IEC/TS 62396-3

Edition 1.0 2008-08

TECHNICAL SPECIFICATION

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

withdrawn

iTeh Standards
(https://standards.iteh.ai)
Document Preview

IEC TS 62396-3:2008
https://standards.iteh.ai/catalog/standards/iec/c95c8d1f-d736-4c4d-8104-35b1a24e8982/iec-ts-62396-3-2008

IEC/TS 62396-3:2008(E)

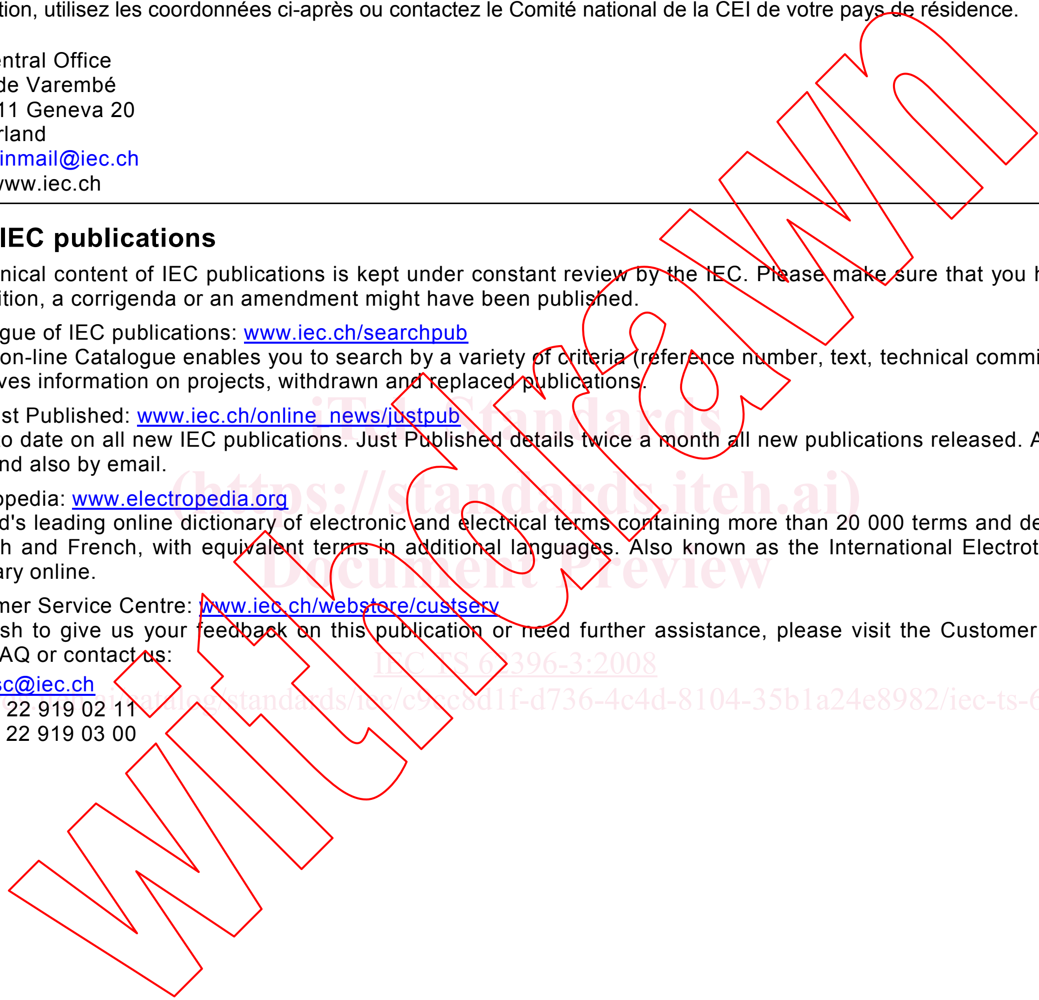
THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2008 IEC, Geneva, Switzerland

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either IEC or IEC's member National Committee in the country of the requester.
If you have any questions about IEC copyright or have an enquiry about obtaining additional rights to this publication, please contact the address below or your local IEC member National Committee for further information.

Droits de reproduction réservés. Sauf indication contraire, aucune partie de cette publication ne peut être reproduite ni utilisée sous quelque forme que ce soit et par aucun procédé, électronique ou mécanique, y compris la photocopie et les microfilms, sans l'accord écrit de la CEI ou du Comité national de la CEI du pays du demandeur.
Si vous avez des questions sur le copyright de la CEI ou si vous désirez obtenir des droits supplémentaires sur cette publication, utilisez les coordonnées ci-après ou contactez le Comité national de la CEI de votre pays de résidence.

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
Email: inmail@iec.ch
Web: www.iec.ch



About IEC publications

The technical content of IEC publications is kept under constant review by the IEC. Please make sure that you have the latest edition, a corrigenda or an amendment might have been published.

- Catalogue of IEC publications: www.iec.ch/searchpub

The IEC on-line Catalogue enables you to search by a variety of criteria (reference number, text, technical committee,…). It also gives information on projects, withdrawn and replaced publications.

- IEC Just Published: www.iec.ch/online_news/justpub

Stay up to date on all new IEC publications. Just Published details twice a month all new publications released. Available on-line and also by email.

- Electropedia: www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 20 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary online.

- Customer Service Centre: www.iec.ch/webstore/custserv

If you wish to give us your feedback on this publication or need further assistance, please visit the Customer Service Centre FAQ or contact us:

Email: csc@iec.ch
Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00

iTeh Standards
(https://standards.iteh.ai)
Document Preview
IEC TS 62396-3:2008
https://standards.iteh.ai/catalog/standards/iec/c95ce8d1f-d736-4c4d-8104-35b1a24e8982/iec-ts-62396-3-2008

IEC/TS 62396-3

Edition 1.0 2008-08

TECHNICAL SPECIFICATION

withdrawn

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

iTeh Standards
(https://standards.iteh.ai)
Document Preview
IEC TS 62396-3:2008
https://standards.iteh.ai/catalog/standards/iec/c9ecc8d1f-d736-4c4d-8104-35b1a24e8982/iec-ts-62396-3-2008

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

PRICE CODE T

ICS 03.100.50; 31.020; 49.060

ISBN 2-8318-9992-3

® Registered trademark of the International Electrotechnical Commission

CONTENTS

FOREWORD....3
INTRODUCTION....5
1 Scope and object....6
2 Normative references....6
3 Terms and definitions....6
4 Process guidance (see Annex A)....9
5 Atmospheric radiation and electronic system faults....10
5.1 Atmospheric radiation effects on avionics....10
5.2 Hard faults....11
5.3 Soft faults....12
6 Aircraft safety assessment....12
6.1 Methodology....12
6.2 Mitigation (see Annex B)....13
6.3 Specific electronic systems (see Annex C)....13
6.3.1 Level A systems....13
6.3.2 Level B systems....16
6.3.3 Level C systems....17
6.3.4 Level D and E systems....17
Annex A (informative) Design process flow diagram for SEE rates....18
Annex B (informative) Some mitigation method considerations for single event effects....19
Annex C (informative) Example systems....22
Bibliography....25

Figure C.1 – Electronic equipment (flight control computers)....22
Figure C.2 – Electronic equipment (flight director computers)....23
Figure C.3 – Electronic equipment (engine control)....23
Figure C.4 – Electronically powered surface....24
Figure C.5 – Hydromechanical drive of surface – electronic valve control....24

Table 1 – Failure effect and occurrence probability....13

Withdrawn
iTeh Standards
(https://standards.iteh.ai)
Document Preview
IEC TS 62396-3:2008
https://standards.iteh.ai/catalog/standards/iec/c99cc8d11-d736-4c4d-8104-35b1a24e8982/iec-ts-62396-3-2008

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

**PROCESS MANAGEMENT FOR AVIONICS –
ATMOSPHERIC RADIATION EFFECTS –**

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

FOREWORD

1) The International Electrotechnical Commission (IEC) is a worldwide organization for standardization comprising all national electrotechnical committees (IEC National Committees). The object of IEC is to promote international co-operation on all questions concerning standardization in the electrical and electronic fields. To this end and in addition to other activities, IEC publishes International Standards, Technical Specifications, Technical Reports, Publicly Available Specifications (PAS) and Guides (hereafter referred to as "IEC Publication(s)"). Their preparation is entrusted to technical committees; any IEC National Committee interested in the subject dealt with may participate in this preparatory work. International, governmental and non-governmental organizations liaising with the IEC also participate in this preparation. IEC collaborates closely with the International Organization for Standardization (ISO) in accordance with conditions determined by agreement between the two organizations.
2) The formal decisions or agreements of IEC on technical matters express, as nearly as possible, an international consensus of opinion on the relevant subjects since each technical committee has representation from all interested IEC National Committees.
3) IEC Publications have the form of recommendations for international use and are accepted by IEC National Committees in that sense. While all reasonable efforts are made to ensure that the technical content of IEC Publications is accurate, IEC cannot be held responsible for the way in which they are used or for any misinterpretation by any end user.
4) In order to promote international uniformity, IEC National Committees undertake to apply IEC Publications transparently to the maximum extent possible in their national and regional publications. Any divergence between any IEC Publication and the corresponding national or regional publication shall be clearly indicated in the latter.
5) IEC provides no marking procedure to indicate its approval and cannot be rendered responsible for any equipment declared to be in conformity with an IEC Publication.
6) All users should ensure that they have the latest edition of this publication.
7) No liability shall attach to IEC or its directors, employees, servants or agents including individual experts and members of its technical committees and IEC National Committees for any personal injury, property damage or other damage of any nature whatsoever, whether direct or indirect, or for costs (including legal fees) and expenses arising out of the publication, use of, or reliance upon, this IEC Publication or any other IEC Publications.
8) Attention is drawn to the Normative references cited in this publication. Use of the referenced publications is indispensable for the correct application of this publication.
9) Attention is drawn to the possibility that some of the elements of this IEC Publication may be the subject of patent rights. IEC shall not be held responsible for identifying any or all such patent rights.

Withdrawn
iTeh Standards
(https://standards.iteh.ai)
Document Preview
IEC TS 62396-3:2008

The main task of IEC technical committees is to prepare International Standards. In exceptional circumstances, a technical committee may propose the publication of a technical specification when

- the required support cannot be obtained for the publication of an International Standard, despite repeated efforts, or
- The subject is still under technical development or where, for any other reason, there is the future but no immediate possibility of an agreement on an International Standard.

Technical specifications are subject to review within three years of publication to decide whether they can be transformed into International Standards.

IEC 62396-3, which is a Technical Specification, has been prepared by IEC technical committee 107: Process management for avionics.

This technical specification cancels and replaces IEC/PAS 62396-3 published in 2007. This first edition constitutes a technical revision.

The text of this standard is based on the following documents:

Enquiry draft	Report on voting
107/84/DTS	107/87/RVC

Full information on the voting for the approval of this standard can be found in the report on voting indicated in the above table.

This publication has been drafted in accordance with the ISO/IEC Directives, Part 2.

A list of all parts of the IEC 62396 series, under the general title *Process management for avionics – Atmospheric radiation effects*, can be found on the IEC website.

The committee has decided that the contents of this publication will remain unchanged until the maintenance result date indicated on the IEC web site under "http://webstore.iec.ch" in the data related to the specific publication. At this date, the publication will be

- transformed into an International standard,
- reconfirmed;
- withdrawn;
- replaced by a revised edition, or
- amended

A bilingual version of this publication may be issued at a later date.

Withdrawn
iTeh Standards
(https://standards.iteh.ai)
Document Preview
IEC TS 62396-3:2008
https://standards.iteh.ai/catalog/standards/iec/c9cc8d1f-d736-4c4d-8104-35b1a24e8982/iec-ts-62396-3-2008

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.

Withdrawn
iTeh Standards
(https://standards.iteh.ai)
Document Preview
IEC TS 62396-3:2008
https://standards.iteh.ai/catalog/standards/iec/c9cc8d1f-d736-4c4d-8104-35b1a24e8982/iec-ts-62396-3-2008

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*

Withdrawn
iTeh Standards
(https://standards.iteh.ai)
Document Preview
IEC TS 62396-3:2008
https://standards.iteh.ai/catalog/standards/iec/e9cc8d1f-d736-4c4d-8104-35b1a24e8982/iec-ts-62396-3-2008

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.

Withdrawn
iTeh Standards
(https://standards.iteh.ai)
Document Preview
IEC TS 62396-3:2008

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
SECDED
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.

iTeh Standards
(https://standards.iteh.ai)
Document Preview
Withdrawn

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

IEC TS 62396-3:2008
https://standards.iteh.ai/catalog/standards/iec/c5ccc8d1f-d736-4c4d-8104-35b1a24e8982/iec-ts-62396-3-2008

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

3.19
Single Event Latch-up
SEL
condition where ionisation deposited by the interaction of a single particle of radiation in a device causes triggering of a parasitic pnpn circuit in semiconductor materials (including bulk CMOS) to occur, 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.

3.20
Single Event Transient
SET
spurious signal or voltage, induced by the deposition of charge by a single particle that can propagate through the circuit path during one clock cycle (see 6.3.1.3.3)

3.21
Single Event Upset
SEU
event which occurs in a semiconductor device when the radiation absorbed by the device is sufficient to change the logical state of a digital electronic logic cell(s) (memory bit cell, register bit cell, latch cell, etc.)

3.22
soft error
term (see also firm error) refers to invalid state changes in digital electronic logic cell(s) that could be induced by atmospheric radiation and which are recoverable by cycling the power off and on

iTeh Standards
(https://standards.iteh.ai)
Document Preview

NOTE Soft error responses could include SEFI, SET and SEU. Such failures may not be manifest during subsequent test and therefore could impact the value for the MTBUR of the LRU.

IEC TS 62396-3:2008
https://standards.iteh.ai/catalog/standards/iec/cacce8d1f-d736-4c4d-8104-35b1a24e8982/iec-ts-62396-3-2008

3.23
soft fault
term used at the aircraft function level safety analysis that refers to the characteristic of invalid digital logic cell(s) state changes within digital hardware electronic circuitry

NOTE This is a fault that does not involve replacement of a permanently damaged component within an LRU, but it does involve restoring the logic cells to valid states before a system/system can be restored to full functionality. Such a fault condition has been suspected in the "no fault found" syndrome for functions implemented with digital technology and it would probably impact the value for the MTBUR of the affected LRU. If a soft fault results in the mistaken replacement of a component within the LRU, the replacement could impact the value for the MTBF of the LRU repaired.

Withdrawn

4 Process guidance (see Annex A)

In an attempt to achieve a high level of confidence in system safety, certification authorities mandate the use of defined design processes for the purpose of identifying and eliminating design faults and providing appropriate feedback mechanisms to ensure a continuous and closed loop development process. This Technical Specification defines methods and guidance to be appropriately used in accommodating SEE related issues in Avionics design. However, this is only one piece in the development assurance process.

To fully address design methodology as it pertains to SEE and the required evidence needed to validate designs, several different processes will require revision to address this design issue. The following is a partial list of the processes that may need revision depending on how processes are currently structured.

- At a program management level, there are often processes in place. In many cases, it may be necessary to address SEE issues generically at this level.