IEC 62396-3

Edition 1.0 2013-09

INTERNATIONAL STANDARD

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC 62396-3:2013
https://standards.iteh.ai/catalog/standards/sist/6af42e6c-b48c-4503-a687-5fe4de64f6a9/iec-62396-3-2013

IEC 62396-3:2013(E)

THIS PUBLICATION IS COPYRIGHT PROTECTED

Copyright © 2013 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.

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland

Tel.: +41 22 919 02 11
Fax: +41 22 919 03 00
info@iec.ch
www.iec.ch

About the IEC

The International Electrotechnical Commission (IEC) is the leading global organization that prepares and publishes International Standards for all electrical, electronic and related technologies.

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.

Useful links:

IEC publications search - www.iec.ch/searchpub

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It also gives information on projects, replaced and withdrawn publications.

IEC Just Published - webstore.iec.ch/justpublished

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

Electropedia - www.electropedia.org

The world's leading online dictionary of electronic and electrical terms containing more than 30 000 terms and definitions in English and French, with equivalent terms in additional languages. Also known as the International Electrotechnical Vocabulary (IEV) on-line.

Customer Service Centre - webstore.iec.ch/csc

If you wish to give us your feedback on this publication or need further assistance, please contact the Customer Service Centre: csc@iec.ch.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC 62396-3:2013
https://standards.iteh.ai/catalog/standards/sist/6af42e6c-b48c-4503-a687-5fe4de64f6a9/iec-62396-3-2013

IEC 62396-3

Edition 1.0 2013-09

INTERNATIONAL STANDARD

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC 62396-3:2013
https://standards.iteh.ai/catalog/standards/sist/6af42e6c-b48c-4503-a687-5fe4de64f6a9/iec-62396-3-2013

INTERNATIONAL
ELECTROTECHNICAL
COMMISSION

PRICE CODE **U**

ICS 03.100.50; 31.020; 49.060

ISBN 978-2-8322-1095-6

Warning! Make sure that you obtained this publication from an authorized distributor.

® Registered trademark of the International Electrotechnical Commission

CONTENTS

FOREWORD ... 3
INTRODUCTION ... 5
1 Scope ... 6
2 Normative references ... 6
3 Terms and definitions ... 6
4 Process guidance ... 10
5 Atmospheric radiation and electronic system faults ... 11
5.1 Atmospheric radiation effects on avionics ... 11
5.2 Hard faults ... 12
5.3 Soft faults ... 13
6 Aircraft safety assessment ... 13
6.1 Methodology ... 13
6.2 Mitigation ... 14
6.3 Specific electronic systems ... 14
6.3.1 Level A systems ... 14
6.3.2 Level B systems ... 17
6.3.3 Level C systems ... 18
6.3.4 Levels D and E systems ... 18
Annex A (informative) Design process flow diagram for SEE rates ... 19
Annex B (informative) Some mitigation method considerations for SEEs ... 20
Annex C (informative) Example systems ... 24
Bibliography ... 28

Figure C.1 – Electronic equipment (flight control computers) ... 24
Figure C.2 – Electronic equipment (flight director computers) ... 25
Figure C.3 – Electronic equipment (engine control) ... 26
Figure C.4 – Electronically powered surface ... 26
Figure C.5 – Hydro mechanical drive of surface – Electronic valve control ... 27

Table 1 – Failure effect and occurrence probability ... 14

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC 62396-3:2013
https://standards.iteh.ai/catalog/standards/sist/6af42e6c-b48c-4503-a687-5fe4de64f6a9/iec-62396-3-2013

INTERNATIONAL ELECTROTECHNICAL COMMISSION

____

PROCESS MANAGEMENT FOR AVIONICS – ATMOSPHERIC RADIATION EFFECTS –

Part 3: System design optimization 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 itself does not provide any attestation of conformity. Independent certification bodies provide conformity assessment services and, in some areas, access to IEC marks of conformity. IEC is not responsible for any services carried out by independent certification bodies.
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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC 62396-3:2013
https://standards.iteh.ai/catalog/standards/sist/6af43e6d-b48c-4593-a687-5fe4de64f6a9/iec-62396-3-2013

International Standard IEC 62396-3 has been prepared by IEC technical committee 107: Process management for avionics.

This first edition cancels and replaces IEC/TS 62396-3 published in 2008. This edition constitutes a technical revision.

This edition includes the following significant technical changes with respect to the previous edition:

a) Reference to IEC 62396-1:2012 included.
b) Some definitions in Clause 3 updated in line with IEC 62396-1:2012.
c) Reference to system level A types I and II removed from 6.3 and Annex C.
d) Replacement in key locations of "may" by a more positive statement.

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

FDIS	Report on voting
107/210/FDIS	107/220/RVD

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 stability 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

- reconfirmed,
- withdrawn,
- replaced by a revised edition, or
- amended.

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

IEC 62396-3:2013
https://standards.iteh.ai/catalog/standards/sist/6af42e6c-b48c-4503-a687-5fe4de64f6a9/iec-62396-3-2013

INTRODUCTION

This industry-wide International Standard 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 (SEE). It builds on the information and guidance on the system level approach to single event effects in IEC 62396-1:2012, considers some avionic systems and provides basic methods to accommodate SEE so that system hardware assurance levels are 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 [1] [1] (accommodation of hard and soft fault rates in general) will also accommodate atmospheric radiation effect rates.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

IEC 62396-3:2013
https://standards.iteh.ai/catalog/standards/sist/6af42e6c-b48c-4503-a687-5fe4de64f6a9/iec-62396-3-2013

1 Numbers in square brackets refer to the Bibliography.

PROCESS MANAGEMENT FOR AVIONICS – ATMOSPHERIC RADIATION EFFECTS –

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

1 Scope

This part of IEC 62396 provides guidance and furthermore it provides necessary requirements for those involved in the design of avionic systems and equipment and the resultant effects of atmospheric radiation-induced single event effects (SEE) on those avionic systems. The outputs of the activities and objectives described in this part of IEC 62396 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 62396-1:2012, considers some avionic systems and provides basic methods to accommodate SEE so that system development assurance levels are met.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC 62396-3:2013
https://standards.iteh.ai/catalog/standards/sist/6af42e6c-b48c-4503-a687-5fe4de64f6a9/iec-62396-3-2013

IEC 62396-1:2012, *Process management for avionics – Atmospheric radiation effects – Part 1: Accommodation of atmospheric radiation effects via single event effects within avionics electronic equipment*

IEC/TS 62239-1, *Process management for avionics – Management plan – Part 1: Preparation and maintenance of an electronic components management plan*

3 Terms and definitions

For the purposes of this document, the terms and definitions of IEC 62396-1:2012, IEC/TS 62239-1 as well as the following apply.

3.1
analogue single event transient
ASET
spurious signal or voltage produced at the output of an analogue device by the deposition of charge by a single particle

[SOURCE: IEC 62396-1:2012, 3.2]

3.2
could not duplicate
CND
reported outcome of diagnostic testing on a piece of equipment

Note 1 to entry: 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 1 to entry: This methodology can correct two bit corruptions and can detect and report three bit corruptions.

3.4
firm error
<semiconductor community> circuit cell failure within a device that cannot be reset other than by rebooting the system or by cycling the power

Note 1 to entry: 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.

Note 2 to entry: See also soft error.

3.5
hard error
permanent or semi-permanent damage of a cell by atmospheric radiation that is not recoverable even by cycling the power off and on

Note 1 to entry: 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.

[SOURCE: IEC 62396-1:2012, 3.24, modified – a note to entry has been added]

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.6
hard fault
term used at the aircraft function level safety analysis referring to the permanent failure of a component within an LRU

IEC 62396-3:2013
https://standards.iteh.ai/catalog/standards/sist/6af42e6c-b48c-4503-a687-5fe4de64f6a9/iec-62396-3-2013

Note 1 to entry: 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.

[SOURCE: IEC 62396-1:2012, 3.25]

3.7
latch-up
condition where triggering of a parasitic p-n-p-n 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 1 to entry: 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.

[SOURCE: IEC 62396-1:2012, 3.29, modified – a note to entry has been added]

3.8
line replaceable unit
LRU
piece of avionics electronic equipment that may be replaced during the maintenance cycle of the system

[SOURCE: IEC 62396-1:2012, 3.32]

3.9
mean time between failure
MTBF
measure of reliability requirements and is the mean time between failure of equipment or a system in service

Note 1 to entry: 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.

[SOURCE: IEC 62396-1:2012, 3.34, modified – a note to entry has been added]

3.10
mean time between unscheduled removals
MTBUR
measure of reliability requirements and is the mean time between unscheduled removal of equipment or a system in service

Note 1 to entry: 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. MTBUR values can have a major impact on airline operational costs.

[SOURCE: IEC 62396-1:2012, 3.35, modified – a note to entry has been added]

3.11
multiple bit upset
MBU
the energy deposited in the silicon of an electronic component by a single ionising particle causes upset to more than one bit in the same word

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC 62396-3:2013
5fe4de64f6a9/iec-62396-3-2013

Note 1 to entry: The definition of MBU has been updated due to the introduction of the definition of MCU.

[SOURCE: IEC 62396-1:2012, 3.36]

3.12
multiple cell upset
MCU
the energy deposited in the silicon of an electronic component by a single ionising particle induces several bits in an integrated circuit (IC) to upset at one time

[SOURCE: IEC 62396-1:2012, 3.37]

3.13
no fault found
NFF
reported outcome of diagnostic testing on a piece of equipment

Note 1 to entry: 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.

3.14
neutron
elementary particle with atomic mass number of one and carries no charge

Note 1 to entry: It is a constituent of every atomic nucleus except hydrogen.

[SOURCE: IEC 62396-1:2012, 3.38]

3.15
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 1 to entry: This methodology can correct one bit corruption and can detect and report two bit corruptions.

3.16
single event burnout
SEB
burnout of a powered electronic component or part thereof as a result of the energy absorption triggered by an individual radiation event

[SOURCE: IEC 62396-1:2012, 3.47]

3.17
single event effect
SEE
response of a component to the impact of a single particle (for example cosmic rays, solar energetic particles, energetic neutrons and protons)

Note 1 to entry: The range of responses can include both non-destructive (for example upset) and destructive (for example latch-up or gate rupture) phenomena.

[SOURCE: IEC 62396-1:2012, 3.48]

iTeh STANDARD PREVIEW
(standards.iteh.ai)
IEC 62396-3:2013

3.18
single event functional interrupt
SEFI
upset, usually in a complex device, for example, a microprocessor, such that a control path is corrupted, leading the part to cease to function properly

Note 1 to entry: This effect has sometimes been referred to as lockup, indicating that sometimes the part can be put into a “frozen” state.

Note 2 to entry: SEFI may be recoverable by resetting the configuration register (F/F) to default values.

[SOURCE: IEC 62396-1:2012, 3.49, modified – a note 2 to entry has been added]

3.19
single event gate rupture
SEGR
occurs in the gate of a powered insulated gate component when the radiation charge absorbed by the device is sufficient to cause gate insulation breakdown which is destructive

[SOURCE: IEC 62396-1:2012, 3.50]

3.20
single event latch-up
SEL
in a device containing a minimum of 4 semiconductor layers (p-n-p-n) when the radiation absorbed by the device is sufficient to cause a node within the powered semiconductor device to be held in a fixed state whatever input is applied until the device is de-powered, such latch up may be destructive or non-destructive

Note 1 to entry: The ionisation deposited by the interaction of a single particle of radiation in a device causes triggering of a parasitic p-n-p-n 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. 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.

[SOURCE: IEC 62396-1:2012, 3.51, modified – a note to entry has been added]

3.21
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

Note 1 to entry: See 6.3.1.3.3.

[SOURCE: IEC 62396-1:2012, 3.52, modified – the note 1 to entry has been modified to refer to the present document]

3.22
single event upset
SEU
occurs in a semiconductor device when the radiation absorbed by the device is sufficient to change a cell's logic state

Note 1 to entry: After a new write cycle, the original state can be recovered.

Note 2 to entry: A logic cell may be a memory bit cell, register bit cell, latch cell, etc.

[SOURCE: IEC 62396-1:2012, 3.53, modified – a note 2 to entry has been added]

iTeh STANDARD PREVIEW
(standards.iteh.ai)

3.23
soft error
change of state of a latched logic state from one to zero or vice-versa

Note 1 to entry: It is also known as a single event upset.

Note 2 to entry: It is non-destructive and can be rewritten or reset.

IEC 62396-3:2013
https://standards.iteh.ai/catalog/standards/sist/6af42e6c-b48c-4503-a687-5fe4de64f6a9/iec-62396-3-2013

[SOURCE: IEC 62396-1:2012, 3.55]

3.24
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 1 to entry: 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 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.

Note 2 to entry: Logic cell(s) includes logic gates and memory elements.

[SOURCE: IEC 62396-1:2012, 3.56, modified – a note 2 to entry has been added]

4 Process guidance

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 part of IEC 62396 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.