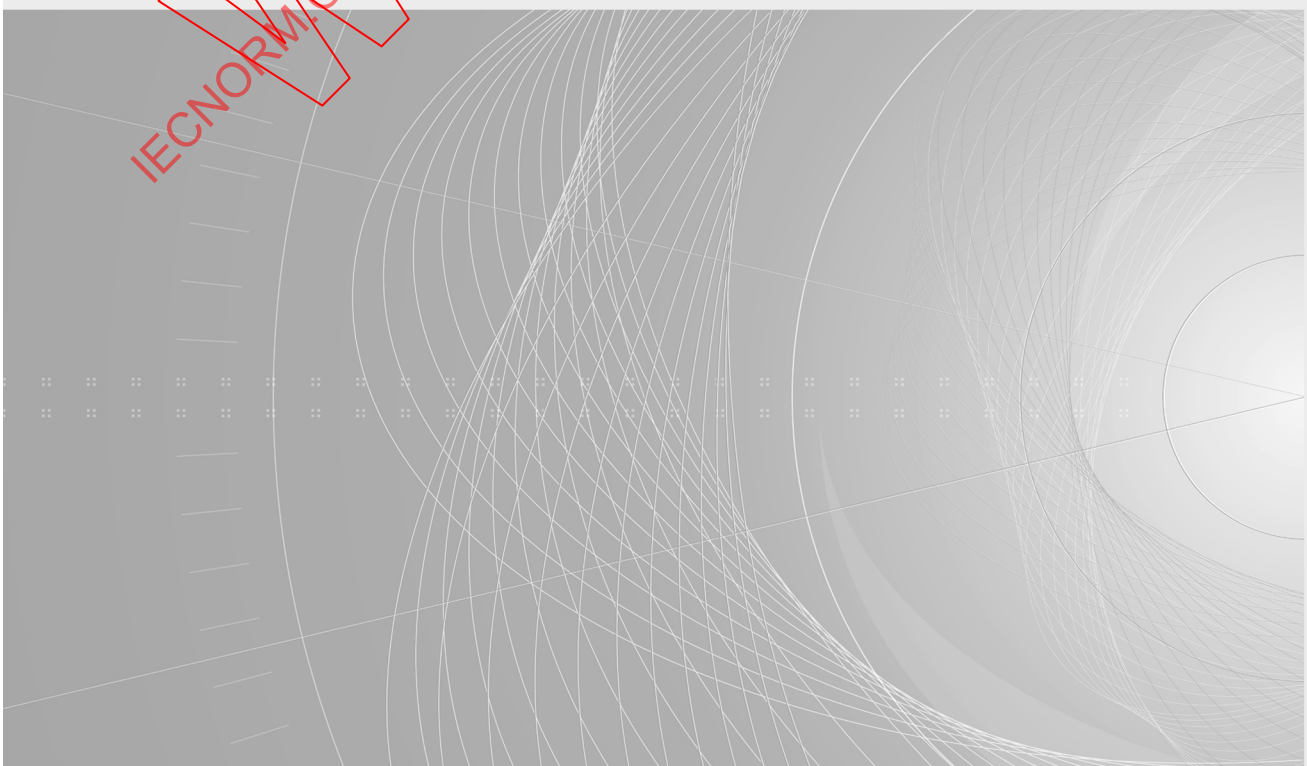
IEC/PAS 62396-3

Edition 1.0 2007-09

PUBLICLY AVAILABLE SPECIFICATION

PRE-STANDARD

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



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

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 It also gives information on projects, withdrawn and replaced publications.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

IEC/PAS 62396-3

Edition 1.0 2007-09

PUBLICLY AVAILABLE SPECIFICATION

PRE-STANDARD

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

INTERNATIONAL ELECTROTECHNICAL COMMISSION

PRICE CODE M

ICS 03.100.50; 31.020; 49.060

ISBN 2-8318-9203-1

CONTENTS

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.

A PAS is a technical specification not fulfilling the requirements for a standard but made available to the public.

IEC-PAS 62396-3 has been processed by IEC technical committee 107: Process management for avionics.

The text of this PAS is based on the following document:

This PAS was approved for publication by the P-members of the committee concerned as indicated in the following document:

Draft PAS	Report on voting
107/62/NP	107/73/RVN

Following publication of this PAS, which is a pre-standard publication, the technical committee or subcommittee concerned will transform it into an International Standard.

This PAS shall remain valid for an initial maximum period of three years starting from 2007-09. The validity may be extended for a single three-year period, following which it shall be revised to become another type of normative document or shall be withdrawn

IEC/PAS 62396 consists of the following parts, under the general title *Process management for avionics – Atmospheric radiation effects:*

- Part 2: Guidelines for single event effects testing for avionics systems
- Part 3: Optimising system design to accommodate the Single Event Effects (SEE) of atmospheric radiation
- Part 4: Guidelines for designing with high voltage aircraft electronics and potential single event effects
- Part 5: Guidelines for assessing thermal neutron fluxes and effects in avionics systems

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 PAS is intended to provide guidance to those involved in the design of avionic systems and equipment. 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 Hardware Assurance levels may be met.

2 Normative references

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

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

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

3 Terms and definitions

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

4 Avionic Systems

In IEC/TS 62396-1, it was detailed that systems for which failure may have the most severe impact on the aircraft are classified as level A and require the most rigorous approach to single event effects and parts control. Two examples of avionic systems are provided for the purposes of clarification.

4.1 Lift control flap and slat

The flow of air over the wing surfaces is controlled by flaps and slats, the position of the majority of these are under the pilot's control, redundancy may be achieved by having more than one actuation method. See Figure 1.

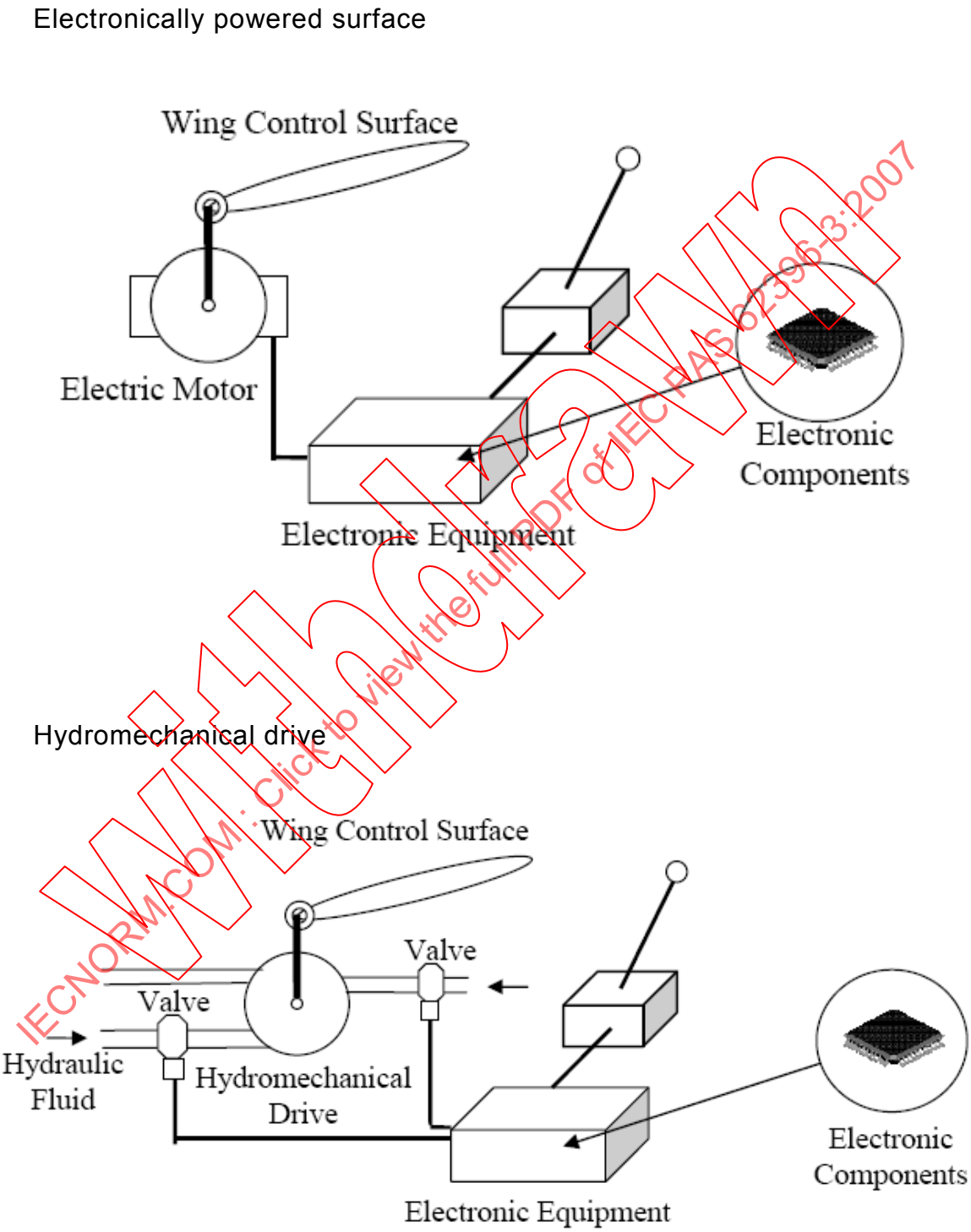


Figure 1 – Lift control flap and slat

4.2 Engine thrust

The engines have to provide thrust as required by the demand and the flight profile. If the aircraft has more than one engine, then loss of engine thrust may be accommodated by the level of redundancy. The engine equipment may be dual redundant and have two lanes either of which can perform the required function if the other fails. See Figure 2.

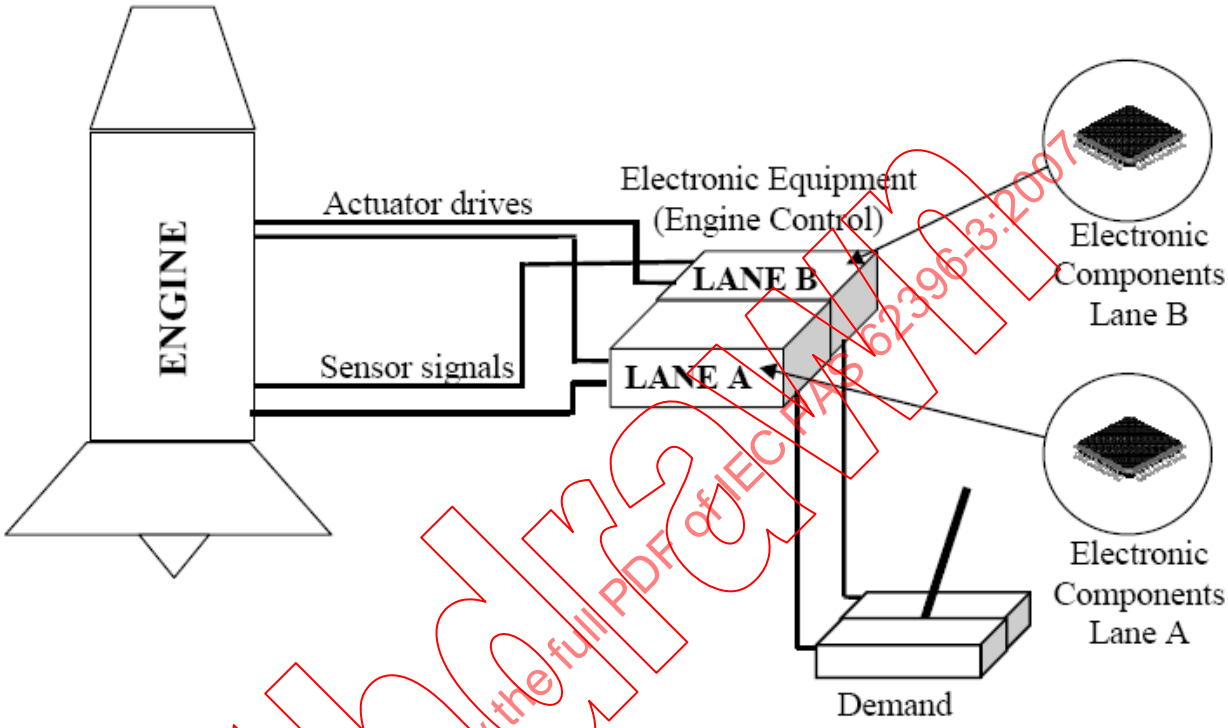


Figure 2 – Engine thrust

4.3 Systems impacted by atmospheric radiation

Atmospheric radiation may affect 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 SEE in the localised area within that device, which may potentially affect the equipment and in turn the system. Current avionic electronic systems use state of the art electronic components with feature sizes well below 1 µm, and SEE do occur in these devices but utilising correct system design aspects for the electronic elements an overall effect on the system performance is avoided. This type of approach requires careful selection and maintenance of electronic components throughout equipment level life see IEC/TS 62239.

The approach to system level optimization of design may be conducted by considering the system at 3 levels.

4.3.1 Aircraft system level

At system level, the System Assurance level may be met by having redundancy, for example multiple engines, below this at equipment level. The System Development Assurance level must be met, refer to IEC/TS 62396-1, Clause 7 and the references within that document.

4.3.2 Electronic equipment level

At the electronic equipment level, redundancy may be used as a method of mitigating failure regardless of whether the pilot is within the loop or not. The electronic equipment may also

employ alternative methods to avoid single point failure. In this PAS, we shall look at equipment level methods of accommodating component level SEE.

4.3.3 Component level

At component level, it is necessary to identify the atmospheric radiation effects on components which may be soft errors where functionality may be recovered or hard faults resulting in permanent failure of the component. The soft error effects may be accommodated by corrective actions within the electronic equipment. As identified in IEC/TS 62396-1, the most frequent SEE is a Single Event Upset that is a soft error effect.

4.4 SEE at system level

This Subclause provides consideration that goes down to component level.

4.4.1 Hard errors and effects

Hard and permanent failures are considered in exactly the same way as for other types of failure within the electronic equipment and for the System hardware assurance levels to be met, the aircraft system allowable failure metrics shall be met, for example MTTF and MTBUR. The atmospheric radiation may produce hard errors including Single Event Latch, SEL, SEFI, Single Event Functional Interrupt and Stuck bits where the hard fault is not recoverable by software reset and the complete removal of power from the component is required to recover normal operation, which will always occur when the equipment is depowered after use. Components that are subject to such SEE should either be avoided by careful selection and component management, or if the fault can be tolerated, then the event shall be logged to avoid unnecessary equipment removal.

4.4.2 Soft error accommodation

Soft errors at component level, for example Single Event Upset, Multiple Bit Upset are generally detected at equipment level and some method of accommodation applied within the equipment. Some methods of detection and accommodation are included in this PAS. These accommodation methods require resources and time to complete the accommodation, therefore there will be a maximum rate of such soft errors that can be accommodated within the equipment.

4.4.3 Component technology susceptibility

Since electronic technology may be included in all parts of any system redundancy, it is important that the rate at which SEE accommodation is required is low enough to avoid impact on the overall system redundancy mitigation. Therefore, to avoid a common mode failure during operation in periods of high neutron fluence, a limit on the soft error rate of any component technology used within the avionic system shall be enforced. This component technology limit may be applied as a combined soft error rate per bit within a designated worst case in the application environment.

5 Optimisation of system design

By suitable design at the equipment level and by careful selection and maintenance of electronic components employed within the design, the system level impact of SEE can be minimised.

5.1 Avionic system optimisation

Redundancy at the aircraft system level ensures that when the equipment level System Development Assurance levels are met, there is a reduced risk of problems from a system safety requirements aspect. However, the allocation of redundancy has an impact on the aircraft for several reasons. Redundancy of equipment will add weight, complexity, method of active equipment choice, increased reliability considerations, and cost. The impact of these

can be seen in that the improvements in overall system reliability that have allowed, in some flight profiles, the use of twin engined aircraft where in the past four engined aircraft would have been mandated.

Therefore it is at electronic equipment level where the maximum benefits from optimised design to mitigate the SEE from electronic components can be made. Although, at 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 parts of the total system memory.

5.2 Equipment level optimisation of soft error SEE

In this Subclause, a number of techniques will be presented that enable the detection and correction of soft errors and faults due to SEE at component level.

5.2.1 SEE Detection

Based on current electronics technology, a number of aspects of detection are identified (5.2.1.1 to 5.2.1.4). When corrupted data or errors are detected at equipment level, a number of scenarios may be chosen dependant on the type of data. Upon error detection, the associated data may be:

a) labelled as faulty;

b) selectively ignored;

c) ignored and the equipment may switch to a known uncorrupted redundant module;

d) deleted and the affected process re-initialised from known good data;

e) corrected using error detection and correction, EDAC within the equipment.

5.2.1.1 Digital memory errors and corrupted data

The atmospheric radiation causes upsets and it is necessary within the equipment to recognise that these have occurred within functional elements and if necessary, take action.

a) Parity

The data word has an additional single parity (odd or even) bit. When any bit within the word is changed, the words parity changes and a parity error can be detected, since the corrupted word parity will be different to the stored parity. This method detects single bit errors only. If two or more bits are changed by a single event within the word, the parity detection may fail to detect the error. As feature sizes and critical charge for SEE have become smaller, the potential for Multiple Bit Upset, MBU has risen; a single high energy neutron may cause upset to several bits in a localised area. Where the individual bits in a word are stored together (contiguously), then it is possible to corrupt several bits in the same word defeating parity error detection. For this reason, many manufacturers of digital memory store individual memory bits of a data word separated by several rows (non-contiguously).

b) Additional data codes

In order to detect (and correct) multiple bit upset, additional data has to be stored with the data word, and this has given rise to error correction codes, for example Hamming Code. The use of such codes will require additional data storage and handling overhead.

c) Comparison

If multiple process paths are used (for example three parallel processes), then voting can be used to mitigate SEE corrupted information. Alternatively, the allowed digital values may be subject to constraint within predetermined limits and identified if outside these limits.

d) 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.

5.2.1.2 Processor and control errors

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

5.2.1.3 Digital combinational logic upset

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

5.2.1.4 Analogue upset

Although analogue parts are generally considered immune to the 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 is an Analogue Single Event Transient, ASET.

a) Comparison

   If multiple analogue process paths are used or values obtained through several monitored redundant loops, then in a similar way to the digital method, a deviating value can be detected by comparison. Alternatively, the allowed analogue values may be subject to constraint within predetermined limits and deviating values identified if they are outside these limits.

b) Rate of change

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

5.2.2 Soft error accommodation, and error detection and correction

5.2.2.1 Digital memory errors and corrupted data

Several different methods may be used to detect and/or correct digital logic errors. Detection and correction methods for single errors in a data word require a minimum of additional memory overhead:

a) SECDED - Single Event Correct Double Event Detect;

b) DECTED - Double Event Correct Triple Event Detect;

c) error detection codes Hamming, etc.;

d) Triple Modular Redundancy, TMR – this requires a voting on the three paths.

5.2.2.2 Processor and control errors

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. The status of the complex device can be recovered from known good data. In order to provide recovery data, a regularly refreshed atmospheric radiation tolerant memory may be employed.