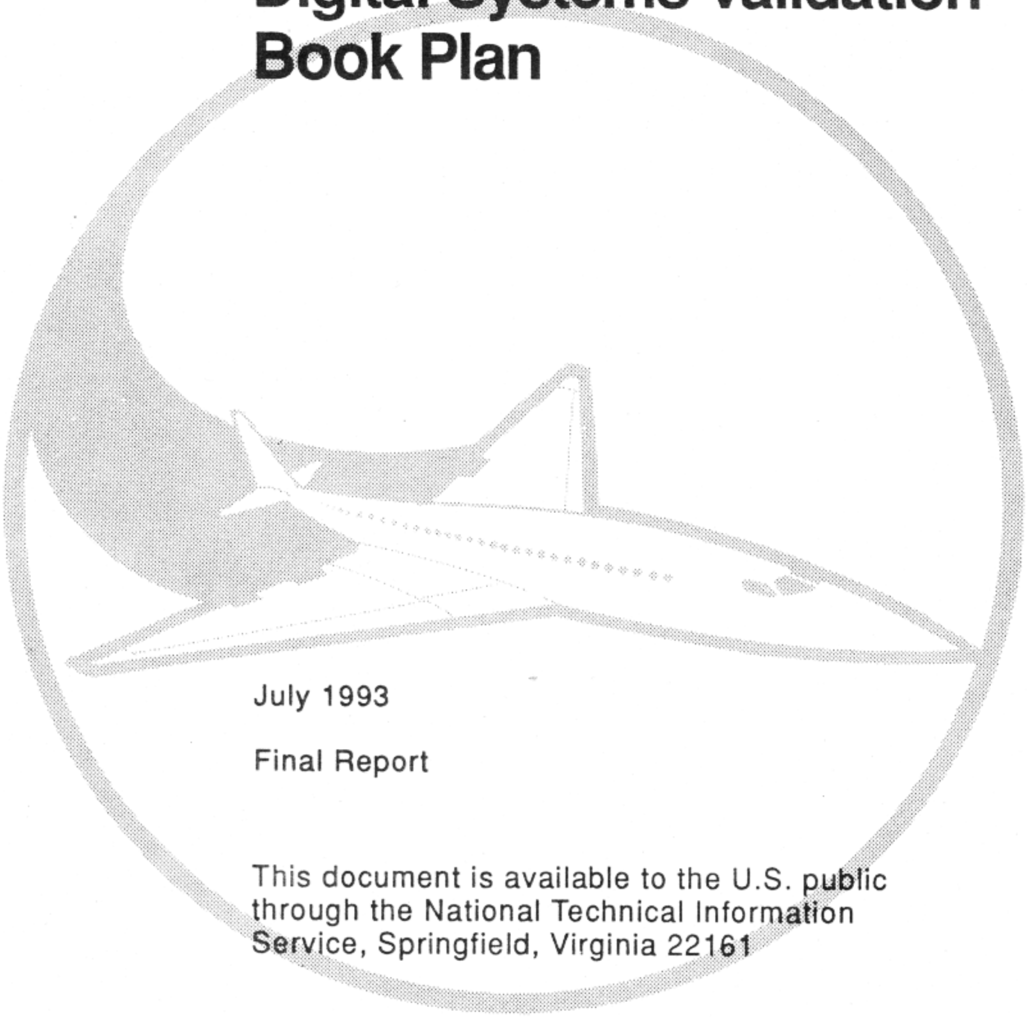
DOT/FAA/CT-93/16

FAA Technical Center
Atlantic City International Airport
N.J. 08405

Handbook - Volume III Digital Systems Validation Book Plan



July 1993

Final Report

This document is available to the U.S. public through the National Technical Information Service, Springfield, Virginia 22161

U.S. Department of Transportation
Federal Aviation Administration

- Techniques for Validation Experiments
  - Reduced testing requirements
  - System observability requirements
- Thermal Analysis/Simulation of Avionic Systems
- Validation of Artificial Intelligence Systems
- Verification of Application Specific Integrated Circuits (ASICs)
- Windshear

☆U.S. GOVERNMENT PRINTING OFFICE: 1993 - 504-078/80183

Technical Report Documentation Page

1. Report No.
DOT/FAA/CT-93/16

2. Government Accession No.

3. Recipient's Catalog No.

4. Title and Subtitle

HANDBOOK - VOLUME III
DIGITAL SYSTEMS VALIDATION BOOK PLAN

5. Report Date
July 1993

6. Performing Organization Code

7. Author(s)
Joan Janowitz

8. Performing Organization Report No.

9. Performing Organization Name and Address

Galaxy Scientific Corporation
2500 English Creek Avenue, Building 11
Pleasantville, NJ 08232

10. Work Unit No. (TRAIS)

11. Contract or Grant No.
DT FA03-89-C-00043

12. Sponsoring Agency Name and Address
U.S. Department of Transportation
Federal Aviation Administration
Technical Center
Atlantic City International Airport, NJ 08405

13. Type of Report and Period Covered
Final Report

14. Sponsoring Agency Code
ACD-230

15. Supplementary Notes
FAA Program Manager: Pete Saraceni
FAA Technical Center, ACD-230, Building 210
Voice: (609) 485-5577, FAX: (609) 485-4005

16. Abstract

The Digital Systems Validation Handbook is a tutorial series designed to provide certification engineers information on current topics related to digital avionics. The book plan lays the foundation for volume III of this series. The purpose of the handbook book plan is to identify technology and related issues that certification engineers are likely to encounter. Volume III of the handbook series will consist of approximately 20 chapters. Sixteen chapters are described in the book plan. Four were reserved for technologies or issues that might emerge during the course of the volume III life cycle.

A list of potential handbook topics was derived from a survey of the literature, conference and seminar attendance, results of an informal questionnaire, and interviews with Federal Aviation Administration (FAA) National Resource Specialists, experts in the field of certification and digital avionics, National Aeronautics and Space Administration (NASA) officials, and persons in private industry. From this input, the list of potential topics was developed and refined into handbook chapters.

In addition to the chapter list and descriptions, the handbook purpose, scope, and use is discussed. The unabridged list of topics is included in the book plan appendix.

17. Key Words
Verification, Validation, Systems,
Certification, Digital Avionics,
Integration, Circuit, Hardware,
Software, Control, Reliability, Safety

18. Distribution Statement
Document is available to the public
through the National Technical
Information Service, Springfield,
Virginia 22161

19. Security Classif. (of this report)
Unclassified

20. Security Classif. (of this page)
Unclassified

21. No. of Pages
17

22. Price

Reproduction of completed page authorized

TABLE OF CONTENTS

LIST OF ABBREVIATIONS AND ACRONYMS

AC	Advisory Circular
AGARD	Advisory Group for Aerospace Research and Development
AI	Artificial Intelligence
ARINC	Aeronautical Radio INCorporated
ASIC	Application Specific Integrated Circuit
ATC	Air Traffic Control
CASE	Computer-Aided Software Engineering
CISC	Complex Instruction Set Computer
DSP	Digital Signal Processor
EMI	ElectroMagnetic Interference
FAA	Federal Aviation Administration
FADEC	Full Authority Digital Engine Control
FAR	Federal Aviation Regulation
FMS	Flight Management System
GPS	Global Positioning System
HIRF	High-Intensity Radiated Fields
IEEE	Institute of Electrical and Electronics Engineers
LRU	Line Replaceable Unit
LSI	Large Scale Integration
NASA	National Aeronautics and Space Administration
RISC	Reduced Instruction Set Computer
RTCA	Requirements and Technical Concepts for Aviation (formerly Radio Technical Commission for Aeronautics)
SAE	The Engineering Society for Advancing Mobility Land Sea Air and Space (formerly Society of Automotive Engineers)
SPS	Standard Positioning System
TCAS	Traffic-Alert and Collision Avoidance System
VLSI	Very Large Scale Integration

DIGITAL SYSTEMS VALIDATION HANDBOOK
VOLUME III BOOK PLAN

1. INTRODUCTION

The Digital Systems Validation Handbook series had its beginnings in the mid-1970's. At that time, digital avionics represented a revolutionary trend. Certifying systems that used digital avionics raised complex issues not encountered in the analog world. Software and a host of new computer hardware devices came onboard aircraft. These newcomers played increasingly important roles in avionic systems.

In the 1990's, the seeds of digital technology sown in earlier times are reaching fruition. Individual systems have become complex and often are integrated with other systems. Even the definition of hardware and software has become less clear. Hardware devices such as Application Specific Integrated Circuits (ASICs) contain embedded code. New digital technology raises issues which challenge existing certification procedures and standards.

The environment in which aircraft operate has become increasingly complex. Aircraft population has swelled. As this occurs, aviation, navigation, and communication in the terminal area become more critical and more complex. An increasing number of entities exert control over the airspace. Air traffic control, airline operators, and sources of vital information such as weather services, interface with the aircraft and provide information which must be processed and acted upon by aircraft systems and the flight crew. In addition to numerous sources of information, unwelcome sources of noise, such as ElectroMagnetic Interference (EMI), have become more common.

Commercial transport aircraft hold an enviable safety record. The challenge of digital systems validation will be to maintain or surpass this safety record with aircraft, flight controls, and avionic systems of the future.

2. HANDBOOK PURPOSE

The Digital Systems Validation Handbook is designed to keep pace with emerging technology. It is a document that will grow and change in concert with technological developments. At the heart of the document is concern for safety. New technology may be more efficient or economical, but it must be proven safe. The intent of the handbook is to provide tutorials about current technology and issues related to digital flight control and avionic systems and certification. Each handbook chapter is a stand alone document. Combined, the chapters represent a collection of information relevant to new technology encountered by certification engineers.

Diverse viewpoints often arise during the development of new technology. Handbook chapters may present alternate viewpoints on specific topics. Also, the handbook may present alternate means of arriving at the same conclusion or output. The handbook presents guidance for understanding new digital flight control and avionic systems.

3. HANDBOOK SCOPE

The Digital Systems Validation Handbook is a tutorial series designed to provide certification engineers information on current topics related to digital flight control and avionic systems. The audience may include recent graduates who are new to certification, transfer personnel who may or may not be new to certification, seasoned certification engineers who require information about new digital technology, and others with interest in digital systems validation.

Handbook chapters are concise, well organized, and readable. The approximate length of each chapter text portion is 100 pages. Handbook chapters frequently are derived from technical reports. If additional information may be beneficial, the reader is encouraged to reference the more comprehensive technical report.

A number of caveats must be mentioned:

- Information included in handbook chapters represents material current at the time of chapter publication. The fast pace of technology may render information out of date past publication time. If funding permits, chapters may be revisited from time to time for updating and revision.

- Information presented in handbook chapters is meant to provide guidelines. Specific rules and requirements can be found in the appropriate government, military, or industry standards documents.

- In the interest of presenting a range of information, diverse or even contradictory viewpoints may be presented in a handbook chapter. References and bibliographic information will allow the reader to pursue additional information about specific viewpoints.

4. NEED FOR VOLUME III

As aircraft and the environment in which they operate become increasingly complex, certification engineers require more information and knowledge. The need for volume III is driven by the certification engineer's need for knowledge. Many sources of information are available on diverse topics. Few address the specific information and issues required by certification engineers. The Digital Systems Validation Handbook series synthesizes information from a variety of sources into a concise tutorial format. Information is gleaned from professional literature and from interviews with subject matter experts. While the presentation of information is concise, each handbook chapter contains an extensive bibliography which can be consulted for additional information about a specific topic.

Change, evolution, and revolution are words which describe progress in the field of digital technology. In addition to reporting new information, material presented in earlier volumes may need to be revisited for updates, expansion, and revision. Volume III will capture current information and present it to the certification engineer in a concise, readable format.

5. DETERMINING THE HANDBOOK TOPICS

The major task of the book plan was to identify approximately 20 topics to be incorporated into handbook chapters. It was suggested that a number of chapters be reserved for new technology or issues that might emerge during the course of the volume III life cycle. Sixteen potential chapters are identified in this plan. However, the entire list of topics is included in appendix A.

A number of steps were taken to determine topics to be included in volume III. Professional literature was surveyed for background information and to start a list of topics. Conferences and seminars were attended to identify additional topics and issues. Federal Aviation Administration (FAA) National Resource Specialists and experts in the field of certification and digital flight control and avionic systems and equipment were interviewed. National Aeronautics and Space Administration (NASA) officials and persons in private industry also were interviewed. These activities provided a basis for creating a list of topics.

5.1 Literature Review

A literature review was the first step toward developing a list of topics and served as preparation for interviews with subject matter experts. Periodicals such as Avionics, Aviation Week and Space Technology, and Institute of Electrical and Electronics Engineers (IEEE) periodicals feature reports of current and developing avionic technology and associated issues. Reports and conference proceedings were additional source of information. Reports and conference proceedings sponsored by the FAA, Human Factors Society, Advisory Group for Aerospace Research and Development (AGARD), American Institute of Aeronautics and Astronautics (AIAA), SAE, Incorporated (SAE, formerly Society of Automotive Engineers), IEEE, and NASA were examined. Standards such as RTCA/DO-160C and the recently issued RTCA/DO-178B were studied. In addition, recent books about digital avionics were reviewed.

The literature review provided a broad knowledge base for determining relevant topics. During the literature review a preliminary list of topics was compiled. This list was expanded and refined during the course of the book plan task.

5.2 Conferences and Seminars

Several conferences and seminars were attended. Keynote speakers, technical sessions by experts in the field, tutorials, exhibits, and informal conversations with persons in the field provided additional information for the topic list. Conferences and seminars attended included:

- 11th Digital Avionics Systems Conference, Seattle, Washington, October 5-8, 1992,
- Avionics Training Seminar, Small Airplane Directorate, Aircraft Certification Service, Kansas City, Missouri, December 8-9, 1993, and
- National Aerospace and Electronics Conference, Dayton, Ohio, May 24-28, 1993.

5.3 Interviews with FAA National Resource Specialists and Experts in the Field

Interviews with FAA National Resource Specialists and experts in the field provided additional information and helped refine the list of topics. Persons interviewed represented expertise in areas of hardware, software, avionic and electrical systems and equipment, verification and validation, and certification. In some cases, the experts shared information from the interview with members of their staff and were able to contribute additional topic input. A preliminary list of topics was shown to the experts for their comments and additions. For some topics the experts were able to recommend subject matter contacts and other resources.

In addition to topic input, there was discussion about expanding handbook utilization. It was suggested that the handbook series could provide an excellent source for training material. Handbook chapters could be used as textbooks, could become part of online databases, or could be adapted to a training medium such as computer-based instruction.

5.4 Topic Questionnaire

For additional input, a list of frequently mentioned topics was incorporated into an informal questionnaire. It was requested that respondents rank topics according to high, medium, or low priority. In addition, space was provided for respondents to suggest aspects of a topic to receive attention, to suggest additional topics, and to identify resources. The questionnaire was distributed to a small number of persons involved with digital flight control and avionic systems and certification. Eight questionnaires were returned.

5.5 Frequently Mentioned Topic Areas

During the course of compiling the list, and from responses to the questionnaire, several topic areas were mentioned frequently as having high priority. Software was one area. When computers came onboard aircraft, software came too. This newcomer continues to present verification and validation challenges. Certification engineers must have knowledge of topics such as software architecture and code, engineering tools used for software development, techniques of modeling and simulation, and software assessment to perform their jobs effectively.

Avionic Systems was another topic area frequently mentioned. Systems are becoming increasingly complex and interrelated. In addition to understanding how a specific system works, certification engineers must understand how these systems function in conjunction with other systems and in the overall aircraft environment.

Specific technology received mention. Technology such as the Global Positioning System (GPS) and data link affect the aircraft and the airspace environment. This technology will be quite influential in the near future.

6. HANDBOOK TOPICS

Based on input from literature searches, conference and seminar attendance, interviews, and questionnaires, 16 topics were selected:

- Formal Methods,
- Software Verification and Validation,
- Certification Issues for Digital Technology,
- Verification of Complex Hardware Circuitry,
- Global Positioning System,
- Validation of Artificial Intelligence (AI) Systems,
- Complex Integrated Systems,
- Computer-Aided Engineering Tools,
- High-Intensity Radiated Fields (HIRF) Update,
- Object Oriented Software Engineering,
- Data Link,
- Engine Control Systems,
- Modeling and Simulation,
- Fly-By-Light/Power-By-Wire,
- Flight Management Systems, and
- Digital Processors.

FORMAL METHODS

Formal methods is a means of managing the process of hardware or software development. It involves the application of rigorous mathematical proofs to verify hardware or software models. The ultimate goal of formal methods is defect prevention. Formal methods are especially relevant to life-critical computer hardware and software applications. Although current formal methods tools are tedious and difficult to use, it is anticipated that breakthroughs in tool development will allow some steps to be automated. As digital flight control and avionic systems dominate aircraft systems of the future, application of formal methods to the verification and validation processes will become accepted practice.

SOFTWARE VERIFICATION AND VALIDATION

With the advent of computer-driven avionic systems, the role of software verification and validation has become increasingly important. This chapter will examine topics such as process assessment, the use of fault trees, software safety analysis, and assessment of multitasking systems.

CERTIFICATION ISSUES FOR DIGITAL TECHNOLOGY

Digital flight control and avionic systems present new certification challenges. This chapter presents an overview of issues related to hardware, software, firmware, and systems as well as issues related to the certification environment.

CERTIFICATION ISSUES FOR COMPLEX HARDWARE CIRCUITRY

Complex hardware circuitry such as ASICs are becoming prevalent in digital avionics. ASICs allow designers to embed custom logic within a hardware device. Although ASICs and other complex hardware circuitry enhance design capabilities, they present a number of certification issues. This chapter will present a complex hardware circuitry tutorial and raises related certification issues.

GLOBAL POSITIONING SYSTEM

GPS is a Department of Defense navigation system. The original purpose of GPS was to provide a highly precise military navigation and positioning system. GPS is operated by the U.S. Air Force and a Standard Positioning System (SPS) will be available for civilian use. When complete, the GPS will consist of 21 satellites and 3 active spares configured in 6 orbital planes. GPS provides highly accurate position and velocity information, as well as precise time. When fully implemented, GPS will make information available world wide, 24 hours a day. A GPS tutorial and related certification issues will be presented in this chapter.

VERIFICATION AND VALIDATION OF ARTIFICIAL INTELLIGENCE SYSTEMS

As AI systems are developed for avionic use, methods for verification and validation of these systems also must be developed. Current and proposed methods for verification and validation of AI systems will be examined in this chapter.

COMPLEX INTEGRATED SYSTEMS

The concept of modular avionics as discreet Line Replaceable Units (LRUs) is being replaced by the concepts of interoperability, integrated modular avionics, and systems. Issues such as fault tolerance, reliability, maintainability, and verification and validation of complex integrated systems will be examined.

COMPUTER-AIDED ENGINEERING

Computer-aided software and hardware engineering allows avionic engineers to use computer-based tools to assist the avionic design process. This chapter will present an overview of computer-aided tools and applications. Software applications such as object-oriented design, structure-based testing, and compilers will be discussed. In addition, the chapter will include hardware and software tools, rapid prototyping, development tools, and conceptualization and realization.

HIGH-INTENSITY RADIATED FIELDS

Research pertaining to High-Intensity Radiated Fields (HIRF) was presented in volume II of the handbook. Since that time, new digital systems and circuit elements, new airframe materials, and new and additional ground sources of HIRF have come into existence. This chapter will revisit HIRF and the certification issues associated with this field.

OBJECT-ORIENTED SOFTWARE ENGINEERING

Object-oriented software engineering is based on relationships among objects. It makes use of Computer-Aided Software Engineering (CASE) tools, libraries, and reusable specifications and code. Object-oriented software engineering will be described and associated certification issues examined in this chapter.

DATA LINK

Data link is a promising communication technology that allows exchange of information between a cockpit computer and a ground facility. Some data link applications include sending and receiving routine flight information messages, weather data, air traffic control instructions and clearances, Air Traffic Control (ATC) flight safety messages, windshear alert messages, and distress calls and messages. A data link tutorial will be presented in this chapter.

ENGINE CONTROL SYSTEMS

Full Authority Digital Engine Control (FADEC) systems have replaced hydromechanical engine control systems in modern commercial aircraft. FADEC systems offer advantages such as less engine wear, improved troubleshooting and maintenance procedures, reduced pilot workload, and more accurate response to engine operation. This chapter will describe FADEC systems and related certification issues.

MODELING AND SIMULATION

Modeling and simulation affect avionics from design through certification. Among many uses, modeling and simulation can be used to aid design decisions, develop rapid prototypes, assist in training, aid verification and validation procedures, and fulfill requirements for certification when actual flight tests would be too dangerous or impractical. Modeling and simulation techniques and issues will be examined in this chapter.

FLIGHT MANAGEMENT SYSTEMS

Flight Management Systems (FMSs) integrate the functions of navigation, guidance, and performance management. The structure and function of FMSs will be explained. FMSs in use today and systems projected for future aircraft will be described. Certification issues for these integrated systems will be raised.

FLY-BY-LIGHT/POWER-BY-WIRE

Optics offer promising advantages for digital avionics systems. Among these advantages are greater data handling capacity, immunity to electromagnetic interference, reduced weight and size, and no electrical fire hazard. This chapter presents an optics tutorial.

DIGITAL PROCESSORS

Digital avionics make use of many types of processors. Processors such as Reduced Instruction Set Computer (RISC), Complex Instruction Set Computer (CISC), Digital Signal Processor (DSP), fuzzy logic, array, parallel, bit slice, neural network, and custom Large Scale Integration (LSI) and Very Large Scale Integration (VLSI) are in use or in development. This report will examine the architecture and implementation of these processors. Developments and trends in processor technology as well as issues pertaining to processor certification will be discussed.

7. HOW TO USE THE HANDBOOK

The handbook is designed as a tool to enable certification engineers to keep up to date on specific topics and certification issues related to digital avionic systems. Individual chapters may be used as stand alone documents or the entire series may be considered an anthology of current topics in digital avionics.

It is the intent of the handbook series to provide timely information. Therefore, handbook chapters will be distributed as they are published. In addition to text, each chapter will contain user aids such as table of contents, acronym and abbreviation list, glossary, bibliography, and index. In addition, a composite volume table of contents, acronym and abbreviation list, glossary, bibliography, and index will be provided. Volume user aids will contain information from individual chapters.

Individual chapters contain information about specific topics. However, some topics may be cited in a number of chapters. For example, a certification engineer may need information about certification regulations and guidelines for a variety of topics. The handbook volume table of contents, index, or bibliography could be consulted for guidance to the appropriate information.

The handbook can be used as a global reference source, a tutorial for specific topics, or a starting point for intensive research. The handbook is a reference tool, a field tool, an instructional tool, and a research tool.

8. HANDBOOK CHAPTERS AND DELIVERABLE ACTIVITIES

Specific activities will lay the foundation for work on each chapter to be included in volume III of the handbook. Handbook chapters will follow the format described in the Handbook Volume III Digital Systems Validation Author's Guide. When funded and activated, each chapter will include the following activities:

- Developing a topic management plan and topic outline,
- Reviewing existing technical literature,
- Performing automated searches of existing literature and abstract databases to investigate additional materials,
- Interviewing subject matter experts,
- Developing a tutorial which:
  - Defines the relevance of materials to current Federal Aviation Regulations (FARs), Advisory Circulars (ACs), special conditions, issue papers, or currently accepted aerospace practices and procedures as defined by Requirements and Technical Concepts for Aviation (RTCA, formerly Radio Technical Commission for Aeronautics), SAE, Aeronautical Radio INCorporated (ARINC), and others,
  - Develops guidance material, explanatory material, and worked examples that provide information and input data to certification engineers so that they can understand technological material being presented for FAA review and approval,
- Developing, preparing, and delivering a draft tutorial based on the material generated in the above activities, and
- Delivering the final tutorial.

APPENDIX A

COMPLETE LIST OF SUGGESTED HANDBOOK TOPICS

- Active Control Systems
- Ada Tutorial
- Aeronautical Telecommunication Network
- Aircraft Cooling Systems
- Aircraft Information Management Systems
- Analysis of Time Limited Dispatch (dispatching planes with faults)
- Applicability of MIL-217
- Certification Credit for Service History
- Certification Issues for Digital Technology
- Complex Systems
- Computer-Aided Engineering Tools
  - Compilers
  - Conceptualization/realization
  - Development tools
  - Rapid prototyping
  - Software tools
  - Structure-based testing
  - Tool qualification
- Computer-Driven Inspection Devices
- Data Communications
- Data Storage on Magnetic Media
- Data Link
  - Airborne
  - Gate link
  - Oceanic
  - Traffic-Alert and Collision Avoidance System (TCAS)
- Electric Power
  - Centralized vs. distributed
  - Electric actuators
  - Power management and distribution
  - Starters/generators
- Engine Control Systems
- Environmental Qualification of Software
- Environmental Effects on Digital Systems
- Failure Mode and Effects Simulation
- Fault Tolerance
- Flight Management Systems
- Flight Data Recorders

- Fly-by-Light/Power-by-Wire
- Generic Design Errors in Complex Hardware
- Global Positioning System
- Hardware Reliability
- High-Intensity Radiated Fields (HIRF)/Lightning (revisited)
    - Avionic bay cavity response
    - Computer modeling
    - Reverberation chamber testing
    - System-level upset detection
- Integrated Modular Avionics
- Integrating Systems on a Bi-Directional Data Bus
- Introduction to Optics
    - Bus architecture
- Maintainability
- Markov Analysis
- Multitasking Systems
- Neural Networks
- Object Oriented Design
- Overview - Emerging Hardware Technologies
- Process Assessment
- Process of designing hardware systems
- Reconfigurable Hardware at Chip Level
- Reduced Instruction Set Computer (RISC) Processors
- RTCA/DO-178B: "Software Considerations In Airborne Systems and Equipment Certification"
- Safety in Software
    - End to end safety assessment in the multi-institutional air space environment)
    - Software safety analysis
- Security of Navigation/Communication Systems
- Simulation
- Software Assessment
    - Commercial off the shelf software
    - Reusable specifications
    - Reusable software
    - Use of fault trees
    - User loadable software
- Software Certification
- Software Reliability
- Software Verification and Validation (revisited)
- Supplemental Type Certification Procedure
- Synthetic Vision
- System Reliability
- Systems Integration