

Process management for avionics — Atmospheric radiation effects —

Part 3: Optimising system design to accommodate the single event effects (SEE) of atmospheric radiation

ICS 31.020; 49.060

National foreword

This Draft for Development is the UK implementation of IEC/TS 62396-3:2008. It supersedes DD IEC/PAS 62396-3:2007 which is withdrawn.

This publication is not to be regarded as a British Standard.

It is being issued in the Draft for Development series of publications and is of a provisional nature. It should be applied on this provisional basis, so that information and experience of its practical application can be obtained.

Comments arising from the use of this Draft for Development are requested so that UK experience can be reported to the international organization responsible for its conversion to an international standard. A review of this publication will be initiated not later than three years after its publication by the international organization so that a decision can be taken on its status. Notification of the start of the review period will be made in an announcement in the appropriate issue of *Update Standards*.

According to the replies received by the end of the review period, the responsible BSI Committee will decide whether to support the conversion into an international Standard, to extend the life of the Technical Specification or to withdraw it. Comments should be sent to the Secretary of the responsible BSI Technical Committee at British Standards House, 389 Chiswick High Road, London W4 4AL.

The UK participation in its preparation was entrusted to Technical Committee GEL/107, Process management for avionics.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

This Draft for Development was published under the authority of the Standards Policy and Strategy Committee on 31 October 2008

© BSI 2008

ISBN 978 0 580 62278 6

Amendments/corrigenda issued since publication

Date	Comments

TECHNICAL SPECIFICATION

**Process management for avionics – Atmospheric radiation effects –
Part 3: Optimising system design to accommodate the single event effects (SEE)
of atmospheric radiation**

CONTENTS

INTRODUCTION.....	3
1 Scope and object.....	4
2 Normative references	4
3 Terms and definitions	4
4 Process guidance (see Annex A)	7
5 Atmospheric radiation and electronic system faults.....	8
5.1 Atmospheric radiation effects on avionics	8
5.2 Hard faults	9
5.3 Soft faults.....	10
6 Aircraft safety assessment.....	10
6.1 Methodology.....	10
6.2 Mitigation (see Annex B)	11
6.3 Specific electronic systems (see Annex C)	11
6.3.1 Level A systems	11
6.3.2 Level B systems	14
6.3.3 Level C systems	15
6.3.4 Level D and E systems	15
Annex A (informative) Design process flow diagram for SEE rates	16
Annex B (informative) Some mitigation method considerations for single event effects	17
Annex C (informative) Example systems	20
Bibliography.....	23
Figure C.1 – Electronic equipment (flight control computers)	20
Figure C.2 – Electronic equipment (flight director computers)	21
Figure C.3 – Electronic equipment (engine control).....	21
Figure C.4 – Electronically powered surface	22
Figure C.5 – Hydromechanical drive of surface – electronic valve control	22
Table 1 – Failure effect and occurrence probability	11

INTRODUCTION

This industry-wide Technical Specification provides additional guidance to avionics systems designers, electronic equipment, component manufacturers and their customers to adopt a standard approach to optimise system design to accommodate atmospheric radiation single event effects. It builds on the information and guidance on the system level approach to Single Event Effects in IEC/TS 62396-1, considers some avionic systems and provides basic methods to accommodate SEE so that System Hardware Assurance levels may be met.

Atmospheric radiation effects are one factor that could contribute to equipment hard and soft fault rates. From a system safety perspective, using derived fault rate values, the existing methodology described in ARP4754 (accommodation of hard and soft fault rates in general) will also accommodate atmospheric radiation effect rates.

PROCESS MANAGEMENT FOR AVIONICS – ATMOSPHERIC RADIATION EFFECTS –

Part 3: Optimising system design to accommodate the single event effects (SEE) of atmospheric radiation

1 Scope and object

This Technical Specification is intended to provide guidance to those involved in the design of avionic systems and equipment and the resultant affects of Atmospheric Radiation induced Single Event Effects (SEE) on those avionic systems. The outputs of the activities and objectives described in this Technical Specification will become inputs to higher level certification activities and required evidences. It builds on the initial guidance on the system level approach to Single Event Effects in IEC/TS 62396-1, considers some avionic systems and provides basic methods to accommodate SEE so that System Development Assurance levels may be met.

2 Normative references

The following referenced documents are indispensable for the application of this document, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

IEC/TS 62396-1, *Process management for avionics – Atmospheric radiation effects – Part 1: Accommodation of atmospheric radiation effects via single event effects within avionics electronic equipment*

IEC/TS 62239, *Process management for avionics – Preparation of an electronic components management plan*

3 Terms and definitions

For the purpose of this document, the terms and definitions of the IEC/TS 62396-1, IEC/TS 62239 and the following apply

3.1

Analogue Single Event Transient ASET

deviation away from the expected operating output of the analogue device for a short duration due to the effects of a radiation deposited charge within the device.

3.2

Could Not Duplicate CND

reported outcome of diagnostic testing on a piece of equipment. Following receipt of an error or fault message during operation, the error or fault condition could not be replicated during subsequent equipment testing.

3.3

Double Error Correction Triple Error Detection DECTED

system or equipment methodology to test a digital word of information to determine if it has been corrupted, and if corrupted, to conditionally apply correction

NOTE This methodology can correct two bit corruptions and can detect and report three bit corruptions.

3.4

firm error

term (see also soft error) used in the semiconductor community referring to a circuit cell failure within a device that cannot be reset other than by rebooting the system or by cycling the power

NOTE Such a failure could be manifest as a soft fault in that it could provide no fault found during subsequent test and impact the value for the MTBUR of the LRU.

3.5

hard error

term used in the semiconductor community referring to permanent or semi-permanent damage of a circuit cell failure within a device by atmospheric radiation that is not recoverable even by cycling the power off and on

NOTE Hard errors could include SEB, SEGR and SEL. Such a fault would be manifest as a hard fault and could impact the value for the MTBF of the LRU.

3.6

hard fault

term used at the aircraft function level safety analysis referring to the permanent failure of a component within an LRU

NOTE A hard fault results in the removal of the LRU affected and the replacement of the permanently damaged component before a system/system architecture can be restored to full functionality. Such a fault could impact the value for the MTBF of the LRU repaired.

3.7

latch-up

condition where triggering of a parasitic pnpn circuit in semiconductor materials (including bulk CMOS) occurs, resulting in a state where the parasitic latched current exceeds the holding current. This state is maintained while power is applied

NOTE Latch-up could be a particular case of a soft fault (firm/soft error) or in the case where it causes device damage, a hard fault.

3.8

Line Replaceable Unit

LRU

piece of avionics electronic equipment that may be replaced during the maintenance cycle of the system

3.9

Mean Time Between Failure

MTBF

term from the world airlines technical glossary referring to the mean time between failure of equipment or a system in service such that it would require the replacement of a damaged component before a system/system architecture can be restored to full functionality and thus it is a measure of reliability requirements for equipment or systems.

3.10

Mean Time Between Unscheduled Removals

MTBUR

term from the world airlines technical glossary referring to the mean time between unscheduled removal of equipment or a system in service that could be the result of soft faults and thus is a measure of reliability for equipment or systems

NOTE MTBUR values can have a major impact on airline operational costs.

3.11**Multiple Bit Upset****MBU**

event which occurs when the energy deposited in the silicon of an electronic component by a single ionising particle causes upset to more than one bit

3.12**No Fault Found****NFF**

reported outcome of diagnostic testing on a piece of equipment. Following receipt of an error or fault message during operation, the equipment is found to be fully functional and within specification during subsequent equipment testing.

3.13**neutron**

elementary particle with atomic mass number of one and carries no charge

NOTE It is a constituent of every atomic nucleus except hydrogen.

3.14**Single Error Correction Double Error Detection****SECEDED**

system or equipment methodology to test a digital word of information to determine if it has been corrupted, and if corrupted, to conditionally apply correction

NOTE This methodology can correct one bit corruption and can detect and report two bit corruptions.

3.15**Single Event Burn Out****SEB**

occurs when a powered electronic component or part thereof is burnt out as a result of the energy absorption triggered by an individual radiation event

3.16**Single Event Effect****SEE**

is the response of a component to the impact of a single particle (for example cosmic rays, solar energetic particles, energetic neutrons and protons)

NOTE The range of responses can include both non-destructive (for example upset) and destructive (for example latch-up or gate rupture) phenomena.

3.17**Single Event Functional Interrupt****SEFI**

upset in a complex device, for example, a microprocessor, such that a control path is corrupted, leading the part to cease to function properly

NOTE This effect has sometimes been referred to as lockup, indicating that sometimes the part can be put into a "frozen" state.

3.18**Single Event Gate Rupture****SEGR**

event which occurs in the gate of a powered insulated gate component when the radiation charge absorbed by the device is sufficient to cause destructive gate insulation breakdown