AGARD-AR-281

AGARD-AR-281

AGARD

ADVISORY GROUP FOR AEROSPACE RESEARCH & DEVELOPMENT

7 RUE ANCELLE 92200 NEUILLY SUR SEINE FRANCE

AGARD ADVISORY REPORT No.281

MAY '90

Technical Evaluation Report on the Guidance and Control Panel 49th Symposium on Fault Tolerant Design Concepts for Highly Integrated Flight Critical Guidance and Control Systems

(Systèmes Tolérants aux Fautes pour les Phases Critiques du Guidage et Pilotage)

NORTH ATLANTIC TREATY ORGANIZATION

DISTRIBUTION AND AVAILABILITY ON BACK COVER

AGARD-AR-281

NORTH ATLANTIC TREATY ORGANIZATION

ADVISORY GROUP FOR AEROSPACE RESEARCH AND DEVELOPMENT

(ORGANISATION DU TRAITE DE L'ATLANTIQUE NORD)

AGARD Advisory Report No.281

TECHNICAL EVALUATION REPORT

on the

GUIDANCE AND CONTROL PANEL 49th SYMPOSIUM

on

Fault Tolerant Design Concepts for Highly Integrated Flight Critical Guidance and Control Systems

(Systèmes Tolérants aux Fautes pour les Phases Critiques du Guidage et Pilotage)

by

Monsieur Bernard Chaillot
Direction des Recherches et Etudes Techniques
(SCDE/CT/DN)
26 boulevard Victor
F-75996 Paris Armées

The Guidance and Control Panel 49th Symposium was held at the Ecole Nationale Supérieure de l'Aéronautique et de l'Espace in Toulouse, France, from 10th to 13th October, 1989.
The papers presented at the Symposium were compiled as Conference Proceedings CP-456.

The Mission of AGARD

According to its Charter, the mission of AGARD is to bring together the leading personalities of the NATO nations in the fields of science and technology relating to aerospace for the following purposes:

— Recommending effective ways for the member nations to use their research and development capabilities for the common benefit of the NATO community;

— Providing scientific and technical advice and assistance to the Military Committee in the field of aerospace research and development (with particular regard to its military application);

— Continuously stimulating advances in the aerospace sciences relevant to strengthening the common defence posture;

— Improving the co-operation among member nations in aerospace research and development;

— Exchange of scientific and technical information;

— Providing assistance to member nations for the purpose of increasing their scientific and technical potential;

— Rendering scientific and technical assistance, as requested, to other NATO bodies and to member nations in connection with research and development problems in the aerospace field.

The highest authority within AGARD is the National Delegates Board consisting of officially appointed senior representatives from each member nation. The mission of AGARD is carried out through the Panels which are composed of experts appointed by the National Delegates, the Consultant and Exchange Programme and the Aerospace Applications Studies Programme. The results of AGARD work are reported to the member nations and the NATO Authorities through the AGARD series of publications of which this is one.

Participation in AGARD activities is by invitation only and is normally limited to citizens of the NATO nations.

The content of this publication has been reproduced
directly from material supplied by AGARD or the authors.

Published May 1990

ISBN 92-835-0559-X

Printed by Specialised Printing Services Limited
40 Chigwell Lane, Loughton, Essex IG10 3TZ

Preface

The trend towards highly integrated systems continues to expand at a rapid rate. Recent examples include automated maneuvering attack systems, flight control/fire control coupling, mission sensor management, real-time armament fuzing and propulsion coupling/performance optimization.

The prospect of improved mission effectiveness through integrated systems is a very real and powerful motivation with far reaching implications. Recent advances in microprocessor technology are bringing about fundamental changes in several traditional functional domains. Specifically, systems architecture requirements, partitioning considerations and functional performance parameters take on new meaning in the context of fully integrated flight critical systems. Effective system integration focuses on end-item functional performance using the most efficient mechanization possible. In this regard, system wide consideration of sensing elements, computational elements and command signalling loops are critically important. Crew station design considerations and the pilot's role must also be thoroughly assessed vis-a-vis varying levels of task automation and overall system wide integrity management requirements.

Achieving the full potential of integrated systems is highly dependent upon demonstrating adequate reliability, safety and survivability. Historical evidence indicates that interfacing subsystems can introduce serious compromises in overall system safety and performance. High integrity software is essential. Satisfying stringent flight critical system requirements necessitates innovative fault tolerant design approaches and mechanization schemes. Adding redundancy levels across the full spectrum of system elements is a self-limiting approach based on practical considerations of weight, volume, cost and supportability. Reconfiguration strategies, graceful degradation and aerodynamic redundancy are but a few of the modern concepts currently under development. State estimation techniques in conjunction with artificial intelligence technology also offer potential fault tolerance enhancements. Blending system elements for fully integrated or multi-purpose usage under both nominal and extreme operating conditions, requires an intensive system integration effort to achieve acceptable levels of fault tolerance.

This symposium focused on advanced fault tolerant design concepts and their practical application to integrated flight critical military systems.

*   *   *

La tendance vers les systèmes hautement intégrés se developpe rapidement. Des exemples récents concernent les manoeuvres automatiques dans la phase d'attaque, le couplage des systèmes de pilotage automatique et de contrôle des armements, les dispositifs permettant la supervision de la mission, la mise à jour automatique d'armes et l'optimisation globale des performances par inclusion du contrôle de la propulsion.

La perspective d'une amélioration de l'efficacité d'une mission grâce à l'intégration des systèmes est une motivation réelle et puissante avec des conséquences à long terme. Les récents progrès dans le domaine des microprocesseurs apportent des changements fondamentaux dans certains domaines traditionnels. Plus précisément, les exigences de l'architecture des systèmes, la répartition des fonctions et les performances des paramètres fonctionnels prennent un nouveau sens dans le contexte de systèmes hautement intégrés contrôlant les phases critiques de la mission. L'efficacité des systèmes intégrés recherche les performances en bout de chaîne en utilisant la meilleure automatisation: les éléments capteurs, les calculateurs et les informations sur l'état du système conditionnent le succès. La conception des postes de pilotage et les rôles des pilotes doivent être définis avec soin en face des tâches automatisées ainsi que les spécifications de l'ensemble du système largement intégré.

L'aboutissement du potentiel total des systèmes intégrés dépend largement de la démonstration d'une fiabilité, sécurité et survivabilité adéquates. Dans le passé, il est apparu que l'interconnexion de sous-systèmes peut conduire à de sévères compromis sur les performances et la sécurité globales du système. Des logiciels à haute fiabilité sont nécessaires. La satisfaction des contraintes dûes à la phase critique de la mission nécessite des concepts nouveaux dans la tolérance aux fautes et dans les schémas d'architecture et d'automatisation du système. L'adjonction de composants, par redondance et à tous niveaux, est un processus qui a ses propres limites pour des questions de poids, de volume, de coût et de réalisation. Les stratégies de reconfiguration, de dégradation acceptables et de redondance aérodynamique sont quelques uns, parmi la multitude, des concepts couramment utilisés. Les techniques d'estimation de l'état du système liées à celles de la technologie de l'intelligence artificielle offrent également un potentiel de résistance aux fautes. L'interconnexion poussée d'éléments du système pour une intégration totale ou une utilisation polyvalente du système à la fois en conditions nominales et en conditions extrêmes nécessite un effort d'intégration intensif pour atteindre un niveau de tolérance acceptable aux pannes.

Ce symposium s'est intéressé aux concepts avancés de systèmes tolérants aux fautes, à leurs applications aux systèmes intégrés militaires "critiques".

Guidance and Control Panel Officers

Chairman: Ir P.Ph. van den Broek
Department of Aerospace Engineering
Delft University of Technology
Kluyverweg 1
2629 HS Delft
The Netherlands

Deputy Chairman: Professor E.B.Stear
Director, Washington Technology Center
University of Washington
376 Loew Hall — FH10
1013 NE 40th Street
Seattle, WA 98195
United States

TECHNICAL PROGRAMME COMMITTEE

Chairman:	Mr J.K.Ramage	US
Members:	Dr M.J.Pelegrin	FR
	Mr U.K.Krogmann	GE
	Pr J.T.Shepherd	UK
	Mr D.E.McIver	US
	Dr G.T.Schmidt	US
	Pr E.B.Stear	US

PANEL EXECUTIVE

From Europe:
Commandant M.Mouhamad, FAF
Executive, GCP
AGARD-OTAN
7 rue Ancelle
F-92200 Neuilly-sur-Seine, France
Telephone: 33 (1) 4738 5780 — Telex: 610 176F — Fax: 33 (1) 4738 5799

For USA and Canada only:
AGARD-NATO
Attention: GCP Executive
APO New York 09777

HOST COORDINATOR

Dr Marc J.Pelegrin
Haut Conseiller
ONERA/CERT
BP 4025
2 avenue Edouard Belin
F-31055 Toulouse
France
Telephone: 33 (61) 557 077 — Telex: 521 596 — Fax: 33 (61) 55 7172

ACKNOWLEDGEMENTS/REMERCIEMENTS

The Panel wishes to express its thanks to the French National Delegates to AGARD for the invitation to hold this meeting in their country and for the facilities and personnel which make the meeting possible.

Le Panel tient à remercier les Délégués Nationaux de la France près l'AGARD de leur invitation à tenir cette réunion dans leurs pays et de la mise à disposition de personnel et des installations nécessaires.

Contents

TECHNICAL EVALUATION REPORT

by
Bernard Chaillot
Sous-Direction Coordination et Evaluation
Direction des Recherches, Etudes et Techniques
00460 ARMEES - FRANCE

EXECUTIVE SUMMARY

The 49th symposium of the AGARD Guidance and Control Panel (GCP) was held in Toulouse, France 10-13 October 1989. The symposium dealt with advances in methods and technologies to design and validate highly integrated, fault tolerant, flight critical guidance and control systems.

Over the past 20 years the guidance and control community has pioneered a number of significant technology advancements, which have had a rather profound impact on combat capabilities of modern day military aircraft.

Current technology trends clearly point in the direction of highly integrated systems to achieve increasing levels of mission effectiveness.

The symposium pinpointed requirements, concepts, flight tests and clearance aspects of flight critical control systems. The design examples covered a broad range of aircrafts : commercial airplane, military aircraft and helicopter. The critical and integrated aspects of new guidance and control issues were addressed and emphasis was given to Terrain Following, Terrain Avoidance, Reconfigurable Control, Vehicle Management, Mission Management, Maintenance Diagnosis.

The trend for highly integrated systems has several far reaching implications with respect to overall system wide integrity management. For example, recent advances in microprocessor technology have brought about fundamental changes in several traditional functional domains.

As a result, system architecture, functional positioning and system performance parameters take on new meaning in the context of a total integrated system design.

Classical approaches involving "brute-force" redundancy, in concert with the use of ultra high reliability piece parts are self-limiting, and simply not practical for application in highly integrated military aircraft flight critical systems.

For military aircraft applications, the key questions remain one of capability, affordability and practicality.

Another key issue of integrated fault tolerant system is system validation. Although traditional methods are applicable new techniques and test philosophies are required to assure overall system wide integrity.

7e The GCP Working Group 9 dealt with this key issue by providing detailed assessments and recommandations for the future. Final report is planned for publication in 1990.

Air vehicles are increasingly reliant on automated flight critical systems ; emphasis must be given within AGARD to automated air vehicle studies and operational acceptance of crew only for supervision.

Modern day guidance and control systems must be considered as a total system entity, including the human pilot or supervisor - vehicle interface.

In this context, innovative fault tolerant technology approaches must be developed and validated, if we are to achieve expanded mission capabilities through highly integrated systems. Failure to properly achieve this, could further aggravate accident statistics with the introduction of highly integrated flight critical systems.

TECHNICAL EVALUATION REPORT (TER) on the
49TH GUIDANCE AND CONTROL PANEL TECHNICAL MEETING
Symposium on

FAULT TOLERANT DESIGN CONCEPTS FOR HIGHLY INTEGRATED FLIGHT CRITICAL GUIDANCE AND CONTROL SYSTEMS

1. TER PURPOSE

This Technical Evaluation Report has been prepared to summarize and assess the 49th Guidance and Control Symposium.

The title of the Symposium is Fault Tolerant Design Concepts for Highly Integrated Flight Critical Guidance and Control Systems. It was held in Toulouse, France, from 10 to 13 October 1989. The program Chairman for this meeting was Mr J.K. RAMAGE.

The program, as presented at the symposium, is appended to this report. The complete compilation of papers will be published as AGARD Conference Proceedings.

2. INTRODUCTION TO THE SYMPOSIUM

The meeting took place at the Ecole Nationale Supérieure de l'Aéronautique et de l'Espace (or SUP AERO), an ingeneer school (Haute Ecole) of the French Ministry of Defence.

2.1. *Symposium objectives :*

This symposium is focused on advanced fault tolerant design concepts and their practical application to integrated flight critical military systems.

The trend towards highly integrated systems continues to expand at a rapid rate. Recent examples include automated maneuvering attack systems, flight control/fire control coupling, mission sensor management, real-time armament fuzing and propulsion coupling/performance optimization.

The lure of improved mission effectiveness through integrated systems is a very real and powerful motivation with far reaching implications. Recent advances in microprocessor technology are bringing about fundamental changes in several traditional functional domains. Specifically, systems architecture requirements, partitioning considerations and functional performance parameters take on new meaning in the context of fully integrated flight critical systems. Effective system integration focuses on end-item functional performance using the most efficient mechanization possible. In this regard, system wide consideration of sensing elements, computational elements and command signalling loops are critically important. Crew station design considerations and the pilots role must also be thoroughly assessed vis-à-vis varying levels of task automation and overall system wide integrity management requirements.

Achieving the full potential of integrated systems is highly dependent upon demonstrating adequate reliability, safety and survivability. Historical evidence indicates that interfacing subsytems can introduce serious compromises in overall system safety and performance. High integrity software is essential. Satisfying stringent flight critical system requirements necessitate innovative fault tolerant design approaches and mechanization schemes. Adding redundancy levels across the full spectrum of system elements is a self-limiting approach based on practical considerations of weight, volume, cost and supportability. Reconfiguration strategies, graceful degradation and aerodynamic redundancy are but a few of the modern concepts currently under development. State estimation techniques in conjunction with artificial intelligence technology also offer potential fault tolerance enhancements. Blending system elements for fully integrated or multi-purpose usage under both nominal and extreme operating conditions, requires an intensive system integration effort to achieve acceptable levels of fault tolerance.

In his introduction the Symposium Chairman indicated the relationship between design deficiencies of subsystem interfacing and accident statistics due to loss of aircraft control. "Brute-force" redundancy and ultra high reliable piece parts are not practical ; high reliable space systems are too costly for military fighter ; innovative fault tolerant technology approaches are needed to design capable, affordable and practicable flight control systems.

Over the past 20 years the guidance and control community has pioneered a number of significant technology advancements, which have had a rather profound impact on combat capabilities of modern day military aircraft. Current technology trends clearly point in the direction of highly integrated systems to achieve increasing levels of mission effectiveness.

This trend has several far reaching implications with respect to overall system wide integrity management. For example, recent advances in microprocessor technology have brought about fundamental changes in several traditional functional domains.

As a result, system architecture, functional positioning and system performance parameters take on new meaning in the context of a total integrated system design.

2.2. *Symposium organization*

The symposium is organized under the following sessions :

	Papers	FR	GE	UK	US
I - TRENDS IN INTEGRATED FLIGHT CRITICAL SYSTEMS	3	1		1	1
II - ADVANCED FAULT TOLERANT DESIGN CONCEPTS	6			2	4
III - SYSTEM ARCHITECTURES, MECHANIZATION AND INTEGRATION ISSUES	4		1	1	2
IV - HIGH INTEGRITY SOFTWARE DESIGN METHODOLOGIES AND ALGORITHMS	4	2		1	1
V - SYSTEM VALIDATION, SIMULATION AND FLIGHT TEST EXPERIENCE	5	1	1		3
TOTALS	22	4	2	5	11

This table takes into account the withdrawal of two papers (from GERMANY).

2.3 *Symposium attendance*

The number of registered participants was around 180. The actual attendance was 144 with the following distribution :

Germany : 34

France : 33

United Kingdom : 30

United States : 28

Italy, The Netherlands : 5

Spain, Turkey : 2

Belgium, Canada, Denmark, Greece, Portugal : 1

3. REVIEW OF SYMPOSIUM PROCEEDINGS

The Symposium Keynote Address, meeting papers and the Round Table Discussion are next reviewed in sequence, as listed in Appendix A, together with session identification.

3.1. *Keynote Address by Gen. François Maurin, Former Chief of Staff at the French Armies, Member of French Conseil d'Etat*

General MAURIN emphasized the need for increasing and improving of flight control and combat aid systems in order to maintain NATO air force technology lead over its adversaries, numerically superior. He addressed the technical, human and financial constraints of design and development of future guidance and control systems. He stressed the necessity to create multidisciplinary teams to deal with such advanced project in order to decrease complexity and cost of the future systems ; simplification instead of sophistication, standardization instead of uncompatibility are the challenge ; and so collaborative work was claimed by the speaker, especially from AGARD and its Guidance and Control Panel.

3.2. *Technical Papers*

All 22 technical papers are included in the summaries and assessments below.

SESSION 1 Paper 11 : FLIGHT CRITICAL DESIGN CONCEPTS FOR LOW-LEVEL TACTICAL GUIDANCE AND CONTROL
by M.R. Griswold, USA.

This paper presents several of the elements of flight critical concepts for low-level tactical operation with autonomous, accurate target acquisition ; the discussion is based on the close Air Support mission using a fast moving, technologically advanced aircraft, F16 derivative, the AFTI/F16. The guidance and control strategies emphasize integrity considerations and performance-versus-safety issues. Many possibilities are offered by the use of on-board terrain data and the need to weigh the risks of database use is pointed out. The principal issues are their accuracy and completeness. The architecture of the guidance and control system is described and the various redundancy techniques are listed. Single thread sensors and single thread computing are used for the avionic manager, physically redundant.

Paper 12 : EVOLUTION DANS LES APPLICATIONS CIVILES (CIVIL APPLICATIONS TRENDS) by P. Traverse, FR.

Airbus A 320 Electric Flight Control System needs for updated system for A 330/340 and trends are reviewed in this paper. Emphasis is given to processor and system architectures and in general to dissimilar redundancies.

The author describes the existing Command and Surveillance Processors and the evolution with respect to the ARINC 651 rule. Much emphasis is given to the use of a distributed system with redundant processors and data synchronisation. A Petri Network based protocol is specified. Optical Flight Control Systems are quoted and leads for safety assess methods are presented.

The lecture was a broad and comprehensive survey of the trends of the computerized flight control system needed for civil aviation as well as the tools to develop and clear them.

Paper 13 : PILOT MONITORING OF DISPLAY ENHANCEMENTS GENERATED FROM A DIGITAL DATA BASE by P.J. Bennett and J.J. Cockburn, UK.

This paper presents a penetration mission and system called PENETRATE. This system is designed to provide aircrew with accurate navigation coupled with head-up and head-down displays of the terrain. The heart of the system is a very large capacity military optical disc drive which contains terrain elevation data, planimetry information, intelligence information and mission information. The system provides terrain referenced navigation, ground proximity warning and displays of navigation, terrain masking and threat avoidance data. Emphasize is given on the different possible displays of terrain to the aircrew which will depend on the visibility of the scene (night, day, good, bad weather). Range of digital terrain displays depends of visibility (6 to 8 miles in standard visibility, further for low visibility). The error of navigation is proportional to the smoothness of the terrain and the automatic mission planning system has to sort out the flight path in order to achieve accuracy but also low intervisibility. The lecture slides showed the collations between actual photographies and obstruction cues which were obtained during flight trials. Data processing and compression may introduce errors and optical disk mass storage has a basic error rate. Careful processing and error correction techniques are mentioned as a solution but are not described.

This session addressed the cautious, relatively short term trends in civil FCS and the new guidance and control issues for military aircraft. The topics of this session were not exhausted but were addressed further (reconfigurable control, mission management, diagnostic system, scheduled maintenance issues).

Session II Paper 21 : TECHNIQUES FOR TRANSIENT ERROR RECOVERY AND AVOIDANCE IN REDUNDANT PROCESSING SYSTEMS by S.J. Adams, M.J. Dzwonczyk, USA.

This paper reviews approaches to detect and restore transient fault memories. The rate of transient memory failures as compared to the rate of fixed failures is highlighted. Error recovery technique is described which use a Segment Access Signature Architecture. Hardware is used to compute a checkword on memory segments and detect which segments have been corrupted by comparizon between redundant processors or at different times in a single processor. But recovery is a problem because time is critical for flight control system, especially for instable aircraft. So a second approach to tolerating transient faults is to use a common fault-tolerant memory which allows errors to be masked and corrected eliminating the need for recovery.

Paper 22 : THE ROLE OF TIME-LIMITED DISPATCH OPERATION IN FAULT TOLERANT FLIGHT CRITICAL CONTROL SYSTEMS by D.F. Allinger, F.J. Leong, P.S. Babcock, G.C. Horan, R.F. LaPrad, USA.

This paper addresses a methodology of establishing dispatch policies of fault-tolerant systems with failed components for a limited time period.

A dual-redundant control actuation system is used to illustrate the analytic techniques which permit to dispatch classification of each system component ; techniques to quantify the impact on system performance are given. Markov model assumptions are taken ; but some work is undertaken to augment the model. Advantages of such a mode of operation are outlined.

The waited advantage of such a mode of operation is that it permits to postpone maintenance operations, consolidating both the logistics and the expertise of maintenance operations ; it is a step towards scheduled mode of maintenance.

But maintenance cost figures have to be computed to assess the possible economic benefit.

Paper 23 : A FAULT TOLERANT FLY-BY-WIRE SYSTEM FOR MAINTENANCE FREE APPLICATIONS by R.W. Dennis, A.D. Hills, UK.

This paper describes a fault-tolerant Primary Flight Computer System for application primarily to commercial aircraft. The test configuration on the Boeing 757 iron bird rig is shown. Reconfigurable, redundant architecture concept is justified and described. A serial interface device is specially developed to support the architecture. To complement this fault-tolerant architecture ASIC design minimizing failure rate of each sub-fonctional element is presented.

This paper addresses perfectly well the topic of this symposium and the lecture was a complete overview of the themes to be developed at this occasion : why fault tolerance ? How ? Redundancy management philosophy, tools to clear the design, result discussion and outlooks.

Paper 24 : THE INTEGRATED AIRFRAME/PROPULSION CONTROL ARCHITECTURE SYSTEM PROGRAM (APSA) by D.L. Palumbo, C.W. Meissner, G.C. Cohen, USA.

This paper provides the example of the integrated Airframe/Propulsion Control System Architecture Program (IAPSA) to highlight the need for adopting a design for validation strategy in order to avoid design errors. It concludes pessimistically that the limitations of analytic techniques can be too restraining and comprehensive validation tools have to be developed.

Reliability and Performance Analysis tools used with the IAPSA program are presented.

Paper 25 : DEPENDABLE SYSTEMS USING "VIPER" by J. Kershaw, UK.

This paper describes a microprocessor, "VIPER", which has been designed to work in pairs to form fault-detecting computing modules. It emphasizes the lessons that have been learned from the use of formal mathematical techniques of design and verification.

This solution arises the problem of specifying and verifying the correctness of the design with a common formal mathematical logic. In fact intelligent exhaustive simulations are also needed.

Paper 26 : FAULT TOLERANT, FLIGHT CRITICAL CONTROL SYSTEMS by T. Sadeghi, G. Mayville, USA.

This paper makes an overview of the tools recently developed within General Electric for fault-tolerant control systems. The goal is to design a reconfigurable flight control system ; an architecture is outlined and simulation results are given for different impairments. Further discussions are the topics of paper n° 53. On-board expert system to support aircraft diagnostics and vehicule management system to support maintainability are then presented. It seems that all these concepts are implemented in the same platform and that it is a little bit confusing.

There was little inter-relation among the papers in this session. There were several examples of fault tolerant concepts, ranged from memory subsystem to integrated Airframe/propulsion control system. But redundancy management philosophy and safety assess tool and method discussions were particularly appropriated.

Session III Paper 31 : METHODS TO PRESERVE THE INTEGRITY OF A COMBAT AIRCRAFT FLIGHT CONTROL SYSTEM THROUGH MAJOR UPGRADE PROGRAMMES by M. Rössler, W. Schmidt, GE.

Based on presently running and intended upgrades of the TORNADO flight control system the paper describes what measures are taken to preserve integrity, fault tolerance and performance of the existing system during a major upgrade. For instance terrain reference navigation mode is going to be implemented together with the present terrain following radar system and combined. Are shown the TORNADO flight control system and the impact of new requirements and advanced basic technologies. The method for the introduction of major modifications consists of an introduction step by step : hardware modifications in the first step while the functionality of the system remains unchanged, software modifications in the second step after implementation and testing. Methods of clearance the new hardware and functions are described.

Paper 32 : FLIGHT CONTROL COMPUTER APPROACH FOR MODERN FLY-BY-WIRE AIRCRAFT by J. Kesberg, R. Hockele, H. Hohner, H. Jacobs, GE.

Withdrawn.

Paper 33 : RESEARCH INTO A MISSION MANAGEMENT AID by J.R. Catford, I.D. Gray, UK.

This paper outlines the program, the joint venture organization, the prototype work and the goal of the mission management aid which is due to decrease pilot workload. The general architecture of the system is given and emphasis is placed on the core functions and integrity.

Mission Management Aid System is intended to be only a technical adviser for aircrew and only conventional information technology techniques are planned to be used so it has not really to comply with safety critical requirements. The program must be seen as a prototype exercise in order to implement and validate a number of algorithms and after that to specify the actual aid system.

Paper 34 : INTEGRATED DIAGNOSTICS FOR FAULT TOLERANT SYSTEMS by H.A. Funk, M.M. Jeppson, USA.

This paper addresses the integrated approach to the maintainability of flight control systems. It emphasizes the goals, the resources available and the constraints of the Integrated Diagnostics concept.

An implementation strategy of an approach utilizing both a portable maintenance aid at the flight line and on-aircraft in-flight diagnostic resources is presented along with a technique which ensures commonality between the on-aircraft and off-aircraft systems.

The paper discusses the results of a present study of integrated maintenance and concludes that the functional model based diagnostic approach provides a common basis for information transfer.

Once again the integrated diagnostics system is not integrated to flight critical control system and so is not submitted to fault tolerancy. The emphasis is given on how to share data and the answer is to model in varying levels of details.

Paper 35 : A BYZANTINE RESILIENT PROCESSOR WITH AN ENCODED FAULT-TOLERANT SHARED MEMORY by R. Harper, B. Butler, USA.

This paper addresses the negative effect on the reliability of the increase of memory size requirements. It describes the use of an encoded memory-based fault-tolerant processor architecture under development at the Charles Stark Draper Laboratory. The paper successively presents an overview of the architecture and its operation, a reliability analysis where it is compared to quadruply redundant designs and a performance analysis. The paper concludes that its primary benefits over other Byzantine resilient architecture are the elimination of memory realignment time, the improvement in short term reliability obtained by the reduced memory requirement and the hardware implemented memory scrubber, the reduced fault latency due to the continual and implicit fault masking, and the improved high-iteration-rate performance.

Byzantine resilience is defined as a sort of resilience to any possible errors in the subsystem, but how to deal with the possible fault of system monitor ? Another layer of processing is needed which has obviously to be fault tolerant.

During the symposium the Session Chairman took the opportunity to offer the speakers a feedback from the audience. A couple of thoughts were exchanged about system architecture update (is it possible ?), reconfigurated flight critical aspect, error propagation, error diagnostic and environment monitoring.

Session IV Paper 41 : A HIGHLY RELIABLE, AUTONOMOUS DATA COMMUNICATION SUBSYSTEM FOR AN ADVANCED INFORMATION PROCESSING SYSTEM by G. Nagle, T. Masotto, L. Alger, USA.

This paper describes the design and implementation of the prototype input/output communication system for the Advanced Information Processing System (AIPS) under development at the Charles Stark Draper Laboratory. The goals are presented which are to design general purpose computer systems and input/output subsystems in order to ease modifications or extensions of flight critical systems. AIPS addresses reliability issues related to data communications by the use of reconfigurable input/output networks including spare interconnections. Performance issues are addressed by using a paralleled computer architecture which decouples input/output redundancy management and input/output processing from the computational stream of an application and so the communication subsystem is transparent to the user.

Paper 42 : FORMALISATION DE DEVELOPPEMENTS : DE LA THEORIE AU PROGRAMME (FORMALIZING DEVELOPMENTS : FROM THEORY TO PRACTICE) by M. Lemoine, K. Bechane, FR.

This paper addresses software development method issues. A project is presented, the Tool Use Project and the language of formalization is described. The DEVA language is a high-order typed λ-calculus. Through the case study of expressing part of the Jackson's Structured Programming method in the DEVA framework the authors show the interest of formal techniques of software development.

So if the fault tolerance requirements are correctly expressed in the specification, this method provides a software which is safe proven in a mathematical sense. Doubts arise from the complexity and unpredictability of the application complex environment and from the original specification completness. Work must be undertaken in that way.

Paper 43 : METHODOLOGIE DE DECOMPOSITION D'APPLICATION DE NAVIGATION CRITIQUE EN ELEMENTS SIMPLES (BREAK-DOWN METHODOLOGY FOR FLIGHT CRITICAL APPLICATIONS INTO ELEMENTARY COMPONENTS) by B. Chavana, F. de Sainte Maresville, FR.

The software design of a helicopter primary reference system is presented. The design methodology goals and implementation are depicted. The simplification method is based on splitting deterministic processes and random interruptions ; the real time complexity is eliminated from each software component and only supported by a monitor ; simplification effects on software production is emphasized (modularity, standardization). The tests were said to be very effective but no demonstration was supplied.

Paper 44 : FAULT TOLERANCE VIA FAULT AVOIDANCE by B.D. Bramson, UK.

The philosophy of the paper is that testing is good at finding errors but bad at demonstrating their absence ; also safe software production conditions are first reminded and then it is claimed that a proof of correctness of one of the software components can imply a proof of safety of the system. A hypothetical processing system design illustrates the claim. MALPAS intermediate language and compliance analysis are respectively presented as a design language and a verification technique.

Before getting methods for proof of correctness in-built system production this paper illustrates the need for minimizing software complexity in order to have mathematically based validated software. System notion, when it expands, involves customer specifications as well and it seems we are looking a perfect world production method, what is highly utopia.

Paper 45 : HIGH INTEGRITY SOFTWARE FOR SAFETY CRITICAL TF/FA FUNCTIONS by H. Wald, H.D. Lerche, GE.

Withdrawn.

The papers of this session address how fault tolerance can be achieved in software. The answers are various : some are negative and claim for software complexity minimization ; some others suggest several methods. And among them there is need to quantify probability of faults in order to improve the design and to have software better and better. Today the bottom line is the human resource. A good method, a powerful technique such as DEVA is waited for.

Paper 51 : PILOTED SIMULATION VERIFICATION OF A CONTROL RECONFIGURATION STRATEGY FOR A FIGHTER AIRCRAFT UNDER IMPAIRMENTS by R. Mercadante, USA.

This paper presents the results obtained during piloted simulation of the Control Reconfigurable Combat Aircraft (CRCA). This study was aimed at the verification of the capability of a reconfiguration strategy to improve aircraft controlability. CRCA configuration, damage and failure modeling, reconfiguration strategy are described. Test conditions are outlined, then the results are shown using pilot workload measurement, target tracking scoring and pilot (using Cooper-Harper rating scale). The improvements of reconfiguration of the control laws following impairments are discussed.

The lecture was accompanied by a video showing the pilot's view through the Head-Up Display while flying with an impairment during short take-off and landing flight condition, successively without and with reconfiguration activated. This illustrated a very important feature : the necessity to alert the pilot about the flight envelope status and it was said that pilots were involved in its design. This lecture was very attractive. Questions were about extension of reconfiguration to engine or fuel circuit failures and about impairment statistics data to help to design reconfiguration laws.

Paper 52 : FLIGHT TEST RESULTS OF FAILURE DETECTION AND ISOLATION ALGORITHMS FOR A REDUNDANT STRAPDOWN INERTIAL MEASUREMENT UNIT by F.R. Morrell, P.R. Motyka, M.L. Bailey, USA.

Two algorithms for failure detection and isolation of a skewed array of collocated inertial sensors are described and compared. Fault tolerance is provided by edge vector test and generalized likelihood test algorithms. To detect the wide range of failure magnitudes in inertial sensors, fault detection and isolation are developed in terms of a multilevel structure.

The development of accelerometer parity equations and the reduction to sensor errors are described and threshold compensation techniques are presented. Flight test equipments and results are shown which allow a comparison of both algorithms and a discussion.

The results are consistent but do not apply in this example to accurate navigation, and redundancy concepts with strapdown inertial system are fairly old now.

Paper 53 : FLIGHT DEMONSTRATION OF A SELF-REPAIRING FLIGHT CONTROL SYSTEM IN A NASA F-15 FIGHTER AIRCRAFT by J.M. Urnes, J. Stewart, R. Eslinger, USA.

This paper presents the real-time reconfiguration development program that is going on in the USA. Software design considerations are presented in paper n° 26. Paper 51 is reporting the same relevant researches. The NASA F-15 flight test of a self repairing flight control system which incorporates real-time reconfiguration and expert maintenance diagnostics is described. The heart of reconfiguration is a Failure Detection, Isolation and Estimation Algorithm where the expected answer of the command is compared to the actual answer. Reconfiguration process and results are presented. Future prospects are outlined.

Here, too, emphasis is given on man-machine interface ; cues of maneuver capability are given to the pilot. The illustration of an on board expert system is very attractive. Questions arise from the need to sophisticate the system which will have to take into account several impairments and to analyse viability of reconfigurated impaired aircraft status.

Paper 54 : FLIGHT TESTING OF A REDUNDANT EXPERIMENTAL FbW/FbL HELICOPTER CONTROL SYSTEM by H. Becker, K. Bender, K.D. Holle, G. Mansfeld, GE.

This paper describes objectives, architecture, hardware, software and flight test results of a helicopter flight control system. Investigation of new hardware technologies and components are aimed at improving reliability. A yaw control system with fiber optic communication between sensors and actuation is implemented. Fiber Optic interfaces also the three redundant flight control computers. Handling quality improvement is claimed. Loss of control is tested.

Paper 55 : UN SYSTEME DE REFERENCES PRIMAIRE DE HAUTE INTEGRITE (A HIGH INTEGRITY FLIGHT DATA SYSTEM) by J.L. ROCH, J. CONTET, FR.

This paper presents the flight data system high integrity and high reliability issues and the answer brought. Software methods are presented in paper n° 43. It describes the overall architecture of the Super PUMA MK2 integrated flight and display system and the requirements for the primary reference system. Quality aspects of the design are outlined and clearance aspects are described ; especially industrial development method approach is emphasized.

The paper does not bring validation of reliability requirements. This is because the flight control system reliability depends on the architecture of the overall system which includes for this helicopter application two flight data systems, back-up sensors and a vertical gyro for doubt erasing. So full budget is at a higher level and the reader is a little bit frustrated.

Except this last paper, which is session II or III relevant, four papers illustrate the extensive and comprehensive flight tests to be done to validate a concept. There is no answer to say if it is sufficient.

3.3. *Round table discussions*

The round table is set up to provide a resume of each major topic of the symposium and serve as a catalyst for discussion and conclusion by all attendees of the symposium.

Round table participants and selected areas are :

Mr J.K. RAMAGE, Chairman
Dr M. PELLEGRIN, Flight Critical System Trends,
Dr R.C. ONKEN, Advanced Fault Tolerant Design Concepts,
Dr E.B. STEAR, System Architectures, Mechanization and Integration Issues
Dr J. KERSHAW, Software Design Methodologies and Algorithms
Dr G.T. SCHMIDT, System Validation, Simulation and Flight Test Experience

STATEMENTS AND DISCUSSIONS :

Dr M. PELLEGRIN, in charge of System Trends, took a provocative position suggesting the on-board crew elimination. Today flight of a modern aircraft is made of sequential automatic modes which are engaged by the pilot. Surety depends on Air Traffic Control (ATC), crew and flight control system errors. Trends are to get an automatic ATC and to increase flight control system reliability ; what about the crew ? It is not possible to rely on one pilot because of its poor reliability (10^{-6}/h) so the question is to suppress or not the two pilots and to have instead supervisor crewman. Dr PELLEGRIN forecasts the suppression will be possible within 5 years.

The audience reaction was that such a change need an evolution of passenger mind and that software error treatment receives a solution.

Dr R.C. ONKEN highlighted the need to design probability figures. This is complicated because Flight Control Systems are critical with respect to hardware or software failures but also critical with respect to enemy threats. And in peace time, when threats are not there, training need is safety critical due to military flights over populated area. Advanced functions, such as vehicle, flight and mission managements which were exclusively assumed by the pilot, are integrated and so the failure rate is increasing. How could we measure the degree of tolerance of integrated systems ?

A pessimistic answer was given by the audience. Failure rate objectives for advanced fault tolerant systems are too high and too difficult to validate with sophisticated but tedious simulations ; the law is to be broken as are the laws made to be violated !

Dr E.B. STEAR emphasized the necessity to cope with increasing complexity due to the add of vehicle management system, mission management system, etc... and the presence of not only random failures but also Byzantine or intentional failures. "There are several key issues for the future, most of them we don't know what to do" the speaker said.

Several comments were made. R and D methods must be transitioned to production line in order to ease the functional complexity transfer towards application. Use diagnostic to fit system and make sure it works. Use protection against designer rather than programmer, report circumstances of failure (what maneuver, what environment, etc...). Validation problem is a key issue : it would be a sort of limiting aspect of validation to make do with running validation from the beginning of the program as it is recommanded.

Dr J. KERSHAW was pleased to hear about powerful techniques such as DEVA but reminded that traditional practice was made of good methods ; subsystem partitioning helps to reduce complexity but it assumes that if a component is correct it stays correct ; the speaker sees no conflict between mission management concept and flight control design but rather synergy. The question posed was if traditional methods are good but are not able to supply software failure rate figures, is good quality feeling enough ?

DR G.T. SCHMIDT summed up the issue of flight test results : because of their specific environment what is their value ? A data bank would be very useful.

Mr J.K. RAMAGE concluded the symposium and addressed the key issues of fault-tolerant flight control systems ; new innovative concepts and methods were interesting to note and trade-off between mission performance, reliability, safety and affordability could be got at a still higher level for both parts thanks to powerful techniques, new tools and skilled people.

Clearly, todays trend towards highly integrated systems has several significant implications with respect to overall system integrity and validation methodologies. It's encouraging to note that several innovative fault tolerant design concepts are being developed within NATO to provide the necessary system integrity for achieving improved mission capabilities. Keynote speaker Gen Maurin highlighted the need to consider modern day guidance and control systems as a total entity, including the pilot vehicle interface. In particular, one must constantly balance mission performance against affordability and safety. Failure to properly achieve this, could further aggravate accident statistics with the introduction of highly integrated flight critical systems. Significant technical challenges remain to assure acceptable risk levels.

4. CONCLUSIONS

The conclusions presented here are those of the author, based on the written papers, presentations, discussions and on the forms handed in by the symposium delegates.

4.1 An overall picture of the topics presented in this symposium is given by the distribution of the papers related to existing, updated or new systems, to specific technology advances or to safety aspects.

Fault-Tolerant Flight Control Sub-system/system :

. existing : 12 (A 320) ; 43,55 (PUMA PSR) ; 52 (INS) ;

. updated : 11 (AFTI/F16) ; 12 (A 330/340) ; 23 (Commercial Airplane FCS) ; 31 (TORNADO)

. new : 12 (Commercial Airplane) ; 24 (integrated Airframe/Propulsion Control System) ; 26, 51, 53 (CRCA).

Fault-Tolerant Technique/Technology Advances :

. Microprocessor : 23,25 ;

. Memory : 21,35 ;

. Communication Network : 41 ;

. Data Base : 11,23 ;

. Displays : 13 ;

. Optical : 12,54 ;

. Expert-System : 26,53 ;

. High Order Language : 42,44.

New Guidance and Control Issues :

. Terrain Following, Terrain Avoidance : 11, 13, 31 ;

. Reconfigurable control : 26,53 ;

. Mission, Vehicle Management : 26,33 ;

. Diagnosis : 26, 34 ;

. Scheduled Maintenance : 22 ;

Safety Assess Tests and Methods : 31, 44, 51, 53, 54, 55 ;

Safety Assess Tools : 12, 24, 25.

4.2 The state of the art Flight Control Systems have been reviewed. System Architecture is lane oriented and system failure tolerance capability is achieved through parallel redundancy. Requirements are more stringent for civil applications. In these applications more emphasis is given on channelizing and dispersing the flight control functions. Commercial Aircraft Controller seems to be more fault-tolerant effective than military Aircraft Controller.

4.3 There is a general consensus in the technical community that the technology is in hand for addressing new guidance and control issues such as reconfigurable control and vehicle management and for allowing pilot workload to decrease with mission management aid system. With respect to fault tolerance crew might be the bottleneck. Out of 40 accidents a year for both commercial and military aircrafts due to control function loss, 80 % are due to the crew or to procedure rules. A complete flight automatic system is claimed to increase reliability. However the key of this new step success is the development of means to assure operational decision makers - or passengers - that they are not at the mercy of a machine.

4.4 Flight Control System will become more complex due to increasing number of functions (Terrain Following, Terrain Avoidance, Reconfigurable Control, Vehicle Management, Maintenance Diagnosis, Mission Management...) and integration (propulsion, fire control, ...). Commonality of hardware and software must be encouraged to increase confidence and to lower cost. Especially reusability of software must be encouraged ; development of means such as software partitioning, complex software replacement by simple hardware is needed because it seems that formal proof could be achieved for simple application.

4.5 The state of the art Flight Control System validation methods and tools have been reviewed. The traditional method can be qualified of good ; it includes modelling phase with Failure Modes and Effects Analysis (F.M.E.A.), the Augmented Failure Modes and Effects and Criticality Analysis (FMECA) and Fault-Tree Methodology, then iron bird integration and testing, flight test and mi-service operation incident report evaluation. No theoretical framework exists for the validation process. A "reliability insurance" must be applied ; it consists to include validation in the design and to consider validation from the creation of the project. Computer-Aided Reliability Estimation will be very useful.

4.6 At present, because of item 4.4 issue, Flight Control System updating is a very hard job.

4.7 Testing is only good at finding errors but not at demonstrating their absence. So there is a need for mature formal proof methods. This need is at present, not satisfied even if some progress has been made. The key issue of fault tolerant system is validation.

7e 5. RECOMMANDATIONS

5.1 The key issue of fault-tolerant Flight Control System must be addressed continuously. With respect to the results of the GCP Working Group 9 on validation of flight critical control systems follow-on action should be given to a Lecture Series to explain validation methods or what methods are asked for (i.e. formal proof validation).

5.2 Air vehicles are still more and more automatic because technology push and requirement pull (especially fire control and threat avoidance system level) ; the dialogue between man and machine is more and more difficult when the responsabilities are not clear or the bandwidths different. Semi-automatic systems are hard to manage because man presence hinders the whole system modelling ; it is the reason why emphasis must be given on automatic air vehicle studies and operational acceptance of crew only for supervision.

APPENDIX

FINAL PROGRAM

FAULT TOLERANT DESIGN CONCEPTS FOR HIGHLY INTEGRATED FLIGHT CRITICAL GUIDANCE AND CONTROL SYSTEMS

Programme Chairman : Mr. James K. RAMAGE (US)

KEYNOTE ADDRESS by Général François Maurin, Member of French Conseil d'Etat and Former Chief of Staff of the French Armies.

Session I - TRENDS IN INTEGRATED FLIGHT CRITICAL SYSTEMS
Chairman : Dr. M.J. PELEGRIN (FR)

11 : Flight critical design concepts for low-level tactical guidance and control

M.R. GRISWOLD	General Dynamics Corporation, Fort Worth Division, TX, USA

12 : Evolution dans les applications civiles
Civil applications trends

P. TRAVERSE	Aérospatiale, Toulouse, FR.

13 : Pilot monitoring of display enhancements generated from a digital data base

P.J. BENNETT, J.J. COCKBURN	Ferranti Defence System Limited Edinburgh, UK

Session II - ADVANCED FAULT TOLERANT DESIGN CONCEPTS
Chairman : Mr. U.K. KROGMANN (GE)

21 : Techniques for transient error recovery and avoidance in redundant processing systems

S.J. ADAMS, M.J. DZWONCZYK	The Charles Stark Draper Laboratory, Inc., Cambridge, MA, USA

22 : The role of time-limited dispatch operation in fault tolerant flight critical control systems

D.F. ALLINGER, F.J. LEONG P.S. BABCOCK	The Charles Stark Draper Laboratory, Inc., Cambridge, MA, USA
G.C. HORAN, R.F. LaPrad	Pratt and Whitney Aircraft Division, E. Hartford, Connecticut, USA

23 : A fault tolerant fly-by-wire system for maintenance free applications

R.W. DENNIS, A.D. HILLS	GEC Avionics Flight Controls Division, Rochester, Kent, UK.

24 : The integrated airframe/propulsion control system architecture program (IAPSA)

D.L. PALUMBO, C.W. MEISSNER	NASA Langley Research Center, Hampton, VA, USA
G.C. COHEN	Boeing Advanced Systems Co., Seattle, WA, USA

25 : Dependable systems using "VIPER"

J. KERSHAW	RSRE, Malvern, UK

26 : Fault tolerant, flight critical control systems

T. SADEGHI, G. MAYVILLE	General Electric Company, Binghampton, NY, USA

SESSION - III SYSTEM ARCHITECTURES, MECHANIZATION AND INTEGRATION ISSUES

Chairman : Professor E.B. STEAR (US)

31 : Methods to preserve the integrity of a combat aircraft flight control system through major upgrade programmes

M. RÖSSLER, W. SCHMIDT — MBB München, GE

33 : Research into a mission management aid

J.R. CATFORD — GEC Avionics, Rochester, Kent, UK
I.D. GRAY — Ferranti Defence Systems, Edinburgh, UK
(Both of the MMA Joint Venture, RAE, Farnborough, Hants)

34 : Integrated diagnostics for fault tolerant systems

H.A FUNK, M.M. JEPPSON — Honeywell Systems and Research Center, Minneapolis, MN,USA

35 : A Byzantine resilient processor with an encoded fault-tolerant shared memory

R.E. HARPER, B. BUTLER — The Charles Stark Draper Laboratory, Inc., Cambridge, MA, USA

SESSION IV - HIGH INTEGRITY SOFTWARE DESIGN METHODOLOGIES AND ALGORITHMS

Chairman : Professor J.T. SHEPHERD (UK)

41 : A highly reliable, autonomous data communication subsystem for an advanced information processing system

G. NAGLE, T. MASOTTO, L. ALGER — The Charles Stark Draper Laboratory, Inc., Cambridge, MA, USA

42 : Formalisation de développements : de la théorie au programme
Formalizing developments : from theory to practice

M. LEMOINE, K. BECHANE — ONERA-CERT, Département d'Etudes et de Recherches en Informatique, Toulouse, FR

43 : Méthodologie de décomposition d'application de navigation critique en éléments simples
Break-down methodology for flight critical applications into elementary components

B. CHAVANA, F. de SAINTE MARESVILLE — CROUZET SA, Valence, FR

44 : Fault tolerance via fault avoidance

B.D. BRAMSON — RSRE, Malvern, Worcs, UK

SESSION V - SYSTEM VALIDATION, SIMULATION AND FLIGHT TEST EXPERIENCE
Chairman : Dr. G.T. SCHMIDT (US)

51 : Piloted simulation verification of a control reconfiguration strategy for a fighter aircraft under impairments

R. MERCADANTE — Grumman Aircraft Systems Division, Bethpage, NY, USA

52 : Flight test results of failure detection and isolation algorithms for a redundant strapdown inertial measurement unit

F.R. MORRELL — NASA Langley Research Center, Hampton, VA, USA
P.R. MOTYKA — The Charles Stark Draper Laboratory, Inc., Cambridge, MA, USA
M.L. BAILEY — PRC Kentron International, Hampton, VA, USA

53 : Flight demonstration of a self-repairing flight control system in a NASA F-15 fighter aircraft

J.M. URNES	McDonnell Aircraft Company, St Louis, MO, USA
J. STEWART	NASA Ames Research Center, Dryden Flight Research Facility, Edwards AFB, CA, USA
R. ESLINGER	Wright Research and Development Center, (WDRC/FIGL), Wright-Patterson AFB, USA

54 : Flight testing of a redundant experimental FbW/FbL helicopter control system

G. MANSFELD, H. BECKER K. BENDER, K.D. HOLLE	DFVLR, Institut für Flugführung, Braunschweig, GE

55 : Un système de références primaires de haute intégrité
A high integrity flight data system

J.L. ROCH, J. CONTET	CROUZET SA, Valence, FR

ROUND TABLE DISCUSSION - FUTURE TRENDS AND KEY ISSUES

REPORT DOCUMENTATION PAGE

1. Recipient's Reference	2. Originator's Reference	3. Further Reference	4. Security Classification of Document
	1/11 AGARD-AR-281	2/08 ISBN 92-835-0559-X	UNCLASSIFIED

5. Originator Advisory Group for Aerospace Research and Development
North Atlantic Treaty Organization
7 rue Ancelle, 92200 Neuilly sur Seine, France 1/14

6. Title TECHNICAL EVALUATION REPORT ON THE 49th GCP SYMPOSIUM ON FAULT TOLERANT DESIGN CONCEPTS FOR HIGHLY INTEGRATED FLIGHT CRITICAL GUIDANCE AND CONTROL SYSTEMS 1/18

7. Presented at

8. Author(s)/Editor(s)	9. Date
Monsieur Bernard Chaillot 2/09	May 1990 1/12 1/13

10. Author's/Editor's Address	11. Pages
Direction des Recherches et Etudes Techniques (SCDE/CT/DN) 26 boulevard Victor, F-75996 Paris Armées	22

12. Distribution Statement This document is distributed in accordance with AGARD policies and regulations, which are outlined on the Outside Back Covers of all AGARD publications.

13. Keywords/Descriptors

Guidance	Terrain avoidance
Control	Reconfigurable control
Fault tolerance system	Vehicle management
Software validation	Mission management
Terrain following	Maintenance diagnosis

~~**14. Abstract**~~
Conference on

Evaluation Report on the Guidance and Control Panel 49th Symposium held at the Ecole Nationale Supérieure de l'Aéronautique et de l'Espace in Toulouse, France, from 10th to 13th October 1989.

In all 23 papers were presented including the Keynote address, covering the following headings:

— Trends in integrated flight critical systems;
— Advanced fault tolerant design concepts;
— System architectures, mechanization and integration issues;
— High integrity software design methodologies and algorithms;
— System validation, simulation and flight test experience.

The full proceedings are available as P-283 719

3/02

AGARD Advisory Report No.281	AGARD-AR-281
Advisory Group for Aerospace Research and Development, NATO TECHNICAL EVALUATION REPORT ON THE 49th GCP SYMPOSIUM ON FAULT TOLERANT DESIGN CONCEPTS FOR HIGHLY INTEGRATED FLIGHT CRITICAL GUIDANCE AND CONTROL SYSTEMS Monsieur Bernard Chaillot Published May 1990 22 pages Evaluation Report on the Guidance and Control Panel 49th Symposium held at the Ecole Nationale Supérieure de l'Aéronautique et de l'Espace in Toulouse, France, from 10th to 13th October 1989. P.T.O.	Guidance Control Fault tolerance system Software validation Terrain following Terrain avoidance Reconfigurable control Vehicle management Mission management Maintenance diagnosis

AGARD Advisory Report No.281	AGARD-AR-281
Advisory Group for Aerospace Research and Development, NATO TECHNICAL EVALUATION REPORT ON THE 49th GCP SYMPOSIUM ON FAULT TOLERANT DESIGN CONCEPTS FOR HIGHLY INTEGRATED FLIGHT CRITICAL GUIDANCE AND CONTROL SYSTEMS Monsieur Bernard Chaillot Published May 1990 22 pages Evaluation Report on the Guidance and Control Panel 49th Symposium held at the Ecole Nationale Supérieure de l'Aéronautique et de l'Espace in Toulouse, France, from 10th to 13th October 1989. P.T.O.	Guidance Control Fault tolerance system Software validation Terrain following Terrain avoidance Reconfigurable control Vehicle management Mission management Maintenance diagnosis

AGARD Advisory Report No.281	AGARD-AR-281
Advisory Group for Aerospace Research and Development, NATO TECHNICAL EVALUATION REPORT ON THE 49th GCP SYMPOSIUM ON FAULT TOLERANT DESIGN CONCEPTS FOR HIGHLY INTEGRATED FLIGHT CRITICAL GUIDANCE AND CONTROL SYSTEMS Monsieur Bernard Chaillot Published May 1990 22 pages Evaluation Report on the Guidance and Control Panel 49th Symposium held at the Ecole Nationale Supérieure de l'Aéronautique et de l'Espace in Toulouse, France, from 10th to 13th October 1989. P.T.O.	Guidance Control Fault tolerance system Software validation Terrain following Terrain avoidance Reconfigurable control Vehicle management Mission management Maintenance diagnosis

AGARD Advisory Report No.281	AGARD-AR-281
Advisory Group for Aerospace Research and Development, NATO TECHNICAL EVALUATION REPORT ON THE 49th GCP SYMPOSIUM ON FAULT TOLERANT DESIGN CONCEPTS FOR HIGHLY INTEGRATED FLIGHT CRITICAL GUIDANCE AND CONTROL SYSTEMS Monsieur Bernard Chaillot Published May 1990 22 pages Evaluation Report on the Guidance and Control Panel 49th Symposium held at the Ecole Nationale Supérieure de l'Aéronautique et de l'Espace in Toulouse, France, from 10th to 13th October 1989. P.T.O.	Guidance Control Fault tolerance system Software validation Terrain following Terrain avoidance Reconfigurable control Vehicle management Mission management Maintenance diagnosis

In all 23 papers were presented including the Keynote address, covering the following headings:

- Trends in integrated flight critical systems;
- Advanced fault tolerant design concepts;
- System architectures, mechanization and integration issues;
- High integrity software design methodologies and algorithms;
- System validation, simulation and flight test experience.

ISBN 92-835-0559-X

In all 23 papers were presented including the Keynote address, covering the following headings:

- Trends in integrated flight critical systems;
- Advanced fault tolerant design concepts;
- System architectures, mechanization and integration issues;
- High integrity software design methodologies and algorithms;
- System validation, simulation and flight test experience.

ISBN 92-835-0559-X

In all 23 papers were presented including the Keynote address, covering the following headings:

- Trends in integrated flight critical systems;
- Advanced fault tolerant design concepts;
- System architectures, mechanization and integration issues;
- High integrity software design methodologies and algorithms;
- System validation, simulation and flight test experience.

ISBN 92-835-0559-X

In all 23 papers were presented including the Keynote address, covering the following headings:

- Trends in integrated flight critical systems;
- Advanced fault tolerant design concepts;
- System architectures, mechanization and integration issues;
- High integrity software design methodologies and algorithms;
- System validation, simulation and flight test experience.

ISBN 92-835-0559-X

AGARD

NATO OTAN

7 rue Ancelle · 92200 NEUILLY-SUR-SEINE

FRANCE

Telephone (1)47.38.57.00 · Telex 610 176

DISTRIBUTION OF UNCLASSIFIED AGARD PUBLICATIONS

AGARD does NOT hold stocks of AGARD publications at the above address for general distribution. Initial distribution of AGARD publications is made to AGARD Member Nations through the following National Distribution Centres.Further copies are sometimes available from these Centres, but if not may be purchased in Microfiche or Photocopy form from the Sales Agencies listed below.

NATIONAL DISTRIBUTION CENTRES

BELGIUM
Coordonnateur AGARD — VSL
Etat-Major de la Force Aérienne
Quartier Reine Elisabeth
Rue d'Evere, 1140 Bruxelles

CANADA
Director Scientific Information Services
Dept of National Defence
Ottawa, Ontario K1A 0K2

DENMARK
Danish Defence Research Board
Ved Idraetsparken 4
2100 Copenhagen Ø

FRANCE
O.N.E.R.A. (Direction)
29 Avenue de la Division Leclerc
92320 Châtillon

GERMANY
Fachinformationszentrum
Karlsruhe
D-7514 Eggenstein-Leopoldshafen 2

GREECE
Hellenic Air Force
Air War College
Scientific and Technical Library
Dekelia Air Force Base
Dekelia, Athens TGA 1010

ICELAND
Director of Aviation
c/o Flugrad
Reyjavik

ITALY
Aeronautica Militare
Ufficio del Delegato Nazionale all'AGARD
3 Piazzale Adenauer
00144 Roma/EUR

LUXEMBOURG
See Belgium

NETHERLANDS
Netherlands Delegation to AGARD
National Aerospace Laboratory, NLR
Kluyverweg 1
2629 HS Delft

NORWAY
Norwegian Defence Research Establishment
Attn: Biblioteket
P.O. Box 25
N-2007 Kjeller

PORTUGAL
Portuguese National Coordinator to AGARD
Gabinete de Estudos e Programas
CLAFA
Base de Alfragide
Alfragide
2700 Amadora

SPAIN
INTA (AGARD Publications)
Pintor Rosales 34
28008 Madrid

TURKEY
Milli Savunma Bakanlığı (MSB)
ARGE Daire Başkanlığı (ARGE)
Ankara

UNITED KINGDOM
Defence Research Information Centre
Kentigern House
65 Brown Street
Glasgow G2 8EX

UNITED STATES
National Aeronautics and Space Administration (NASA)
Langley Research Center
M/S 180
Hampton, Virginia 23665

THE UNITED STATES NATIONAL DISTRIBUTION CENTRE (NASA) DOES NOT HOLD STOCKS OF AGARD PUBLICATIONS, AND APPLICATIONS FOR COPIES SHOULD BE MADE DIRECT TO THE NATIONAL TECHNICAL INFORMATION SERVICE (NTIS) AT THE ADDRESS BELOW.

SALES AGENCIES

National Technical
Information Service (NTIS)
5285 Port Royal Road
Springfield
Virginia 22161, USA

ESA/Information Retrieval Service
European Space Agency
10, rue Mario Nikis
75015 Paris, France

The British Library
Document Supply Centre
Boston Spa, Wetherby
West Yorkshire LS23 7BQ
England

Requests for microfiche or photocopies of AGARD documents should include the AGARD serial number, title, author or editor, and publication date. Requests to NTIS should include the NASA accession report number. Full bibliographical references and abstracts of AGARD publications are given in the following journals:

Scientific and Technical Aerospace Reports (STAR)
published by NASA Scientific and Technical
Information Branch
NASA H
Washingt

Government Reports Announcements (GRA)
published by the National Technical
Information Services, Springfield