft GNSS Performance Requirements*; South Brisbane, February 1997

[75] – ICAO/GNSSP/3: *Report of the 3rd Meeting*, Global Navigation Satellite Systems Panel, April 1999

[76] – ICAO/SARPs: *Draft ICAO GNSS SARPs*; Version 7.0, September 1998

[77] – JAA/TGL-2: *Temporary Guidance Leaflet No. 2 - JAA Interim Guidance Material on Airworthiness Approval and Operational Criteria for the Use of Navigation Systems in European Airspace Designated for Basic RNAV Operations*; JAA, Final Draft May 1997

[78] – JAA/TGL-3: *Temporary Guidance Leaflet No. 3 - JAA Interim Guidance Material on Airworthiness Approval and Operational Criteria for the Use of the NAVSTAR Global Positioning System (GPS)*; JAA, June 1997

[79] – LLOYD'S REGISTER/EUROCONTROL: *Space System Safety Case*; EUROCONTROL Experimental Centre, Report No. 312, Volume I-III, June 1997

[80] – HSE: *Railway Safety Cases – Guidance on Regulation*; Health & Safety Executive, ISBN 0 7176 0699 6, 1994

[81] – RTCA/DO-208: *Minimum Operational Performance Standards (MOPS) for Airborne Supplemental Navigation Equipment Using Global Positioning System (GPS)*; SC-159, July 1991

[82] – RTCA/DO-217: *Minimum Aviation System Performance Standards DGNSS Instrument Approach System: Special Category I (SCAT-I)*; SC-159, August 1993

[83] – RTCA/DO-229: *Minimum Operational Performance Standards for Global Positioning System / Wide Area Augmentation System Airborne Equipment*; SC159, January 1996

[84] – RTCA/DO-229A: *Minimum Operational Performance Standards for Global Positioning System / Wide Area Augmentation System Airborne Equipment*; SC159, 1998

[85] – TSO-129A: *Airborne Supplemental Navigation Equipment Using the Global Positioning System (GPS)*; DoT, FAA Aircraft Certification Service, Washington DC, July 1996

[86] – TU DELFT/EUROCONTROL: *Technical and Operational Assessment of the Suitability of GPS to meet the BRNAV Requirements*; EUROCONTROL, Report No. REP9706A, June 1997

[87] – U.S. DEPARTMENT OF DEFENSE: *Global Positioning System Standard Positioning Service Signal Specification*; 2nd Edition, 02 June 1995

ANNEX A - DEFINITIONS

Accuracy	Given Service Reliability, the percentage of time over a specified time interval that the difference between the measured and expected user position or time is within a specified tolerance at any point on or near the Earth. [U.S. DoD, 1995]
Accuracy	The degree of conformance between the estimated or measured position and/or velocity of a platform at a given time and its true position and/or velocity. Radio navigation accuracy is usually presented as statistical measure of system error and is specified as:

a) *Predictable*. The accuracy of a position with respect to the geographic or geodetic co-ordinates of the Earth;

b) *Repeatable*. The accuracy with which the user can return to a position whose co-ordinates have been measured at a previous time with the same navigation system; and

c) *Relative*. The accuracy with which a user can determine one position relative to another position regardless of any error in their true positions. [ICAO/GNSS, 1996]

Availability	The availability of a navigation system is the percentage of time that the services of the system are usable. Availability is an indication of the ability of the system to provide usable service within the specified coverage area. Signal availability is the percentage of time that navigational signals transmitted from external sources are available for use. Availability is a function of both the physical characteristics of the environment and the technical capabilities of the transmitter facilities. [ICAO/GNSS, 1996]
Coverage	The percentage of time over a specified time interval that a sufficient number of satellites are above a specific mask angle and provide an acceptable position solution geometry at any

point on or near the Earth. [U.s. DoD, 1995]

GNSS Accuracy   The degree of conformance between the GNSS output of position and time and the true position and time. [Icao/Gnss, 1996]

GNSS Continuity   The probability that the GNSS will be available for the duration of a phase of operation, presuming that the GNSS was available at the beginning of that phase of operation. [Icao/Gnss, 1996]

GNSS Fault Detection and Isolation (FDI)   A combination of internal and external integrity monitoring which will identify any source of error in GNSS navigation signals and negate the effect within the system. [Icao/Gnss, 1996]

GNSS Integrity   The assurance that all functions of the system perform within GNSS operational performance limits. [Icao/Gnss, 1996]

Integrity   The ability of a system to provide timely warnings to the users when the system should not be used for navigation. [Icao/Gnss, 1996]

Primary-Means Navigation System   A navigation system approved for a given operation or phase of flight that must meet accuracy and integrity requirements, but need not meet full availability and continuity of service requirements. Safety is achieved by limiting flights to specific time periods and through appropriate procedural restrictions.

Note. - There is no requirement to have a sole-means navigation system onboard to support the primary-means system. [Icao/Gnss, 1996]

Service Availability   Given Coverage, the percentage of time over a specified time interval that a sufficient number of satellites are transmitting a usable ranging signal within view of any point on or near the Earth. [U.s. DoD, 1995]

Service Reliability   Given Service Availability , the percentage of time over a specified time interval that the instantaneous predictable horizontal error is maintained within a specified reliability

threshold at any point on or near the Earth. Note that Service Reliability does not take into consideration that reliability characteristics of the SPS receiver or possible signal interference. Service Reliability may be used to measure the total number of major failure hours experienced by the satellite constellation over a specified time interval. [U.s. DoD, 1995]

Sole-Means Navigation System

A sole-means navigation system approved for a given operation or phase of flight must allow the aircraft to meet, for that operation or phase of flight, all four navigation system performance requirements: accuracy, integrity, availability and continuity of service.

Note. - This definition does not exclude the carriage of other navigation systems. Any sole-means navigation system could include one (stand-alone installation) or several sensors, possibly of different types (multi-sensor installation). [ICAO/GNSS, 1996]

Supplemental-Means Navigation System

A navigation system that must be used in conjunction with a sole-means navigation system. Approval for supplemental-means for a given phase of flight requires that a sole-means navigation system for that phase of flight must be onboard. Amongst the navigation system performance requirements for a given operation or phase of flight, a supplemental-means navigation system must meet the accuracy and integrity requirements for that operation or phase of flight; there is no requirement to meet availability and continuity requirements.

Note. - Operationally, while accuracy and integrity requirements are met, a supplemental-means system can be used without any cross-check with the sole-means system. Any navigation system approved for supplemental-means could involve one (stand-alone installation) or several sensors possibly of different types (multi-sensor installation). [ICAO/GNSS, 1996]

ANNEX B - ABBREVIATIONS

AAIM	Aircraft Autonomous Integrity Monitoring
ACC	Air Traffic Control Centre
ADD	Architectural Design Document
ADF	Automatic Direction Finder
ALARP	As Low As Reasonable Practical
APL	Applied Physics Laboratory
ATC	Air Traffic Control
ATFM	Air Traffic Flow Management
ATM	Air Traffic Management
ATS	Air Traffic Service
AWOP	All Weather Operations Panel
BRNAV	Basic Area Navigation
C/A	Course Aquisition
CFAR	Constant False Alarm Rate
CFIT	Controlled Flight Into Terrain
CNS	Communications, Navigation and Surveillance
CPOD	Constant Probability Of Detection
DDD	Detailed Design Document
DME	Distance Measurement Equipment
DoD	Department of Defense
EC	European Commission
ECAC	European Civil Aviation Conference
EGNOS	European Geostationary Navigation Overlay Service
ESA	European Space Agency
FAA	Federal Aviation Authority
FANS	Future Air Navigation System
FDMA	Frequency Division Multiple Access
FDI	Failure Detection & Isolation
FSA	Formal Safety Assessment
FTE	Flight Technical Error
GBAS	Ground Based Augmentation System
GLONASS	Global Orbiting Navigation Satellite System
GNSS	Global Navigation Satellite System
GNSSP	Global Navigation Satellite System Panel
GPS	Global Positioning System

HCI	Human-Computer Interaction
HDOP	Horizontal Dilution Of Precision
ICAO	International Civil Aviation Organisation
IEC	International Electro-technical Commission
EGS	European GNSS Secretariat
ILS	Instrument Landing System
INS	Inertial Navigation System
IMO	International Maritime Organisation
ITD	Integration Test Document
ITP	Integration Test Plan
JAA	Joint Aviation Authorities
MSAS	Multi-transport Satellite based Augmentation System
MTBF	Mean Time Between Failure
NAVSTAR	Navigation Satellite Time And Ranging
NDB	Non-Directional Beacon
NPA	Non-Precision Approach
NSE	Navigation System Error
PA	Precision Approach
PDOP	Position Dilution Of Precision
PPS	Precise Positioning Service
PRN	Pseudo Random Code
RAIM	Receiver Autonomous Integrity Monitoring
RNP	Required Navigation Performance
RTCA	RTCA Inc.
SA	Selective Availability
SARPs	Standards and Recommended Practices
SATP	Software Acceptance Test Plan
SBAS	Space Based Augmentation System
SC	Safety Case
SCMP	Software Configuration Management Plan
SITP	Software Integration Test Plan
SPS	Standard Positioning Service
SQAP	Software Quality Assurance Plan
SRC	Safety Regulation Commission
SRD	Software Requirements Document
STD	Software Transfer Document
SUM	Software User Manual
SUTP	Software Unit Test Plan
SVD	System Validation Document
TGL	Temporary Guidance Leaflet

TLS	Target Level of Safety
TSE	Total System Error
TSO	Technical Standard Order
URD	User Requirements Document
UTC	Universal Time Co-ordinated
UTD	Unit Test Document
UTP	Unit Test Plan
VDOP	Vertical Dilution Of Precision
VLF	Very Low Frequency
VOR	Very High Frequency Omni-Directional Range
WAAS	Wide Area Augmentation System
WGS	World Geodetic System

ANNEX C - GPS PERFORMANCE STANDARD

Coverage Standard	Conditions and Constraints
≥ 99.9% global average	• Probability of 4 or more satellites in view over any 24 hour interval, averaged over the globe • 4 satellites must provide PDOP of 6 or less • 5° mask angle with no obscura • Standard is predicated on 24 operational satellites, as the constellation is defined in the almanac
≥ 96.9% at worst-case point	• as above
Service Availability Standard	**Conditions and Constraints**
≥ 99.85% global average	• Conditioned on coverage standard
≥ 83.87% at worst-case point on worst-case day	• as above • Standard based on a worst-case 24 hour interval, for the worst-case point on the globe
Service Reliability Standard	**Conditions and Constraints**
≥ 99.97% global average	• Conditioned on coverage and service availability standards • 500 meter Not-to-Exceed (NTE) predictable horizontal error reliability threshold • Standard based on a measurement interval of one year; average of daily values over the globe • Standard predicated on a maximum of 18 hours of major service failure behaviour over the sample interval
≥ 99.79% single point average	• as above • Standard based on a measurement interval of one year; average of daily values from the worst-case point on the globe
Accuracy Standard	**Conditions and Constraints**
≤ 100 m horizontal error 95% of time ≤ 156 m vertical error 95% of time ≤ 300 m horizontal error 99.99% of time ≤ 500 m vertical error 99.99% of time	• Conditioned on coverage, service availability and service reliability standards • Standard based on a measurement interval of 24 hours, for any point on the globe.

Table 20: GPS SPS Minimum Performance Standards [U.s. DoD, 1995]

ANNEX D - ONBOARD DATA RECORDING

GPSSU DIGITAL DATA OUTPUT[5] (GENERAL DATA CHARACTERISTICS; DOC-No 465111-17 Table 2)							
Label	Parameter	Unit	Range	Sig. Bits	Resolution	Update Rate	ADRAS™ Parameter
060	Measurement Status - Satellite PRN Number - Operation Mode - Measurement Status - Carrier to Noise Ratio	N/A	N/A	8x N/A	N/A	1 Hz	SVNx[6] OPMx Msx CNOx
061	Pseudo Range	m	268435456	8x 23	256 m	1 Hz	PRC
062	Pseudo Range Fine	m	256	8x 14	0.125 m	1 Hz	PRF
063	Range Rate	ms^{-1}	4096	8x 23	$0.0039\ ms^{-1}$	1 Hz	RR
064	Delta Range	m	4096	8x 23	0.0039 m	1 Hz	DR
074	UTC Meas. Time	s	10	8x 23	0.0000095*4* s	1 Hz	GUTC
076	GPS Altitude	ft	131072	23	0.125 ft	1 Hz	GALT
101	HDOP	N/A	1024	18	0.031*25*	1 Hz	HDOP
102	VDOP	N/A	1024	18	0.031*25*	1 Hz	VDOP
110	GPS Latitude	1°	±180	23	$1.7166°*10^{-4}$	1 Hz	GLAT
111	GPS Longitude	1°	±180	23	$1.7166°*10^{-4}$	1 Hz	GLON
120	GPS Lat Fine	1°	±0.000172	14	$8.381903°*10^{-8}$	1 Hz	GLATF
121	GPS Long Fine	1°	±0.000172	14	$8.381903°*10^{-8}$	1 Hz	GLONF
130	Horizont. Int. Limit	NM	16	21	$6.1004*10^{-5}$	1 Hz	HINTL
140	UTC Fine	s	1.0	23	$9.5*10^{-7}$ s	1 Hz	UTCF
141	UTC Fine Fraction	s	$9.5*10^{-7}$	13	$9.3132*10^{-10}$ s	1 Hz	UTCFF
150	UTC	hr:min:s	23:59:59	20	1 s	1 Hz	UTC ...
260	Date	d:m:yr	N/A	9	1 day	1 Hz	...day ...month ...year
273	GPS Sensor Status	N/A	N/A	22	N/A	1 Hz	SATT SATV GMODE

Table 21: GPSSU Data Recording Format

---

[5] Almanach, Ephemeris and correction parameters transmitted by the GPS satellites have to be collected from separate sources.

[6] For clarification: SVNx represents the **PRN** numbers which are also used in the Ephemeris data format.

ADIRU / IR BINARY/BCD DIGITAL OUTPUT (GENERAL DATA CHARACTERISTICS; DOC-No 463861 Table 5.2.1.1-3/4/5)							
Label	Parameter	Unit	Range	Sig. Bits	Resolution	Update Rate	ADRAS™ Parameter
150	UTC (GPS / A/C)	hr:min:s	23:59:59	20	1 s	1 Hz	ACUTC ...
270	IR Discrete Word #1	N/A	N/A	22	N/A	1 Hz	IRDISC
275	IR Discrete Word #2	N/A	N/A	22	N/A	1 Hz	IRDIS2/ DARID
310	Pres Pos - Lat	1°	±180	23	$1.7166° \times 10^{-4}$	1 Hz	LATP
311	Pres Pos - Lon	1°	±180	23	$1.7166° \times 10^{-4}$	1 Hz	LONP
312	Ground Speed	kn	±4096a	18	0.125 kn	16 Hz	GS
313	Track Angle True	1°	±180	18	0.0054931 6°	16 Hz	TRK
314	True Heading	1°	±180	18	0.0054931 6°	1 Hz	THDG
315	Wind Speed	kn	±256a	18	0.0078125 kn	1 Hz	WS
316	Wind Direct True	1°	±180	18	0.0054931 6°	1 Hz	WD
324	Pitch Angle	1°	±180	18	0.0054931 6°	1 Hz	PTCH
325	Roll Angle	1°	±180	18	0.0054931 6°	1 Hz	ROLL
326	Body Pitch Rate	$1°s^{-1}$	±128	18	$0.00390625°s^{-1}$	16 Hz	PTCR
327	Body Roll Rate	$1°s^{-1}$	±128	18	$0.00390625°s^{-1}$	16 Hz	ROLR
330	Body Yaw Rate	$1°s^{-1}$	±128	18	$0.00390625°s^{-1}$	16 Hz	YAW
331	Body Longit Accel	g	±4	18	0.00012207 g	16 Hz	LONG
332	Body Lateral Accel	g	±4	18	0.00012207 g	16 Hz	LATG
333	Body Normal Accel	g	±4	18	0.00012207 g	16 Hz	VRTG
361	Inertial Altitude	ft	±131072	23	0.125 ft	1 Hz	IALT
365	Inertial Vertic.Speed	$ft\ min^{-1}$	±32768	18	$1.00\ ft\ min^{-1}$	16 Hz	IVV

Table 22: ADIRU/IR Data Recording Format

ADIRU / ADR BINARY/BCD DIGITAL OUTPUT							
(GENERAL DATA CHARACTERISTICS; DOC-No 463861 Table 6.2.1.1-1/2)							
Label	Parameter[7]	Unit	Range	Sig. Bits	Resolution	Update Rate	ADRAS™ Parameter
~~203~~	~~Altitude(1013.25 mb)~~	ft	131071	20	1 ft	1 Hz	ALT
~~205~~	~~Mach~~	M	4.096	19	0.0000625	1 Hz	MN
~~206~~	~~Computed Airspeed~~	kn	1023.75	17	0.0625	1 Hz	CAS
~~210~~	~~True Airspeed~~	kn	2048	18	0.0625 kn	1 Hz	TAS
211	Total Air Temp	°C	511.75	14	0.125 °C	1 Hz	TAT
~~213~~	~~Static Air Temp~~	°C	511.97	14	0.125 °C	1 Hz	SAT
241	Corr Angle of Attack	1°	±180	15	0.0439453°	1 Hz	AOA
242	Total Pressure	mb	2047.97	21	.0078125mb	1 Hz	PT
246	Corr Average Static Pressure	mb	2047.97	21	.0078125mb	1 Hz	PSTAT
270	ADR Discrete Word#1	N/A	N/A	22	N/A	1 Hz	ADISC

Table 23: ADIRU/ADR Data Recording Format

---

[77] Parameters contained in Label 211, 242 and 246 have to be recorded as minimum. Formulae can be provided to calculate the other parameters. For cross-check purposes it would be desirable to record all parameters as given in this table.

CURRICULUM VITAE

NAME	Bernd Tiemeyer
DATE OF BIRTH	19. November 1965
PLACE OF BIRTH	Herford, Germany

EDUCATION

Aug 1972 – Jun 1976	Grundschule (Primary School) Quernheim, Germany
Aug 1976 – May 1985	Freiherr-vom-Stein Gymnasium Bünde, Germany
15. May 1985	Abitur

HIGHER EDUCATION

Oct 1985 – Jun 1991	Studies of Mechanical / Aerospace Engineering Technical University of Braunschweig, Germany
18. Juni 1991	Diplom-Ingenieur (Dipl.-Ing.)

EMPLOYMENT

Jul 1991 – Dec 1994	Research Engineer (Satellite Navigation and Flight Testing) GNSS Engineer delegated to EUROCONTROL from Jan 1994 Institute of Flight Guidance and Control, Technical University of Braunschweig, Germany
Jan 1995 – Aug 1995	GNSS Engineer delegated to EUROCONTROL Avionik Zentrum Braunschweig GmbH, Germany
Sep 1995 - to date	Project Manager, EATMP GNSS Programme Sub-Programme Manager, RVSM Safety EUROCONTROL Experimental Centre, Brétigny s/Orge, France

OTHER

Sep 1991	"Deutsche Lufthansa-Preis 1991" awarded by the "Deutsche Gesellschaft für Luft- und Raumfahrt (DGLR)" for a thesis on integrated Inertial/Satellite Navigation Systems