RTCA, Inc.
1828 L Street, NW, Suite 805
Washington, D.C. 20036-5133 USA

Safety Requirements Standard for Aeronautical Operational Control (AOC) Datalink Messages

RTCA DO-296
October 19, 2004

Prepared by: SC-201
© 2004 RTCA, Inc.

Copies of this document may be obtained from

RTCA, Inc.

Telephone: 202-833-9339
Facsimile: 202-833-9434
Internet: www.rtca.org

Please visit the RTCA Online Store for document pricing and ordering information.

FOREWORD

This guidance document was prepared by Special Committee 201 (SC-201) and approved by the RTCA Program Management Committee (PMC) on October 19, 2004.

RTCA, Incorporated is a not-for-profit corporation formed to advance the art and science of aviation and aviation electronic systems for the benefit of the public. The organization functions as a Federal Advisory Committee and develops consensus-based recommendations on contemporary aviation issues. RTCA's objectives include but are not limited to:

- Coalescing aviation system user and provider technical requirements in a manner that helps government and industry meet their mutual objectives and responsibilities;

- Analyzing and recommending solutions to the system technical issues that aviation faces as it continues to pursue increased safety, system capacity and efficiency;

- Developing consensus on the application of pertinent technology to fulfill user and provider requirements, including development of minimum operational performance standards for electronic systems and equipment that support aviation; and

- Assisting in developing the appropriate technical material upon which positions for the International Civil Aviation Organization and the International Telecommunication Union and other appropriate international organizations can be based.

The organization's recommendations are often used as a basis for government and private sector decisions as well as the foundation for many Federal Aviation Administration Technical Standard Orders.

Since RTCA is not an official agency of the United States Government, its recommendations may not be regarded as statements of official government policy unless so enunciated by the U.S. government organization or agency have statutory jurisdiction over any matters to which the recommendations relate.

This Page Intentionally Left Blank.

TABLE OF CONTENTS

1 INTRODUCTION 1

1.1 BACKGROUND 1
1.1.1 Relationship to Flight Safety and Efficiency 2
1.1.2 Regulatory Means of Compliance 3
1.2 PURPOSE 4
1.3 SCOPE 4
1.4 DESCRIPTION OF THIS DOCUMENT 5
1.4.1 Mandating and Recommending Phrases 5
1.4.2 Document Organization 6
1.4.3 How to Comply With The Guidelines of This Document 6
1.4.4 Acronyms 7
1.4.5 Glossary of Terms 8
1.5 REFERENCES 10

2 AOC DATALINK MESSAGES 11

2.1 OPERATIONAL OBJECTIVES 11
2.2 ENVIRONMENTAL CONSIDERATIONS 12

3 GUIDELINES FOR APPROVAL OF AOC DATALINK MESSAGES 13

3.1 TYPE DESIGN APPROVAL 13
3.2 OPERATIONAL APPROVAL 14
3.2.1 AOC Datalink Message Identification 15
3.2.2 Assess AOC System Design Assurance Level 15
3.2.3 Assess Failures During Transmission For Each AOC Messages 16
3.2.4 Classify AOC Message Failure Effects Upon the Aircraft, Aircrew and Passengers 17
3.3 RISK REDUCTION STRATEGIES 18
3.3.1 Establish the Need for Risk Reduction Strategies 19
3.3.2 Architectural Risk Reduction Strategies 20
3.3.3 Procedural Risk Reduction Strategies 20
3.3.4 Operational Environment Considerations 21

4 RECOMMENDATIONS 25

4.1 RECOMMENDATIONS FOR FAA AIRCRAFT CERTIFICATION SERVICE 25
4.1.1 Recommendation 25
4.1.2 Recommendation 25
4.1.3 Recommendation 25
4.2 RECOMMENDATIONS FOR FAA FLIGHT STANDARDS SERVICE 26
4.2.1 Recommendation 26
4.2.2 Recommendation 26
4.2.3 Recommendation 26
4.2.4 Recommendation 26
4.2.5 Recommendation 26
4.2.6 Recommendation 27
4.2.7 Recommendation 27

4.3 RECOMMENDATIONS FOR OPERATORS 27
4.3.1 Recommendation 27
4.3.2 Recommendation 27

MEMBERSHIP 29

APPENDIX A - APPLICATION OF GUIDELINES FOR APPROVAL OF AOC DATALINK MESSAGES – WEIGHT AND BALANCE 1

1 INTRODUCTION 1

2 OPERATIONAL APPROVAL 1

2.1 IDENTIFY MESSAGE 1
2.2 ASSESS AOC SYSTEM DESIGN ASSURANCE LEVEL 2
2.3 ASSESS FAILURES/CLASSIFY EFFECTS 2
2.4 ESTABLISH NEED FOR RISK REDUCTION 3
2.5 IDENTIFY RISK REDUCTION STRATEGIES 3

3 OPERATIONAL APPROVAL CHECKLIST FOR WEIGHT AND BALANCE MESSAGE 6

APPENDIX B – APPLICATION OF GUIDELINES FOR APPROVAL OF AOC DATALINK MESSAGES – TAKEOFF DATA 1

1 INTRODUCTION 1

2 OPERATIONAL APPROVAL 1

2.1 IDENTIFY MESSAGE 1
2.2 ASSESS AOC SYSTEM DESIGN ASSURANCE LEVEL 1
2.3 ASSESS FAILURES/CLASSIFY EFFECTS 1
2.4 ESTABLISH NEED FOR RISK REDUCTION 2
2.5 IDENTIFY RISK REDUCTION STRATEGIES 2

3 OPERATIONAL APPROVAL CHECKLIST FOR TAKEOFF DATA MESSAGE .5

APPENDIX C – APPLICATION OF GUIDELINES FOR APPROVAL OF AOC DATALINK MESSAGES – PRE-DEPARTURE CLEARANCE 1

1 INTRODUCTION 1

2 OPERATIONAL APPROVAL 1

2.1 IDENTIFY MESSAGE 1
2.2 ASSESS AOC SYSTEM DESIGN ASSURANCE LEVEL 2
2.3 ASSESS FAILURES/CLASSIFY EFFECTS 2
2.4 ESTABLISH NEED FOR RISK REDUCTION 3
2.5 IDENTIFY RISK REDUCTION STRATEGIES 4

3 OPERATIONAL APPROVAL CHECKLIST FOR PRE-DEPARTURE CLEARANCE MESSAGE 6

APPENDIX D – APPLICATION OF GUIDELINES FOR APPROVAL OF AOC DATALINK MESSAGES – DIGITAL-AUTOMATIC TERMINAL INFORMATION SYSTEM 1

1 INTRODUCTION 1

2 OPERATIONAL APPROVAL 1

2.1 IDENTIFY MESSAGE 1
2.2 2.1-3 D-ATIS SUPPLEMENTS THE EXISTING VOICE BROADCAST ATIS. ASSESS AOC SYSTEM DESIGN ASSURANCE LEVEL 1
2.3 ASSESS FAILURES/CLASSIFY EFFECTS 1
2.4 ESTABLISH NEED FOR RISK REDUCTION 3
2.5 IDENTIFY RISK REDUCTION STRATEGIES 3

3 OPERATIONAL APPROVAL CHECKLIST FOR D-ATIS MESSAGE 5

APPENDIX E – APPLICATION OF GUIDELINES FOR APPROVAL OF AOC DATALINK MESSAGES – OCEANIC CLEARANCE (OCX) 1

1 INTRODUCTION 1

2 OPERATIONAL APPROVAL 1

2.1 IDENTIFY MESSAGE 1
2.2 ASSESS AOC SYSTEM DESIGN ASSURANCE LEVEL 1
2.3 ASSESS FAILURES/CLASSIFY EFFECTS 1
2.4 ESTABLISH NEED FOR RISK REDUCTION 2
2.5 IDENTIFY RISK REDUCTION STRATEGIES 3

3 OPERATIONAL APPROVAL CHECKLIST FOR OCEANIC CLEARANCE MESSAGE 5

APPENDIX F – OPERATIONAL APPROVAL CHECKLIST 1

Table of Figures

Figure 1-1: Overview of datalink system with AOC source 2
Figure 1-2: Flowchart of AOC Message Operational Approval Process 7
Figure 2-1: Examples of AOC Datalink Messages 11
Figure 2-2: AOC Message Environment 12

Table of Tables

Appendix A
Table A-1 - Weight and Balance Message Hazard Identification/Classification A-3
Table A-2 - Example Risk Reduction Strategies for Undetected Loss of Amended Weight and Balance Function (WB-H-2) A-4
Table A-3 - Example Risk Reduction Strategies for Undetected Misdirection of Weight and Balance Function (WB-H-4) A-4
Table A-4 - Example Risk Reduction Strategies for Undetected Corruption of Weight and Balance Function (WB-H-6) A-5

Appendix B
Table B-1 - Takeoff Data Message Hazard Identification/Classification B-2
Table B-2 - Example Risk Reduction Strategies for Undetected Loss of Amended Takeoff Data (TD-H-2) B-3
Table B-3 - Example Risk Reduction Strategies for Undetected Misdirection of Takeoff Data (TD-H-4) B-3
Table B-4 - Example Risk Reduction Strategies for Undetected Corruption of Takeoff Data (TD-H-6) B-4

Appendix C
Table C-1 - Pre-Departure Clearance Message Hazard Identification/Classification C-2
Table C-2 - Risk Reduction Strategies for Undetected Loss of a Revision to PDC (PDC-H-4) C-4
Table C-3 - Risk Reduction Strategies for Undetected Misdirection of PDC Information (PDC-H-8) C-4
Table C-4 - Example Risk Reduction Strategies for Undetected Corruption of PDC Information (PDC-H-10) C-5

Appendix D
Table D-1 - D-ATIS Data Message Hazard Identification/Classification D-2
Table D-2 - Example Risk Reduction Strategies for Undetected Loss of Revision to Local Terminal Information (D-ATIS-H-3) D-3
Table D-3 - Example Risk Reduction Strategies for Undetected Misdirection of Local Terminal Information (D-ATIS-H-7) D-4
Table D-4 - Example Risk Reduction Strategies for Undetected Corruption of Local Terminal Information (ATIS-H-10) D-4

Appendix E
Table E-1 - Oceanic Clearance (OCX) Message Hazard Identification/Classification E-2
Table E-2 - Example Risk Reduction Strategies for Undetected Loss of Amended Oceanic Clearance Function (OCX-H-2) E-3
Table E-3 - Example Risk Reduction Strategies for Undetected Misdirection of Oceanic Clearance (OCX) Function (OCX-H-4) E-3
Table E-4 - Example Risk Reduction Strategies for Undetected Corruption of Oceanic Clearance Function (OCX-H-6) E-4

1 INTRODUCTION

This document provides minimum safety requirements for Aeronautical Operational Control (AOC) and certain Air Traffic Services (ATS) datalink messages. The two means of addressing the hazards identified in this document are approval via design assurance alone or design assurance in conjunction with risk reduction strategies. To satisfy regulatory means of compliance, the solution must provide adequate assurance that the parts of the AOC datalink system, when operating together, will perform their intended function for the purpose of receiving and displaying/printing AOC data messages within the datalink system in an acceptably safe manner. These datalink system components comprise the ground airline host, datalink service provider and aircraft system. This document provides recommendations of alternative strategies that could be used to demonstrate to a regulatory authority a composite approach to safety that is deemed equivalent to that provided solely by a design assurance solution.

1.1 BACKGROUND

1.1-1 Aeronautical Operational Control messages are typically exchanged with ground system components via aircraft equipment commonly referred to as the Aircraft Communications Addressing and Reporting System (ACARS). The ACARS was originally certified on a "non-interference, no hazard" basis. This approval basis allowed for installation of datalink equipment without having to assess the hardware/software design assurance considerations. Airworthiness authorities accepted this basis because the initial intended uses of datalink had no impact on safety, e.g., the operational basis for approval was intended for Aeronautical Administrative Communication (AAC) only. Datalink has evolved to include applications for AOC and ATS communications. **The anomalous behavior of AOC and ATS applications has the potential to affect the safety of operations by contributing to major category hazards as defined in various aircraft certification advisory material in compliance with AC 25.1309-1A. A higher severity classification is excluded from evaluation using this document.**

1.1-2 Guidance for the design approval of airborne data communication equipment is provided in FAA Advisory Circular (AC) 20-140. RTCA and EUROCAE committees and working groups, such as RTCA SC-189/EUROCAE WG-53, are also producing documents to provide for identification and coordination of safety, performance, and interoperability of ATS datalink messages. There is no commensurate guidance, nor standards, for AOC datalink messages.

1.1-3 Currently, Airplane Flight Manual (AFM) or Rotorcraft Flight Manual (RFM) limitations require flight crew "procedural" risk reduction strategies to provide adequate protection against major hazards. However, based on procedures approved by Operations Specifications (OpSpecs) and relevant service experience, operators are confident that the datalink and associated procedures are adequate for the intended AOC uses without the need for AFM/RFM limitations.

1.1-4 Additionally, airworthiness authorities are concerned with potential error sources which are not part of the aircraft architecture, but which may contribute to aircraft level hazards. This includes procedural errors on the flight deck and within company AOC,

© RTCA, Inc. 2004

and systems and equipment that are not on the aircraft. Figure 1-1 provides an overview of a typical datalink system with a company's AOC source. The Figure was taken from FAA AC 20-140 and adapted for AOC operations. Traditional aircraft certification requires a system safety assessment to evaluate anomalous aircraft system behavior. Based on the results of a functional hazard assessment, various means are applied to mitigate the risks of the anomalous behavior to an acceptable confidence level. The confidence level will vary depending on the severity of the effects of the anomalous behavior of the system. The FAA airworthiness certification processes currently do not adequately address potential error sources that are outside the aircraft environment, specifically when evaluating AOC applications.

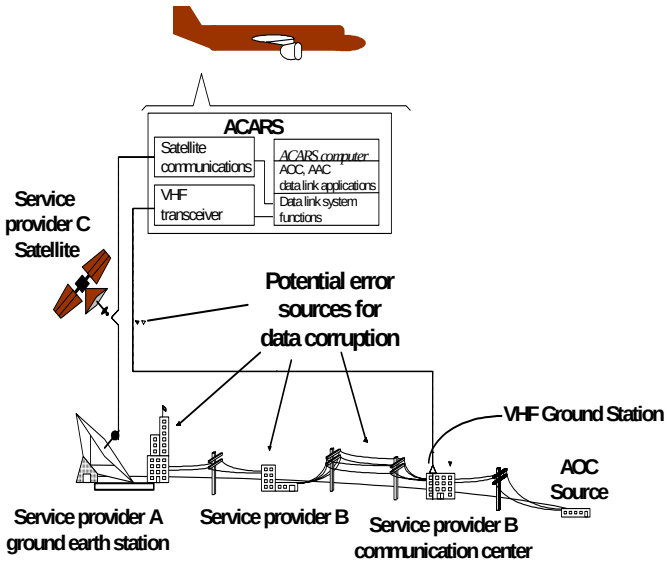


Figure 1-1: Overview of datalink system with AOC source

1.1.1 Relationship to Flight Safety and Efficiency

1.1.1-1 The importance of expedient and efficient delivery of AOC datalink messages to the operator, in terms of both safety and regularity of flight, cannot be overestimated. Centralized calculation of takeoff parameters takes into account information collected from various sources. This information converges only at the operator's AOC facility. Without the ability to deliver the results of these calculations directly to the cockpit, the operator would not be able to maintain their schedules during high volume periods at the major airports.

1.1.1-2 Any interruption or impact to AOC datalink message delivery would require use of an alternative or supplemental means of communicating the same information to the flight crew. Current AOC architecture and operations require that voice communications or "hard copy delivery" be used as the alternate or supplemental means of communication.

© RTCA, Inc. 2004

1.1.1-3 In developing this document and its recommendations, care was taken to balance the datalink-centric communication scheme against alternative communication schemes. While the datalink has potential error sources, its advantages include known performance and efficiency. Utilizing other communications methods with little or no relevant service history for these applications would introduce greater problems. Still other methods, such as voice delivery via radio or printed hard-copy from the gate, have been superceded by datalink messages for good reasons.

1.1.2 Regulatory Means of Compliance

1.1.2-1 FAA Advisory Circular (AC) 20-140, Guidelines for Design Approval for Aircraft Data Communication Systems, identifies objectives which provide a means of compliance to 14 Code of Federal Regulations (CFR) Parts 23, 25, 27 and 29. AC 20-140 requires the applicant for data communication equipment installation to identify the intended operational environment, perform a safety assessment, classify resultant hazards, and allocate safety requirements. In accordance with this published criteria, the FAA Aircraft Certification Service has made a determination that certain AOC messages viewed in the cockpit have a potential to present a major category hazard if they are lost, delayed, misdirected or corrupted. Since datalink has only been certified to minor hazard category criteria, applicants for datalink equipment installation are required to identify and allocate means of mitigating those hazards.

1.1.2-2 A commensurate means of compliance in the form of FAA Advisory Circular material for the operational approval and use of AOC datalink messages does not exist (i.e., means of compliance to 14 CFR Parts 91, 121, 135, 139).

1.1.2-3 AAC and AOC messages, carried over datalink, have been used for many years by many operators. However, until recently, the use of these messages has not been formally evaluated as part of the type design approval (e.g., 14 CFR Part 25), but have been approved as part of their operational approval process (e.g., 14 CFR Part 121) using operational risk reduction strategies. Recently, operators expressed the concern that the split approach to AOC data communication approval has the potential to result in the FAA imposing additional means of hazard risk reduction which could result in tremendous costs to the operators. Therefore, the FAA and industry agreed to identify a standardized means of addressing safety considerations for AOC datalink communications.

1.1.2-4 The regulatory approval of the datalink equipment is accomplished in two parts. The FAA type design approval will demonstrate the operational software to the standards referenced in RTCA DO-178B Level D and to FAA AC 20-140. In addition, functions such as company menu and uplink and downlink formats and content have been evaluated and determined to be modifiable without further FAA type design finding of compliance. FAA operational authorities are responsible for approval of changes to the user modifiable software. The operator is responsible to ensure that further hazards have not been introduced.

1.1.2-5 The regulatory approval of the content and use of AOC messages installed into the datalink system after type design approval are currently covered by operational approvals. These operational approvals are typically not coupled to the type design approval basis of the airborne equipment. This lack of a common basis for approval and

© RTCA, Inc. 2004

coordination of requirements between the type design and operational approval processes (or the mechanism to utilize operational approvals to mitigate shortcomings in design assurance considerations) has led to the incorporation of restrictive AFM/RFM Section 1 Limitation wording.

1.1.2-6 As a result of these concerns, industry petitioned RTCA to form a group to produce a document which would describe acceptable risk reduction strategies for those AOC datalink messages deemed to pose a major hazard if delayed, lost, misdirected or corrupted. The goal is for the FAA to participate in the process and to take the resultant RTCA guidance material and invoke it as formal guidance on the subject. The FAA adoption of the resultant guidance material is expected to be via policy memoranda, advisory circular, operations specification material, etc. With such a mechanism available to the operators and FAA, the need for AFM/RFM limitations related to these concerns would be obviated. This group was officially sanctioned as RTCA Special Committee 201.

1.2 PURPOSE

The purpose of this document is to define the set of recommendations for the operational and safety aspects for implementations of AOC datalink messages. This document will identify risk reduction strategies for datalink messages that support AOC messages, provide specific examples of AOC message risk reduction strategies, and offer forth recommendations to regulatory authorities on how to streamline the regulatory approval process.

1.3 SCOPE

1.3-1 This document addresses risk reduction strategies for aircraft hazards resulting from structured uplink, structured downlink and free text (uplink and downlink) messages irrespective of the system components (e.g., ground airline host, datalink service provider and aircraft system) which may contribute toward those hazards. 1.3-2 The scope of this document includes the definition of relevant AOC or ATS datalink messages, the environmental characteristics relevant to the implementation of those datalink messages, and the operational and safety requirements for using the datalink messages to facilitate AOC and related flight operations.

1.3-3 Aeronautical operations in which the datalink will be used for AOC communications (i.e., datalink messages) shall be evaluated to determine if the AOC datalink equipment has the appropriate design assurance level. For those aircraft which can demonstrate that the AOC datalink equipment or the end system (e.g., flight management computer) has been developed commensurate with the hazard level associated with an identified message element (e.g., DO-178B Level C, DO-254 Level C for a major hazard), identification of risk reduction strategies shall not be required.

1.3-4 Relevant AOC or ATS datalink messages have either not been certified to the appropriate design assurance level by type design approval as part of the evaluation of datalink avionics equipment or are not included in type design evaluation because they are implemented within user modifiable partitions.

© RTCA, Inc. 2004

1.3-5 The datalink messages of primary focus are described in detail in Appendices A through E. They are:

a) Weight and balance - Data that is required to assure that the aircraft operates within its design operational limits, including zero fuel weight, gross weight, center of gravity (e.g., distribution of fuel, passengers and cargo).

b) Takeoff data - Data that is used to assure that the aircraft operates within its design operational limits such as V-speeds, aircraft configuration (e.g., flaps, slats and stab trim), power settings, runway limits and takeoff gross weight.

c) Pre-Departure Clearance – The pre-departure clearance is generated by the Air Traffic Service authority as a non-voice clearance to proceed with the requested flight plan. This clearance is transmitted to the aircraft prior to the departure phase of flight. It is normally transmitted when the aircraft is at the gate prior to taxi.

d) Digital Automatic Terminal Information Service – The D-ATIS service provides automated assistance in requesting and delivering air traffic information including: meteorological conditions, operating procedures, runways and approaches in use, and various other information which may affect the departure, approach and landing flight phases as well as surface operations. The D-ATIS information is updated upon the issuance of a new weather report, or when conditions or procedures affecting various components of the D-ATIS message change by specified criteria.

e) Oceanic Clearance - The oceanic clearance message is transmitted to an aircraft prior to entrance into a controlled oceanic airspace to notify the aircrew of the entry point or latitude/longitude, entry time, altitude, speed and route of flight. It could additionally include Reclearance and Free Text information.

Note 1: The guidelines contained in this document are not intended to limit the use of an implementation only to the AOC datalink messages and operational context defined herein. However, in cases where it is intended to support other AOC operations or define new AOC datalink messages, the safety requirements will need to be established as a basis for approval.

Note 2: Requirements related to securing datalink messages that would provide for protection against malicious or intentional behavior to cause harm are beyond the scope of this document.

1.4 DESCRIPTION OF THIS DOCUMENT

1.4.1 Mandating and Recommending Phrases

The main body of this document contains “shall” and “should” statements with the following meanings:

- The use of the word “shall” indicates a requirement on the AOC datalink service, the aircraft equipage, or procedure.

© RTCA, Inc. 2004

- The use of the word "should" indicates a guideline for assessments, developing new requirements, or providing assurance that an implementation satisfies a requirement. In such cases, where an applicant deviates from guidelines, alternatives should be identified in appropriate approval plans and agreement sought from the approval authority.

1.4.2 Document Organization

- Section 1 provides an introduction, background and description of how to comply with this document.
- Section 2 provides a description of the operational objectives and environment for AOC datalink messages.
- Appendix A provides acceptable risk reduction strategies for the weight and balance message.
- Appendix B provides acceptable risk reduction strategies for the takeoff data message.
- Appendix C provides acceptable risk reduction strategies for the pre-departure clearance message.
- Appendix D provides acceptable risk reduction strategies for the D-ATIS message.
- Appendix E provides acceptable risk reduction strategies for the oceanic clearance message.
- Appendix F provides a compliance checklist.
- Appendix G is a listing of all members of Special Committee 201.

1.4.3 How to Comply With The Guidelines of This Document

1.4.3-1 The guidance material contained in this document recommends minimum acceptable criteria for the regulatory approval of AOC datalink communication systems. This guidance material is in the form of requirements and evidence of compliance. Requirements refer to those activities necessary to demonstrate compliance with specific document objectives. For each requirement, evidence of compliance must be submitted either as part of the installation (aircraft type design) approval or operator (operational) approval.

1.4.3-2 The following flowchart shows the operational approval process for AOC datalink messages.

© RTCA, Inc. 2004