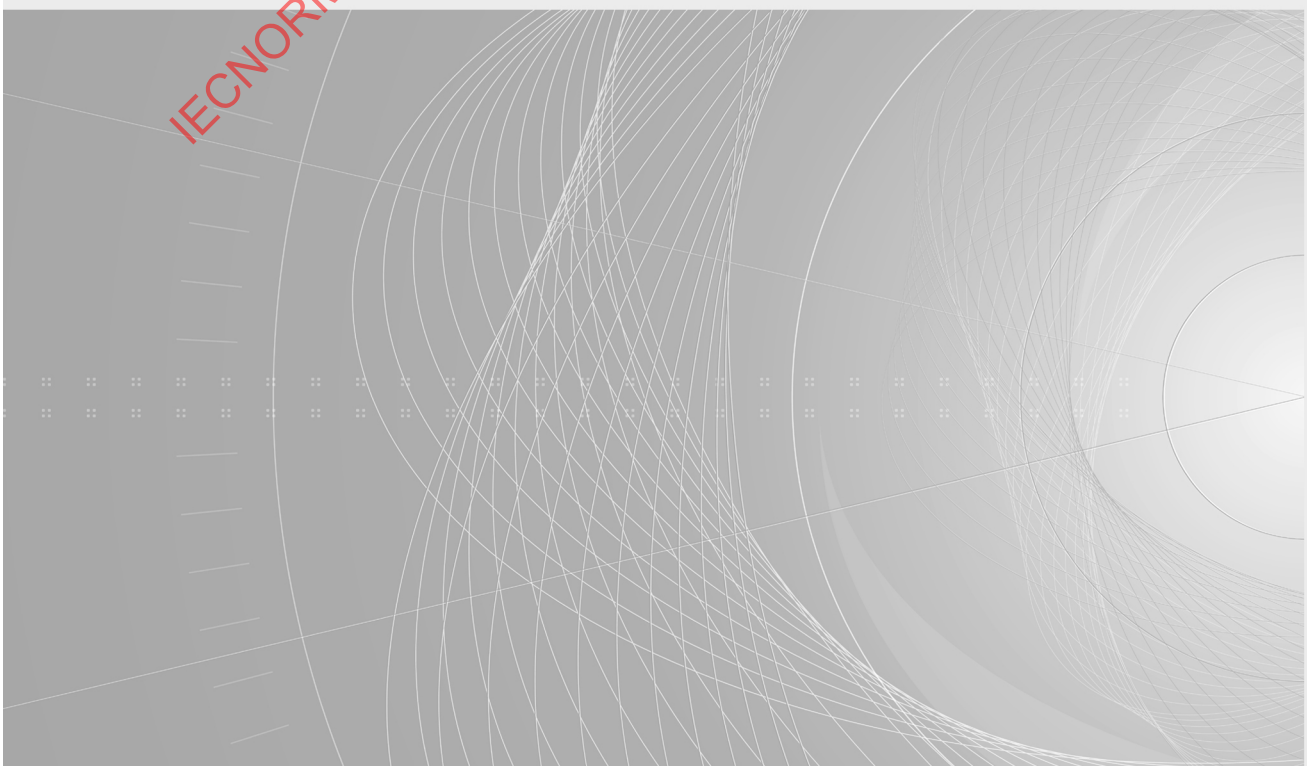
IEC 62396-3

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



IEC 62396-3:2013(E)

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It also gives information on projects, replaced and withdrawn publications.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.

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

PRICE CODE U

ICS 03.100.50; 31.020; 49.060

ISBN 978-2-8322-1095-6

CONTENTS

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.

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.

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.

[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.

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]

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 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

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]

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]

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.

[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.

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 shall be reviewed for revision depending on how processes are currently structured.

– At a program management level, there are often processes in place. In many cases, it is necessary to address SEE issues generically at this level.
– System level processes are likely to require addressing SEE issues and providing specific direction as to how these processes should be handled, communicated and fed back through the development process. This is important, because SEE issues, in contrast to standard reliability numbers, have been fed back into the design process that has resulted in design and requirements changes. These changes have been developed to mitigate various aspects of the effects and then resulted in revised SEE calculations made against the new design. This makes SEE an aspect of reliability, and system reliability determination an iterative process in ways that never happened previously.
– Reliability/safety analysis processes will need (depending on system criticality) to address SEE issues and develop formal mechanisms to address the iterative design aspects that have taken place in ways not previously experienced.
– Component management plans will require modification to address SEE issues in initial parts selection and also as manufacturers revise parts. Some processes will need to be in place (also depending on system criticality) to ensure that new parts used in the manufacturing process will perform the same as the original parts from a SEE perspective.

Guidance for the integration of evolving processes to measure SEE rates and the accommodation of those rates in digital systems (flight controls, avionics, etc.) into existing safety analysis/system design methodology (component reliability, redundancy, mitigation) is provided in Clauses 5 and 6.

5 Atmospheric radiation and electronic system faults

5.1 Atmospheric radiation effects on avionics

Atmospheric radiation affects the electronic parts of the system. The high energy secondary or thermal neutron radiation interacts with the silicon within semiconductor elements of an electronic component to produce a charge which may cause a single event effect (SEE) in the localised area within that device. Atmospheric radiation at aircraft altitudes has not been a significant problem in the past, prior to 1990, due to the relatively large feature sizes (above 1 μm) with similarly large critical charge. Current avionic electronic systems use state-of-the-art electronic/digital devices with feature sizes well below 1 μm, which makes SEE much more probable (the energy transfer generated charge required to produce SEE becomes less) in these devices.

When aircraft functions are implemented using digital technology, atmospheric radiation effects can show up as digital device failures that in turn can propagate to failures within systems and possibly, failure of an aircraft function. The failure rate of each piece of electronic equipment which comprises a system is the aggregate rate of the components which make up that piece of electronic equipment. The failure rate of each component is the aggregate rate of all failure mechanisms of that component which dominate that failure rate. As the feature sizes of individual circuits within digital devices continue to decrease and the corresponding failure rate due to SEE rises, SEE mechanisms may become a dominant driver of the failure rates for these devices. The testing of small feature size IC components for secondary neutron SEE in suitable simulators or with terrestrial facilities is becoming more commonplace. Although this is more commonplace, it is still difficult and costly.

Although analogue parts are generally considered immune to atmospheric radiation effects, some device scaling has occurred in the technology. As a result, a neutron SEE event within the device may be sufficient to cause a short duration transient from the correct output. This kind of transient is referred to as an analogue single event transient (ASET).

Reliability engineering can calculate equipment failure rates from component failure rates and system engineering can design an architecture that will satisfy the reliability and availability requirements for the function. At a system architectural level, redundancy is a common strategy to achieve the required function reliability. In order for redundancy to be cost effective, equipment failure rates cannot exceed certain limits. Naturally, if the failure rates of electronic devices become too great, equipment failure rates become prohibitively high. In the past, atmospheric SEE rates have not been a noticeable driver in the failure rate of digital devices. Where SEE rates become a significant failure rate driver, these rates need to be included by reliability engineering in the equipment failure rate calculation. It should be recognized that, since SEE involves unique technology and associated specialists to determine component SEE rates, another engineering discipline would need to be in place to provide those rates to reliability and systems engineering.

From a system safety perspective, faults can essentially be categorized as:

– hard, i.e. those which result in permanent failure of the affected LRU(s), and
– soft, i.e. those which may be recovered with no loss of system functionality or redundancy.

These categories arise from the device SEE: the atmospheric radiation effects on components may result in soft faults where functionality should be recovered or hard faults resulting in permanent failure of the component. Soft fault effects should be accommodated by corrective actions within the electronic equipment. As identified in IEC 62396-1:2012, the most frequent SEE that produces soft faults and associated effects is the single event upset (SEU).

NOTE

– Reliability is determined from the sum of hard fault failure rates.
– Availability is determined from the sum of hard faults and the sum of soft faults.

Hard faults result in a piece of system equipment requiring repair/replacement to clear the hard fault (see 5.2). Significant hard fault rates can be induced within digital components by neutrons in the atmosphere.

Availability recognizes that soft faults can occur, but that they can also be corrected and within a defined period of time, the redundant system element can return to service and be counted in the original redundancy scheme (see 5.3). It is the inducing of significant soft fault rates within digital components that adds another dimension to reliability data and system engineering.

Since electronic technology may be included in all arms of any system using redundancy, it is important that the SEE rate to be accommodated is low enough to avoid impact on the overall system redundancy mitigation. Therefore to avoid a common mode failure when operating in the atmospheric neutron environment, a limit should be established on neutron-induced soft (soft error, etc) and hard fault rates of any component technology used within the digital system.

The perspective of this part of IEC 62396 is SEE on aircraft functions due to SEE on the electronic systems that provide their implementation. In this part of IEC 62396, the terms ‘hard fault’ and ‘soft fault’ from the system safety community will be used. There are a number of terms commonly used in the semiconductor and radiation effects communities to describe component errors/failures (for example, hard errors, soft error rate, firm errors, latch-up, burnout, upset, functional interrupt). All of these component errors/failures types (with their associated terminology) will be grouped into hard fault or soft fault categories. Those component failures that would impact the mean time between failure (MTBF) are categorized as hard faults.

5.2 Hard faults

Hard faults refer to a damaged component whose effects cause a system malfunction and require repair or replacement of the component to clear the fault. When a repair or replacement action is taken, it reflects upon the MTBF rate history for that item. Within

electronic equipment, SEE-induced permanent failures (component or device) are considered in exactly the same way as for other types of failure. For the failure rate criteria of the system to be met, the aircraft system allowable failure metrics for electronic equipment within that system shall be met, for example, the MTBF. Atmospheric radiation can produce hard faults including single event latch (SEL) induced damage, single event burnout (SEB), and single event gate rupture (SEGR). There are suitable test methods available to determine the SEE-induced hard fault susceptibilities of devices and electronic components. When rates are found to be too high, a more tolerant part should be selected.

5.3 Soft faults

Soft faults are digital hardware (counter, register, memory, etc.) issues. A soft fault is a condition whereby a latch of some form within a digital device becomes set to an incorrect state. Since the device is not damaged, if the soft fault can be detected and corrected in a timely manner, then there is no impact on the performance of the system. If the soft fault is not corrected, there may be a significant impact on system performance or redundancy, which in turn, when reported will lead to removal of the faulty equipment for repair. However, upon removal and reapplication of power to the device, soft faults will always clear and therefore no fault will be found. Such attempted corrective actions negatively impact the MTBUR rate history for equipment. Unscheduled removals negatively impact system operational cost. A soft fault could certainly be a contributor to the CND/NFF categories for MTBUR metrics.

As their effects should be and often are mitigated and shall not result in equipment repair, soft faults associated with SEE could be considered a departure from the traditional reliability approach. However, because of their potential negative effects on MTBUR and system functionality, digital device SEE-induced soft fault rates:

– should be characterised and mitigated in the system architecture design;
– along with failure modes, should be obtained by and be available from reliability engineering.

Components that are subject to SEE-induced soft faults which cannot be reset by hardware or the software it executes and persist as a fault while power remains applied are becoming more prevalent. Soft faults of this type and their system effects would need to be managed by appropriate mitigation. Note that a finite time will be taken for effective recovery of the system or device from such a fault. An example of this kind of soft fault would be a non-destructive SEL. In the semiconductor and radiation effects communities, a non-destructive SEL might be categorized as a firm error. Recovery from SEL could require independent hardware and software for detection and recycling power.

For the failure rate criteria of the system to be met (which, in turn, results in the aircraft function meeting allowable failure metrics), failure metrics for electronic equipment within that system shall be met, for example MTBUR. Without mitigation, soft fault rates could have a significant negative effect on the ability of a system to meet its allowable MTBUR.

6 Aircraft safety assessment

6.1 Methodology

In IEC 62396-1:2012, it is recognized that, within the systems which implement aircraft functions, the method of assessing the safety impact of radiation-induced effects on electronic (particularly digital) components should be identical to that used to assess functional hazards due to other failure modes and effects traditionally recognized. This is particularly the case for electronic equipment. This methodology is driven by requirements governing function failure effects and the probability per flight hour of their occurrence. As an example, Table 1 provides the probability requirement for the various types of failure effect for Part 23 (general aviation category airplanes [2]) and Part 25 (transport category airplanes [3]) of the airworthiness standards.

Table 1 – Failure effect and occurrence probability

Functional failure condition classification per AC/AMJ 1309 and ARP4754	Probability (per flight hour) of occurrence
Catastrophic	10^{-9} or less (extremely improbable)
Severe major/hazardous	10^{-7} or less
Major	10^{-5} or less
Minor	10^{-3} or less
No effect	No requirement

6.2 Mitigation

Failure effects can manifest themselves in a system as a hard or soft error, as well as a hard failure. In addition to a thorough evaluation and parts selection process, where SEE occurs mitigation is necessary to ensure proper system performance. There are various mitigation techniques that can be employed at the component, circuit and system level to diminish the effects.

By suitable design at the system architecture and equipment level and also by careful selection and management (see IEC 62396-1:2012, 7.4 and 9.5.2) of electronic components employed within the design, the system level impact of SEE can be reduced to acceptable levels. The approach to system level optimization of design for mitigation of SEE is conducted by considering the system at three levels:

– system architecture;
– individual electronic equipment within the system architecture;
– components within the electronic equipment.

6.3 Specific electronic systems

System development assurance levels drive the discipline and rigour needed throughout the development cycle of products associated with that system. Just as the failure effect of a function implemented by a system (particularly systems based in electronic technology) determines the required probability of such a failure, it also determines the assurance level associated with that system. Systems are classified as level A when failures of such systems may have a catastrophic effect on the aircraft. Level A systems require the most rigorous approach to single event effects and parts control. In order of reducing degree of requirement for compliance demonstration, the other significant assurance levels are classified as level B, level C and level D. Examples of typical systems are given in Annex C, Figures C.1 to C.5.

For additional information regarding assurance levels, refer to IEC 62396-1:2012, Clause 7 and the references within that international standard. Regardless of assurance level, mitigation considerations will be in terms of hard and soft faults. As detailed in 5.3, soft fault effects appear as system performance degradation and they consist of faults or errors that clear (SEFI, SET, SEU, SHE) upon removal and reapplication of power or in some cases, upon refresh.

6.3.1 Level A systems

6.3.1.1 General

These systems shall be designed so that the failure rate of the function they provide is 10^{-9} or less per flight hour. Level A systems require the most rigorous processes to achieve the 10^{-9} function failure criteria. Level A systems would include a primary flight control system that is completely computer controlled.

Some full authority digital engine controls (FADEC) systems are also classified as level A. FADEC systems installed on Part 25 aircraft have their software and complex electronic hardware classified as level A due to the nature of the common mode threat. As to SEE, FADEC systems that implement certain critical functions (over speed, reverser control, etc.) should also be considered level A as well.

Level A systems include systems which implement functions in which the pilot is in the control loop. The pilot closes the control loop through pilot/system information exchange from display systems, for example closing the flight control loop using information from a primary flight director (PFD) system. It should be noted that the PFD system could provide catastrophically misleading information and is categorized as level A. Any other display system that could provide catastrophically misleading information would also be categorized as level A.

6.3.1.2 Hard faults

6.3.1.2.1 Recovery

Hard faults require device replacement to enable full recovery of system function or redundancy capability. Their effects can be mitigated at the system architecture, electronic equipment, or component/device level.

6.3.1.2.2 System architecture

At the architecture level, redundancy and redundancy management techniques are employed to accommodate failures that would lead to catastrophic failure effects at the aircraft level. Multiple control surfaces and multiple engines would be examples at the structure and propulsion aircraft level. Multiple actuators and associated electronic equipment would manage effector (aircraft control surface, engine valve, etc.) movement. When electronic system development assurance levels are met, redundancy within the system architecture ensures that there is no problem from a safety requirements aspect at the aircraft function level. It is the electronic equipment that is SEE sensitive; mechanical equipment would be inherently immune and is mentioned only to illustrate the concept of redundancy.

Since monitoring across redundant elements could be relatively easily implemented within computers, redundancy can be an effective means of detecting the occurrence of faults. The occurrence of a fault can be detected by monitoring across two or more redundant elements (e.g. effectors, actuators, computers, microprocessors).

However, the allocation of redundancy has an impact on the aircraft for several reasons. Redundancy of equipment will add weight and complexity due to the need for a method of active equipment choice. It will therefore also reduce reliability and increase power consumption, and thus affect overall cost. However, the impact of increased fault tolerance and system availability has allowed, for example, the use of twin-engine aircraft in some flight profiles where in the past three- or four-engine aircraft would have been mandated. Intuitively, the life cycle cost of a twin-engine aircraft should be significantly lower than a similar aircraft with three or more engines.

6.3.1.2.3 Electronic equipment

At the electronic equipment level, redundancy may be used as a method of accommodating failure by removing the failed equipment from contributing to the system output; the pilot may be within the loop or not.

6.3.1.2.4 Electronic component/device

System design may be optimized by limiting the range of components used. In space applications, components have been tested for potential latch-up in their radiation environment and in many applications component types that are subject to SEL have been avoided. Many other destructive failure modes have been identified, e.g. SEB and SEGR, see IEC 62396-1:2012. There are suitable test methods to determine non-destructive SEL

susceptibility of devices. Such parts, once identified, are to be avoided if the level of susceptibility is unacceptable. This type of approach requires careful selection and control of electronic components throughout the equipment life cycle, see IEC 62396-1:2012, 7.4 and 9.5.2.

6.3.1.3 Soft faults

6.3.1.3.1 Recovery

Soft faults do not require digital device replacement to restore the system to full capacity. Their effects can be mitigated at the system, electronic equipment, or component/device level. Some soft fault detection/mitigation methods are mentioned in 6.3.1.3. Additional guidance regarding mitigation of SEE-induced electronic equipment soft faults is found in Annex B.

6.3.1.3.2 System architecture

Like hard faults, at the architecture level, redundancy and redundancy management can provide coverage for soft faults. Regarding mitigation, since monitoring across redundant elements could be relatively easily implemented within computers, redundancy can be an effective means to detect the occurrence of faults. The occurrence of a fault can be detected by monitoring across two or more redundant electronic elements (e.g. computers).

In addition to soft fault detection, systems can be designed to provide timely recovery from soft faults: the design objective for such recovery mechanisms is that there shall be no significant effect on function performance, data integrity, and that they are not noticeable by pilots.

6.3.1.3.3 Electronic equipment

It is at electronic equipment level where the maximum benefits from optimised design to accommodate the SEE from electronic components can be gained. A number of techniques that enable the detection and correction of soft faults due to SEE at the component level are presented. As long as the hardware processing unit of a digital computer remains operational, software mitigation methods should be effective.

Soft faults at the component level, for example SEU (single/multiple bit upset, etc.) can be generally detected at the equipment level and some method of accommodation applied within the equipment.

These accommodation methods require resources and time to complete the accommodation, therefore there will be a maximum rate at which soft errors can be accommodated within the equipment.

Rapid recovery refers to an electronic equipment methodology where soft faults are detected in a timely manner, so that:

– state data can be recovered from a protected source;
– computation can be restarted from an appropriate place in instruction execution such that equipment and system recovery would be transparent to the function performance.

When corrupted data or errors are detected at equipment level, a number of recovery methods are available to be chosen depending on system requirements. Upon error detection, the associated data may be:

a) labelled as faulty;
b) the data may be selectively ignored;
c) the equipment may initiate a switch to a known uncorrupted redundant module;
d) the data is deleted and the affected process re-initialised from known good data.

An SEE within the control paths of a complex device (including microprocessors and microcontrollers) could produce a number of word errors as a result of an interruption of normal operation. These errors can be detected by comparison between a number of separate parallel functions or by detection of the large number of SEE errors.

Generally, combinational logic has not been subject to atmospheric radiation SEE. However, because devices with reducing critical charges and with operating frequencies increasing above 50 MHz are being applied to avionics electronics, consideration of the effects of propagation of combinational logic errors is necessary. These SEE are very fast transients of signal level from the correct logic level (glitches). These normally occur for a short period of time with respect to the clock signal, and are called single event transients (SET). SET can have a large impact on the clock signals where their edges may induce or terminate digital processes.

When the interruption of the device normal operation has been detected, the device can normally be recovered using a software reset. This takes a finite time and is dependent upon a sufficiently operational processing unit.

For the case of a non-operational processing unit, an independent hardware reset would be required. Again, as with a software reset, this would take a finite time. The status of equipment based upon complex electronic devices can be recovered from known good data. In order to provide recovery data a regularly refreshed atmospheric radiation tolerant memory may be employed.

Analogue single event transient (ASET) could be detected by:

a) comparison;

b) rate-of-change. Where the maximum rate of change for an analogue parameter or value is limited within defined normal system operating conditions, any rapid change due to SEE may be detected.

6.3.1.3.4 Electronic component/device

It would be possible to produce electronic controls in technology using larger feature sizes, and they would therefore be immune to SEE, but this would severely limit the capability and functionality of the equipment. Additionally, there may be problems with the availability of certain types of components in larger feature sizes, for example SRAM memory. At the component level, careful choice of certain component elements within the design can provide design benefits, for example the use of small amounts of atmospheric radiation tolerant devices as part of the total system memory.

Soft fault accommodation can be applied within a digital device:

– Random access memories typically can be configured to use some form of error detection and correction.

– The occurrence of a soft fault can be detected by monitoring across two or more redundant computing elements (triple modular redundant microprocessors are becoming common).

Alternatively, it is possible to design a complex system with current state-of-the-art technology accepting that SEE will occur and providing recovery mechanisms that may require the system to have a SEE tolerant memory backup storage for rapid recovery after detection of an event.

6.3.2 Level B systems

These systems shall be designed such that the failure rate of the function they provide is 10^{-7} or less, but may be greater than 10^{-9} per flight hour. The architectural approach should be based upon either:

a) level A rigour/discipline, or

b) architectures based upon failure/fault rates traceable to SEE tests on similar parts using test results from non-neutron testing facilities (see IEC 62396-1:2012, 7.4.3, 9.5.1 and 9.5.2).

6.3.3 Level C systems

These systems shall be designed such that the failure rate of the function they provide is 10^{-5} or less but may be greater than 10^{-7} per flight hour. The architectural approach should be based upon either:

a) level B rigour/discipline, or

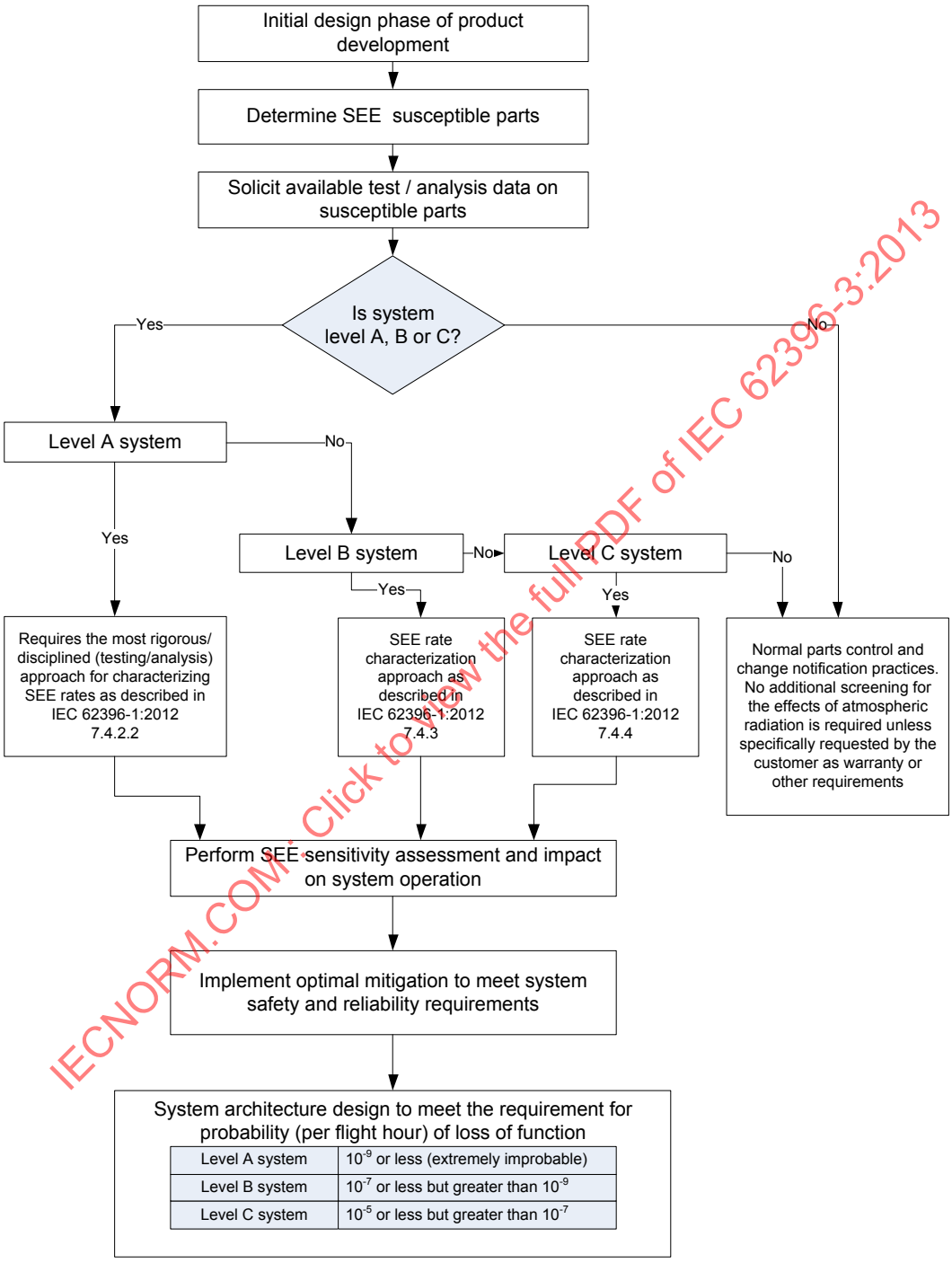
b) architectures based upon failure/fault rates traceable to testing results via a SEE failure/fault model (use of an average SEE error rate for all potentially sensitive components – in these instances, the SEE error rate may be high for some components and low for others, but the overall equipment failure rate can be expected to be acceptable (see IEC 62396-1:2012, 7.4.4, 9.5.1 and 9.5.2).

6.3.4 Levels D and E systems

These systems shall be designed such that the failure rate of the function they provide is 10^{-3} per flight hour or less (level D), and for level E systems there is no requirement. Since from a safety perspective, their failure effects are minor or none, these systems can use architectural approaches consistent with that based upon normal parts control and change notification practices (see IEC 62396-1:2012, 7.4.5, 9.5.1 and 9.5.2).

Annex A
(informative)

Design process flow diagram for SEE rates



Annex B
(informative)

Some mitigation method considerations for SEEs

B.1 General

Mitigation options include component level technology solutions, circuit design and fault-tolerant system architectures. The goal is, through a combination of mitigation techniques, to produce a system which meets all safety and reliability requirements.

The following guidelines provide examples of mitigation methods which can be employed for SEEs at the component, LRU and system level. While many mitigation schemes provide detection and corrections of soft faults, the design practice of logging errors which occur at the device level would provide system benefits.

B.2 Memory devices

At the chip level, there are a number of different techniques that can be used. Most RAM memory used in avionics systems are protected by an error correction code (ECC) also called error detection and correction (EDAC). This approach uses extra bits that are incorporated in each word to allow the erroneous bit to be identified and corrected. The most commonly used method of EDAC results in single error correction double error detection (SECDED).

With SECDED all single bit errors are corrected and detected, but if two bits are upset at one time (multiple cell upset), and if the bits are in two separate words, the error is equivalent to two independent single bit errors and SECDED succeeds by correcting the two errors. However, if the two errors are in same word, SECDED won't work because only one of the errors in the word will be corrected and the word will still remain in error. To avoid this, interleaving is generally used, meaning that the bits used in a logic word are selected to be physically separated from one another on the memory device, which greatly reduces the possibility of two errors being in the same word. This is because the bits that are upset by a single neutron strike will be physically adjacent to one another, since this effect is usually caused by charge sharing among the nearby bits or other mechanisms such as bipolar action in a well.

Additional types of on-chip error mitigation methods include:

- Parity, capable of detecting single bit errors.
- Cyclic redundancy code, capable of detecting multiple bit errors.
- Hamming code, normally capable of detecting two-bit errors and correcting one-bit error.
- Reed-Solomon code, capable of correcting multiple symbol errors.
- Convolution codes, capable of correcting burst of errors.
- Selective use of SEU-immune digital cell (e.g. flip-flop, latch, memory, counter register). Cell design options could include usage of large feature size transistors, energy storage within the cell structure, etc.
- RAM data use restrictions: data stored in RAM should not be assumed to be accurate, especially when that data has to be used for critical decisions/calculations – data could be recalculated instead of using the stored data. Many parameters may be only determined one time, such as at power on; such data is vulnerable to corruption, so use of such data should be minimized.
- Some designs read "program constants data " from upset-hard memory (ROM) only at power up and store this information in RAM which can suffer SEU. To mitigate RAM SEU

instead of relying on the stored information in the RAM, the hardware “constants” should be rewritten into the RAM from ROM memory at every available refresh cycle.

- When counting up in a computing process, action the “function” not only when required count is achieved but also when it is exceeded. Whilst the counter is counting up, should an SEU occur and the required count is exceeded, action the “function”; then the process is reset and the SEU impact limited; see example below. This limitation can be achieved by replacing strictly “greater than” or “less than” with “greater than or equal to” or “less than or equal to” respectively and also by the use of “greater than or equal to” or “less than or equal to” instead of “equal to", wherever possible. This is an example of counter usage; a process is required to be executed every 30 frames and this is done with the following code:

```
begin module
if count = 30
then turn all outputs on for 15 μs
end if
inc count
end module
```

If the RAM location that stored the 8-bit variable "count" had an SEU in bit 5 (or 6 or 7), then the value of count would be greater than 30. This would continue until "count" reached 255, at which point the variable increment would cause a wrap back to 0. With a frame time of 100 ms, an SEU turning on of all outputs could take an additional 23,3 s, i.e. instead of every 3 s, the output would occur at 25,3 s once and then recover. This could result in a nuisance fault that would cause the unit to be returned to the manufacturer where no fault would be found. To minimise the impact of SEU the code would be changed to:

```
begin module
if count ≥ 30
then turn all outputs on for 15 μs
end if
inc count
end module
```

- Refreshing a portion of the chip on a very frequent basis so that those bits, that are potentially liable to contain a SEE error, will only have an error for a brief period between refresh. The data should be refreshed at a rate such that no undesired system effects can result from erroneous operation within the duration of a refresh cycle.

B.3 Microprocessors

Microprocessors have complex circuitry, hidden registers, and cache memories, all of which contribute to SEE-induced errors. A single-bit upset can disrupt processor operation, either by changing an operation code or a data value that determines program execution. Resulting conditions include the issuance of an incorrect command, incorrect data or functional interrupts of system operation.

Mitigation techniques for microprocessors include parity checking, flushing of the low-end pipeline, refreshing cache, and implementing a dual processor configuration. Additional measures include implementing time redundancy at the end of each stage of the processor pipeline, the REESE approach (redundant execution using spare elements), reverse instruction generation and comparison, and two-rail coding. All of these solutions require additional logic and have significant impacts on performance. It is important, when selecting a microprocessor, to verify the upset protection of internal registers and cache memory functionality.

B.4 FPGAs

In complex devices like FPGAs, an effective way of protecting the SRAM bits within the configuration memory is by means of triple modular redundancy (TMR). With TMR three

sections of the memory carry out the same operation and the results are compared and voted on, so that if one of the sections is in error, it is voted out. A similar type of error mitigation technique that is sometimes applied to protect microprocessors is to utilize two processors that operate in “lock step” with one another. A fault in the circuit will be manifested as a difference in the results between the two circuits, and if such an error occurs, the circuit has to go back to the last state which had previously been correct.

B.5 System level techniques

- Parity.
- Cyclic redundancy checks (CRC).
- Checksums real-time configuration monitors.
- Watchdog timer (WDT), capable of detecting timing and scheduling errors. A "smart" WDT could expect a rotating 8-bit pattern, which could be written from several different software modules.
- Voting redundant outputs, capable of detecting and selecting most probable correct value.
- If multiple analogue process paths are used or values are obtained through several monitored redundant loops, then, in a similar way to the digital method, a deviating value can be detected by comparison. Triple modular and lockstep are examples of redundancy strategies used for digital processing electronics. Alternatively, the allowed analogue values may subject to constraint within predetermined limits and deviating values identified if outside these limits.
- Repeated calculations, capable of overcoming transient errors.
- Define constants in ROM locations.
- Write output states to hardware latches every frame. The hardware latch is susceptible to SEU.
- Continuously check the configuration state of devices that have been initialized by software. Data stored in SEU-susceptible locations in these devices defining the device configuration could be changed by an SEU. If the configuration state of a hardware device cannot be checked continuously, then reset the device and re-write the configuration state, if a continuous monitor detects a failure with the device.
- Rate of change. Where the maximum rate of change for a digital parameter or value is limited within defined normal system operating limits, any rapid change due to SEE corruption of a value may be detected.
- Filter input data. This includes ARINC 629 data, ARINC 429 data.
- Whenever BIT (Built-In Tester) detects a failure, rerun the test to confirm the failure. An SEU could have caused the test to fail or changed the RAM location containing the pass-fail flag.
- When using bi-directional I/O ports (an I/O port that can be programmed to be used as an input port or an output port), the configuration of the I/O port should be periodically refreshed. Example: some microprocessors require that the states of a bi-directional I/O port’s output buffers shall be all 1 s when the port is to be used as an input. Typically, such buffers power up in the default state of all 1 s, and if the design uses that port strictly as an input port and nowhere in the design is that state changed, then the design would never need to write 1 s to the output buffer. However, if the output state is not refreshed periodically, an SEU could disable the port’s ability to read inputs.

  The default power-up state should not be trusted; the required state should always be explicitly set by the system software.
- Where registers are used to define the CPU configuration, the configuration should be refreshed periodically.
- Pointers should be range-checked when used so that if corruption has occurred, the error may be detected. Similarly, integrator state values may need to be bounded and checked upon use.

- As the operating frequency of combinational logic has risen, the probability that “glitches” (very short duration deviations from the correct logic state) may be propagated through a logic block has risen. The effect of these glitches may be mitigated by using triple delay paths and voting at the end of the block. The three arms of the delay paths have staggered delays (direct, single delay, double delay), followed by majority voting. If the delay is longer than the glitch, then the signal is propagated glitch-free.
- For analogue signals, parallel signal and processing paths for the same function may be compared at a suitable stage to check that values are within expected tolerances of one another and within specified ranges.
- TVF (timing vulnerability factor) bits are not vulnerable to faults 100 % between writes. [4]
- AVF (architectural vulnerability factor) usually only for microprocessors (not all faults yield erroneous data or processing). [4], [5]