DOT/FAA/TC-15/62

Federal Aviation Administration
William J. Hughes Technical Center
Aviation Research Division
Atlantic City International Airport
New Jersey 08405

Single Event Effects Mitigation Techniques Report

February 2016

Final Report

U.S. Department of Transportation
Federal Aviation Administration

NOTICE

This document is disseminated under the sponsorship of the U.S. Department of Transportation in the interest of information exchange. The U.S. Government assumes no liability for the contents or use thereof. The U.S. Government does not endorse products or manufacturers. Trade or manufacturers' names appear herein solely because they are considered essential to the objective of this report. The findings and conclusions in this report are those of the author(s) and do not necessarily represent the views of the funding agency. This document does not constitute FAA policy. Consult the FAA sponsoring organization listed on the Technical Documentation page as to its use.

This report is available at the Federal Aviation Administration William J. Hughes Technical Center's Full-Text Technical Reports page: actlibrary.tc.faa.gov in Adobe Acrobat portable document format (PDF).

Technical Report Documentation Page

1. Report No. DOT/FAA/TC-15/62	2. Government Accession No.	3. Recipient's Catalog No.

4. Title and Subtitle SINGLE EVENT EFFECT MITIGATION TECHNIQUES REPORT	5. Report Date February 2016
	6. Performing Organization Code
7. Author(s) L.H. Mutuel	8. Performing Organization Report No. D12
9. Performing Organization Name and Address Thales Avionics, Inc. 2811 South 102nd Street, Suite 100 Seattle, WA 98168	10. Work Unit No. (TRAIS)
	11. Contract or Grant No. DTFACT-13-D-0008
12. Sponsoring Agency Name and Address Federal Aviation Administration FAA National Headquarters 950 L'Enfant Plaza N SW Washington, DC 20024	13. Type of Report and Period Covered Final Report
	14. Sponsoring Agency Code AIR-134

15. Supplementary Notes

The Federal Aviation Administration Aviation William J. Hughes Technical Center Aviation Research Division COR was John Zvanya.

16. Abstract

The research objectives were to articulate the criteria for selecting components for single event effect (SEE) analysis and collect considerations pertaining to SEE mitigation techniques. A proposed process to integrate the SEE analysis that incorporates this information is defined at both the system and equipment level. The following highlights the main take-away findings.

The requirement to perform an SEE safety analysis as part of the system level safety assessment is dependent on the system criticality, contribution of the system to catastrophic and/or hazardous failure conditions. The analysis results in the determination of whether or not the SEE error rate is acceptable with regard to the safety objectives.

The determination of the SEE error rate can be made at different levels of system integration (e.g., electronic component, integrated circuit, system, and equipment) and with different levels of accuracy. The system designer needs to ensure that the data supporting the determination of the SEE rate are commensurate with the criticality of the system to be assessed. The vast majority of the recommendations are therefore related to the acceptable level of scrutiny to be applied.

Similarly, the selection and effectiveness of mitigation techniques are dependent on the type of SEE to be mitigated and the functions of the component to be protected. All mitigations carry penalties and no mitigation covers the full range of SEE. The system developer will use its knowledge of the circuit layout, critical elements, and functions to determine tradeoffs between protection coverage and the level of effectiveness of the mitigation and associated penalties, which are specific to each design.

Because there is no one-fits-all strategy to address SEE, there are recommended avenues and minimum substantiation to be provided by the system designer as part of the demonstration of compliance with SEE safety assessment.

17. Key Words Single event effect, Semiconductor electronics, Mitigation, Safety assessment	18. Distribution Statement This document is available to the U.S. public through the National Technical Information Service (NTIS), Springfield, Virginia 22161. This document is also available from the Federal Aviation Administration William J. Hughes Technical Center at actlibrary.tc.faa.gov.

19. Security Classif. (of this report) Unclassified	20. Security Classif. (of this page) Unclassified	21. No. of Pages 296	22. Price

TABLE OF CONTENTS

APPENDICES

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS AND ACRONYMS

AC	Alternating current
ACARS	Aircraft communications addressing and reporting system
ADC	Analog to Digital Converter
ADF	Automatic Direction Finder
AFGCS	Auto-Flight Guidance and Control System
AHRS	Attitude and Heading Reference System
AIMS	Aircraft Information Management System
ARP	Aerospace Recommended Practice
ASIC	Application-specific integrated circuit
ATA	Air Transport Association [of America] (currently known as Airlines for America$^{\circledR}$)
ATCRBS	Air Traffic Control Radar Beacon System
BCH	Bose-Chaudhuri-Hocquenghem
BISER	Built-in Soft Error Resilience
BJT	Bipolar junction transistor
BLM	Backlighting module
BoM	Bill of material
BRAM	Block random access memory
CAM	Content addressable memory
CAS	Crew Alerting System
CAT	Catastrophic (failure condition)
CD	Center display
CDS	Cockpit display system
CLB	Configurable logic block
CM	Certification Memorandum (EASA)
CMA	Common mode analysis
CMOS	Complementary metal-oxide semiconductor
CPM	Core processing module
CPU	Central processing unit
CRC	Cyclic redundancy code
DAC	Digital-to-analog converter
DAEC	Double adjacent error correction
DAL	Development assurance level
DC	Direct current
DICE	Dual interlock storage cell
DME	Distance measuring equipment
DMR	Double modular redundancy
DRAM	Dynamic random access memory
DSM	Deep sub-micron
DTMR	Double-triple modular redundancy
DU	Display unit
DUT	Device under test
DWC	Duplication with comparison
EASA	European Aviation Safety Agency
ECC	Error correcting code

ECP	EICAS control panel
EDAC	Error detection and correction
EEPROM	Electrically erasable programmable read-only memory
EICAS	Engine indication and crew alerting system
EPLD	Erasable programmable logic device
EWD	Engine and Warning Display
EWE	EDAC word error
EWER	EDAC word error rate
FC	Failure condition
FCC	Flight control computer
FET	Field effect transistor
FF	Flip-flop
FFPA	Functional failure path analysis
FHA	Functional hazard assessment
FIT	Failure in time
FMEA	Failure mode and effects analysis
FMES	Failure mode and effects summary
FMS	Flight management system
FPGA	Field programmable gate array
FTA	Fault tree analysis
FWS	Flight warning system
GGM	Graphic generation module
GPU	Graphics processing unit
HAZ	Hazardous (failure condition)
HF	High frequency
HFDL	High-frequency data link
HIT	Heavy ion transient
I/O	Input/output
ICD	Invalid corrupted data
IEEE	Institute of Electrical and Electronics Engineers
IGBT	Insulated gate bipolar transistor
IL	Inner left
IMA	Integrated modular avionics
IOM	Input/output module
IP	Internet Protocol
IR	Inner right
LAM	LCD assembly module
LCD	Liquid crystal display
LET	Linear energy transfer
LNAV	Lateral navigation
LP	Localizer performance
LPV	Localizer performance with vertical guidance
LRU	Line replaceable unit
LUT	Lookup table
MAJ	Major (failure condition)
MBU	Multiple bit upset

MCU	Multiple cell upset
MFD	Multi-format display
MIN	Minor (failure condition)
MOSFET	Metal-oxide-semiconductor field effect transistor
MTBE	Mean time between errors
MTBF	Mean time between failure
MTBUR	Mean time between unscheduled removal
MTTR	Mean time to repair
NAND	NOT AND
NASA	National Aeronautics and Space Administration
ND	Navigation Display
NOR	NOT OR
NSE	No safety effect
OL	Outer left
OpAmp	Operational amplifier
OR	Outer right
PFD	Primary Flight Display
PLD	Programmable logic device
PN	Junction formed from p-type and n-type semiconductor materials
PRAM	Phase-changed random access memory
PROM	Programmable read-only memory
PSM	Power supply module
PSSA	Preliminary system safety assessment
QDI	Quasi delay insensitive
RADECS	Radiation Effects Data Workshop
RAM	Random access memory
RCP	Reconfiguration control panel
RCS	Recoverable Control System
RHBD	Radiation hardened by design
RHBP	Radiation hardened by process
RNP	Required Navigation Performance
ROM	Read-only memory
SB	Safety barrier
SD	System Display
SEB	Single Event Burnout
SEC-DED	Single error correction and double error detection
SED	Single event disturb
SEDR	Single event dielectric rupture
SEE	Single event effects
SEFI	Single event functional interrupt
SEGR	Single event gate rupture
SEL	Single event latch-up
SERT	Single event resistant topology
SESB	Single Event Snap-Back
SET	Single event transient
SEU	Single event upset

SEUPI	Single event upset probability impact
SHE	Single Event Hard Error
SIRF	Single event immune reconfigurable FPGA
SJ	Super junction
SOI	Silicon on insulator
SPS	SEL protection switch
SRAM	Static random access memory
SSA	System safety assessment
SSM	Sign/status matrix
TAWS	Terrain Awareness and Warning System
TCAS	Traffic Alert and Collision Avoidance System
TID	Total ionization dose
TMR	Triple modular redundancy
TSO	Technical Standard Order
UHF	Ultra-high frequency
VBI	Vulnerability-based interleaving
VCD	Valid corrupted data
VHF	Very high frequency
VNAV	Vertical navigation
VOR	VHF omnidirectional radio
*x*AED	Scalable adjacent error detection

EXECUTIVE SUMMARY

The research objectives for this report were to articulate the criteria to select avionics components and systems for which a single event effect (SEE) safety analysis should be performed and to develop a compendium on SEE mitigation techniques and the assessment of their effectiveness. Both aspects are integrated in the proposed process for system-level and equipment-level safety assessment, explicitly incorporating SEE considerations. This report organizes the findings and recommendations according to the steps of the safety assessment.

The requirement to perform an SEE safety analysis, as part of the system level safety assessment, is dependent on the system criticality, namely on the system's involvement in catastrophic (CAT) or hazardous failure conditions (FCs). The error rates caused by SEEs at the system level are integrated within the system failure rates. The objective at the system level is to verify that the consolidated failure rates are compliant with the safety objectives derived from the functional hazard assessment of the system. At system level, the SEE error rates need to be coherent with the operational functions and the mission profile of the aircraft.

The SEE safety analysis is conducted at equipment level and relies on the determination of SEE error rates on the relevant equipment. Relevance is first characterized by the presence of semiconductor electronics in the equipment, then by the type of functions implemented by these components. Although all types of SEEs need to be considered during the start of the analysis, the type of electronics and functionality may justify a focus on the most relevant types of SEEs. The determination of the SEE error rate can be made at different levels of system integration (e.g., electronic component, integrated circuit, system, and equipment) and with different levels of accuracy. The system designer needs to ensure that the data supporting the determination of the SEE rates are commensurate with the criticality of the equipment to be assessed, implementing semiconductor technology, and envisioned operations.

Similarly, the selection and effectiveness of mitigation techniques are dependent on the type of SEE to be mitigated and functions of the component to be protected. All mitigations carry penalties and no mitigation covers the full range of SEEs. The system developer will use its knowledge of the circuit layout and critical elements and functions to determine tradeoffs between protection coverage, level of effectiveness of the mitigation, and the associated penalties. Each SEE is a statistically independent event; therefore, at the level of an integrated circuit or avionics equipment, the aggregated SEE error rate may be the result of several possible combinations of elemental SEE error rates. This wide range of possibilities makes the mitigation strategy specific to each design.

The safety analysis at equipment level is completed when the SEE error rate is found to be negligible (i.e., an order of magnitude lower) compared to the failure rates obtained from the failure mode and effects analysis of the equipment. If it is not negligible, redesign is needed either at the component level or system level if the system level FC was CAT. Redesign may include changing the electronic component or adding mitigations.

Because there is no one-fit-all strategy to address SEEs and their mitigations, there are recommended avenues and minimum substantiation to be provided by the system designer as part of the demonstration of compliance with SEE safety assessment.

1. INTRODUCTION

1.1 PURPOSE

The objectives of this research support the development of guidelines for the acceptance of semiconductor microelectronic devices and electronic systems. They are illustrated through a series of recommendations and guidelines for the successful insertion of a specific analysis of single event effects (SEEs) that integrate within the system safety assessment (SSA) process. Specifically, the research findings articulate the following:

- The identification of components sensitive to SEEs
- The considerations to be made when assessing mitigation techniques against SEEs
- The integration of the SEE analysis within the SSA process at system and equipment levels

This document is organized around key elements of the safety analysis to be performed. Section 2 starts with the overview of SEEs and their impact on semiconductor microelectronics used in avionics, then presents a high-level view of the safety assessment process at system level and equipment level, including the specific steps for the SEE analysis. Sections 3–7 detail the research findings at system and equipment level and present a detailed rationale for the recommendations in section 8. This section gathers the recommendations sorted thematically to reflect the findings described earlier. Finally, summary statements on the investigations performed, which are open to areas of future research, are included in section 9.

The reader is directed to sections 2 and 8 for a quick read through of the material (without reading through the investigations) to extract the essence of the findings.

References are listed in section 10. A glossary for electronic components impacted by SEEs is provided in appendix H.

Appendices offer supplemental information in the form of a full list of Air Transport Association (ATA) chapter numbers (A), examples of failure rates for Xilinx products (B), details on the static memory content of Xilinx Virtex-5 (C), the details of the fault tree analysis (FTA) for the cockpit display example (D), a summary of the recommendations organized by proposed SEE analysis phase (E and F), and an example worksheet to determine SEE rates (G).

1.2 BACKGROUND

Several trends in avionics systems justify the further consideration of atmospheric radiation in the design phase:

- Both the increased density of semiconductors and the lower voltages increase the sensitivity to atmospheric radiation.
- The significant increase in the number of memory bits and registers increases the likelihood of an SEE.

- Flights at higher altitudes, for extended duration and/or on polar routes, increase the exposure time to atmospheric radiation.

The various effects of atmospheric radiation can be mitigated at various levels of efficiency and application (e.g., semiconductor layers, device, equipment, or system). The guidelines for the acceptance of semiconductor microelectronic devices and electronic systems need to be developed while considering the appropriate match between the mitigation techniques, effects to be mitigated, and acceptable error rates for the system. If the sensitivity to a single event is not integrated in the safety analysis, it may produce an overly optimistic safety assessment, allowing the implementation of a design that will exhibit higher failure rates in-service. Conversely, integrating overly stringent safety arguments for single events may increase allotted condition (FC) budgets, resulting in designs that are more costly and complex.

1.3 METHODOLOGY

This research was organized into five technical tasks highlighting steps in the SEE safety analysis process:

1. The identification of safety critical avionics components and systems in transport aircraft, rotorcraft, and engines that may experience FCs related to SEEs (detailed research included in section 3).
2. The identification of mitigation techniques against SEEs applicable to the components and systems identified as sensitive (detailed research included in section 4).
3. A focused investigation on the most common mitigation technique not built into devices to highlight potential trade-space, its effectiveness, and its limitations. Redundancy is the technique selected (detailed research included in section 5).
4. A focused investigation on the most common mitigation technique that is built into devices to highlight potential trade-space, its effectiveness, and its limitations. Error correcting code (ECC) is the technique selected. Detailed research is included in section 6).
5. The performance of a sample SSA on one of the systems identified as sensitive. A cockpit display system (CDS) is selected. Detailed research is included in section 7)

The final activity involved collecting the findings of the previous activities and producing a series of recommendations to support the development of the guidance material shown in section 8.

Figure 1 summarizes the methodology and flow of information between research activities.

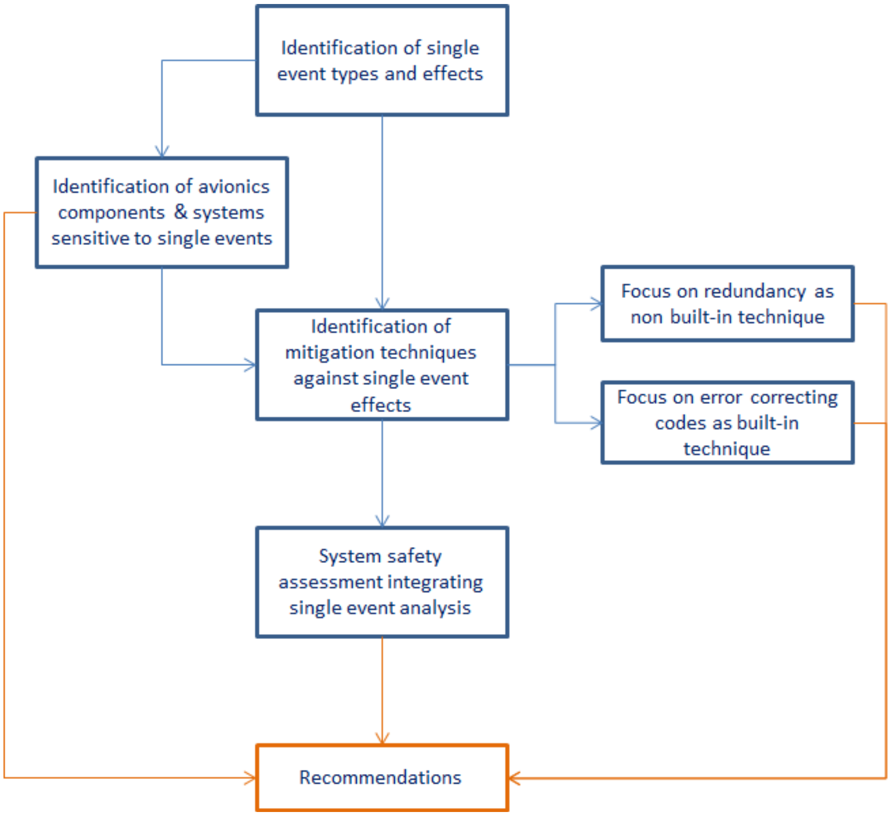

Identification of single event types and effects
Identification of avionics components & systems sensitive to single events
Identification of mitigation techniques against single event effects
Focus on redundancy as non built-in technique
Focus on error correcting codes as built-in technique
System safety assessment integrating single event analysis
Recommendations

Figure 1. Summary information flow between research activities

1.4 THE SEE DEFINITION

The European Aviation Safety Agency (EASA)[1] defines SEE as:

“Atmospheric radiation is a generic term which refers to all types of electromagnetic radiation which can penetrate the earth’s atmosphere. The main contributors to atmospheric radiation are solar and galactic radiation. Solar radiation is emitted from the sun and galactic radiation originates from outside our solar system. Both types of radiation can be affected (distorted or bent) by the earth’s magnetic field.

SEEs occur when atmospheric radiation, comprising high energy particles, collide with specific locations on semiconductor devices contained in aircraft systems. Memory devices, microprocessors and FPGAs[1] are most sensitive to SEE.

Some examples of these types of effects are Single Event Upsets (SEU), Multiple Bit Upset (MBU), Single Event Gate Rupture (SEGR) and Single Event Burn-out (SEB). However, SEU and MBU are the two single effects that present the largest potential threat to aircraft systems.

The rates of SEE are likely to be greater on aircraft flying at high altitudes and high geographic latitudes. This is due to the effects of atmospheric absorption and magnetic deflection of solar and galactic radiation. Although the intensity of atmospheric radiation varies with altitude and geographic latitude, the high energy particles are randomly distributed at any given location. Due to this, the predicted SEE rates can be derived based on the

[1] Field Programmable Gate Arrays

characteristics of the aircraft equipment (number of vulnerable elements) and operating conditions (altitude, latitude).”

2. SEE TYPES AND ANALYSES

2.1 TYPES OF SEE

SEEs can be classified into two broad categories: destructive and non-destructive [2]. Because a destructive effect is permanent, a nondestructive effect can be either temporary or permanent. Finally, the functional impacts range from data corruption to loss of function.

2.1.1 Descriptions of SEE

2.1.1.1 SEU

An SEU causes a change of state in a storage cell. The SEU affects memory devices, latches, registers, and sequential logic. Depending on the size of the deposition region and the amount of charge deposited, a single event can upset more than one storage cell (i.e., the charge is collected by multiple transistors) and the effect is called a multiple cell upset (MCU).

2.1.1.2 MBU

An MBU is defined as a single event that causes more than one bit to be upset during a single measurement. During an MBU, multiple bit errors in a single word can be introduced, as well as single bit errors in multiple adjacent words.

2.1.1.3 Single Event Functional Interrupt

The loss of functionality (or interruption of normal operation) in complex integrated circuits due to perturbation of control registers or clocks is called a single event functional interrupt (SEFI). An SEFI can generate a burst of errors or long duration loss of functionality (e.g., lockup). In general, an SEFI is not accompanied by a high current condition associated with a single event latch-up (SEL) or single event snap-back (SESB). The functionality may be recovered either by cycling the power, resetting, or reloading a configuration register.

2.1.1.4 Single Event Transient

A single event transient (SET) is a short (transient) impulse generated in a gate resulting in the wrong logic state at the combinatorial logic output. The wrong logic state will propagate if it appeared during the active clock edge. The pulse may eventually be latched in a storage cell (e.g., a latch or flip-flop [FF]). However, three types of masking can limit the propagation down to an error and can be the basis for the following mitigation techniques: logic masking (SET affects a non-sensitized path), latch window or timing masking (SET affects elements outside their latching time window), and electrical masking (SET is attenuated by subsequent logic gates until filtered out)[3].

2.1.1.5 Single Event Disturb

The transient unstable state of a static random access memory (SRAM) cell is described as resulting from a single event disturb (SED). This unstable SRAM state will eventually reach a stable state and the characterization will fall under SEU. Because the unstable state of the cell can be long enough that read instructions can be performed and soft errors generated, SEDs are identified separately.

2.1.1.6 Single Event Hard Error

A single event hard error (SHE) is used to highlight the fact that the neutron-induced upset (e.g., SEU, MBU) is not recoverable. For example, when a particle hit causes damage to the device substrate in addition to the flipping bit, an SHE is declared in lieu of an SEU.

2.1.1.7 The SEL

In a four-layer semiconductor device, an SEL occurs when the energized particle activates one of a pair of the parasitic transistors, which combines into a circuit with large positive feedback. As a result, the circuit turns fully on and causes a short across the device until it burns up or the power is cycled. The effect of an electric short is potentially destructive when it results in overheating of the structure and localized metal fusion.

2.1.1.8 SESB

SESBs are a subtype of SEL and, like SEL, they exhibit a high current consuming condition in the affected device. When the energized particle hits near the drain, an avalanche multiplication of the charge carriers is created. The transistor is open and remains so (hence, the reference to a latch-up condition) until the power is cycled (the device snaps back).

2.1.1.9 Single Event Burnout

A single event burnout (SEB) is a condition that can cause device destruction due to a high current state in a power transistor, and the resulting failure is permanent. An SEB susceptibility has been shown to decrease with increasing temperature. SEBs include burnout of power metal-oxide-semiconductor field effect transistor (MOSFET), gate rupture, frozen bits, and noise in charge-coupled devices.

2.1.1.10 SEGR

An SEGR is caused by particle bombardment that creates a damaging ionization column between the gate oxide and drain in power components. It typically results in leakage currents at the gate and drain that exceed the normal leakage current on a non-exposed device. SEGRs may have destructive consequences.

2.1.1.11 Single Event Dielectric Rupture

The single event dielectric rupture (SEDR) has been observed in testing but not in space-flight data. Therefore, it is currently considered mostly an academic curiosity. An SEDR is identified from a small permanent jump in the core power supply current.

2.1.2 Criteria for Determining SEE Sensitivity

The probability of an SEE occurring depends on the amount of energy deposited on the semiconductor material. For short segments of high-energy particle tracks, the energy deposited by a single event is proportional to the chord length of the sensitive material. Therefore, the device shape and size is critical to determine the SEE-sensitivity; the smaller the feature size, the higher the sensitivity to radiation.

Table 1 proposes the major dependencies existing between SEE types, technology, and environmental factors. Not all SEE types have evident correlation, such as SEFI, which can stem from various sources. The table can be used by system developers as a reminder to pay specific attention when obtaining substantiation information (e.g., temperature testing for SEL and SEB).

Table 1. Trend correlations between SEE types, technology, and environmental factors

	Non-Destructive SEE Categories						Destructive SEE Categories					
	SEU	MBU	MCU	SEFI	SET	SED	SHE	SEL	SESB	SEB	SEGR	SEDR
Feature size ↘	↗[2]				↗		↗			↗		
Cell density ↗	↗	↗	↗									
Power (voltage) ↘	↗[3]	↗[3]								↗[4]		
Direct current ↗										↗		
Switching speed ↗	↗[5]						↗[5]					
Clock frequency ↗		↗										
Pulse width ↗					↗							
Crosstalk ↗		↗										
Temperature ↘								↘[6]		↗		
Altitude ↗										↗		

[2] The deep sub-micron technology is sensitive, with a typical threshold value of 90 nm.

[3] Protons more likely generate MBU, whereas neutrons generate SEU.

[4] SEB is inversely related to the voltage stress, but the relationship is highly nonlinear.

[5] Increased switching speed affects the substrate and therefore increases the proportion of SEU that are not recoverable.

[6] The dependency of SEL to temperature is related to the increase of cross-section with temperature. This increase can be captured by testing; it is difficult to model.

2.1.3 Synopsis of SEE types, Effects, and Impacted Electronic Components

Table 2 provides a summary view of the types of SEEs, the visible effects, and the types of electronic components sensitive to the SEE type. When considering the impact of a single event, the designer should investigate the local direct impact as well as the potential for propagation because different mitigation techniques will be applied.

Table 2. Overview of SEE

SEE type	Effect	Affected Electronics
SEU	Corruption of the information stored in a memory element	Memories, latches in logic devices
MBU	Corruption of several memory elements in a single hit	Memories, latches in logic devices
SEFI	Loss of normal operation	Complex devices with built-in state/control sections
SET	Impulse response of certain amplitude and duration	Analog and mixed-signal circuits, photonics
SED	Momentary corruption of the information stored in a bit	Combinatorial logic, latches in logic devices
SHE	Unalterable change of state in a memory element	Memories, latches in logic devices
SEL$^{(*)}$	High-current conditions	CMOS[7], BiCMOS[8] devices
SESB$^{(*)}$	High-current conditions	N-channel MOSFET
SEB$^{(*)}$	Destructive burnout	Bipolar junction transistors, N-channel power MOSFET
SEGR$^{(*)}$	Rupture of gate dielectric	Power MOSFET
SEDR$^{(*)}$	Rupture of dielectric	Non-volatile NMOS[9] structures, FPGA, linear devices

Note: $^{(*)}$ = potentially destructive SEE-types, NMOS = n-metal oxide semiconductor

[7] Complementary Metal-Oxide Semiconductor

[8] Bi-complementary Metal-Oxide Semiconductor

[9] N-Metal-Oxide Semiconductor

2.2 SAFETY ANALYSIS

Compliance with the regulatory documents is demonstrated via a combination of analyses and testing defined in the aviation regulations as acceptable means of compliance. The demonstration of compliance involves several quantitative and qualitative analyses for which guidelines can be found in reference [4].

Such analyses include:

- Significant single failure analysis using failure mode and effects analysis (FMEA) at equipment level
- Significant multiple FCs analyses:
    - FTA techniques applied at system level
    - Common mode analysis (CMA) applied at system level
    - Development assurance level (DAL) allocation

2.2.1 Objectives and Scope of the SEE Analysis

The objective of the SEE safety analysis is to demonstrate that the system is adequately mitigated against SEEs. Such mitigations can be achieved through architectural system considerations, equipment design, component selection, component testing, or a suitable combination thereof. Section 2.4.3 discusses the research findings with regard to mitigation techniques.

The effect of atmospheric radiation is one factor that could contribute to equipment loss or malfunction. From a system safety perspective, the existing methodology covering random failures (i.e., FMEA and FTA) is used in the assessment of atmospheric radiation effect rates and consequences [1].

This analysis assumes normal atmospheric radiation levels, meaning levels that could be experienced during a typical flight, but not levels that could be experienced during a solar flare. As stated in references 1, 5, and 6, solar flares that result in the arrival of large bursts of solar particles into the atmosphere (creating a significant increase in atmospheric radiation with higher levels than normally expected and of a short duration [order of hours]) should result in operational limitations relating to the routing of the flight (i.e., avoiding high latitudes).

2.2.2 SEE Analysis Method

Figure 2 illustrates the proposed SEE analysis method and its integration within the overall safety analysis, and figure 3 is the corresponding legend. The process covers the safety analysis at both system level and equipment level. These aspects will be detailed in sections 2.3 and 2.4, respectively.

At the system level, the preparation phase includes the description of the system and its operational functions. The environment in which the system is intended to be operated is defined within the aircraft mission profile. In accordance with Aerospace Recommended Practice (ARP) 4761 [4], a functional hazard assessment (FHA) is used to derive FCs associated with the system, its functions, and its operational environment. A first inner loop consists of verifying the compliance with the safety objectives associated with the FHA-derived FCs, taking into account the safety barriers (SBs) implemented in the system architecture. Relevant SEE mitigations are included in the system-level SBs. The verification uses a system-level fault-tree analysis and a common mode analysis. The FTA is the input to the CMA, which is performed for AND gates and catastrophic (CAT) FCs. The output of the fault-tree analysis is the determination of quantitative safety budgets and associated DAL for each component of the system. The analysis then shifts from the system to the equipment level.

The SSA is completed when compliance with the safety objectives is shown for the design. System-level SBs are adjusted until the compliance is demonstrated.

At the equipment level, the SEE analysis is performed for all equipment involved in CAT and hazardous (HAZ) FCs, and includes the determination of SEE-sensitive components, the identification of mitigation methods that are implemented and their coverage (qualitatively), and a quantitative assessment of error rates due to SEEs. The equipment FMEA is performed based on its functional breakdown and built-in tests mechanisms side by side with the SEE analysis. A first verification of compliance against the quantitative safety budget allocated to the equipment is performed to validate the design. The SEE safety analysis is integrated via the comparison of the SEE error rate against the FMEA-derived rate. If the SEE contribution is negligible, the design is validated. If not, the process moves to redesign, either at the equipment or system level. The process may be iterative, each step integrating the SEE impact in the fault-tree budgets.

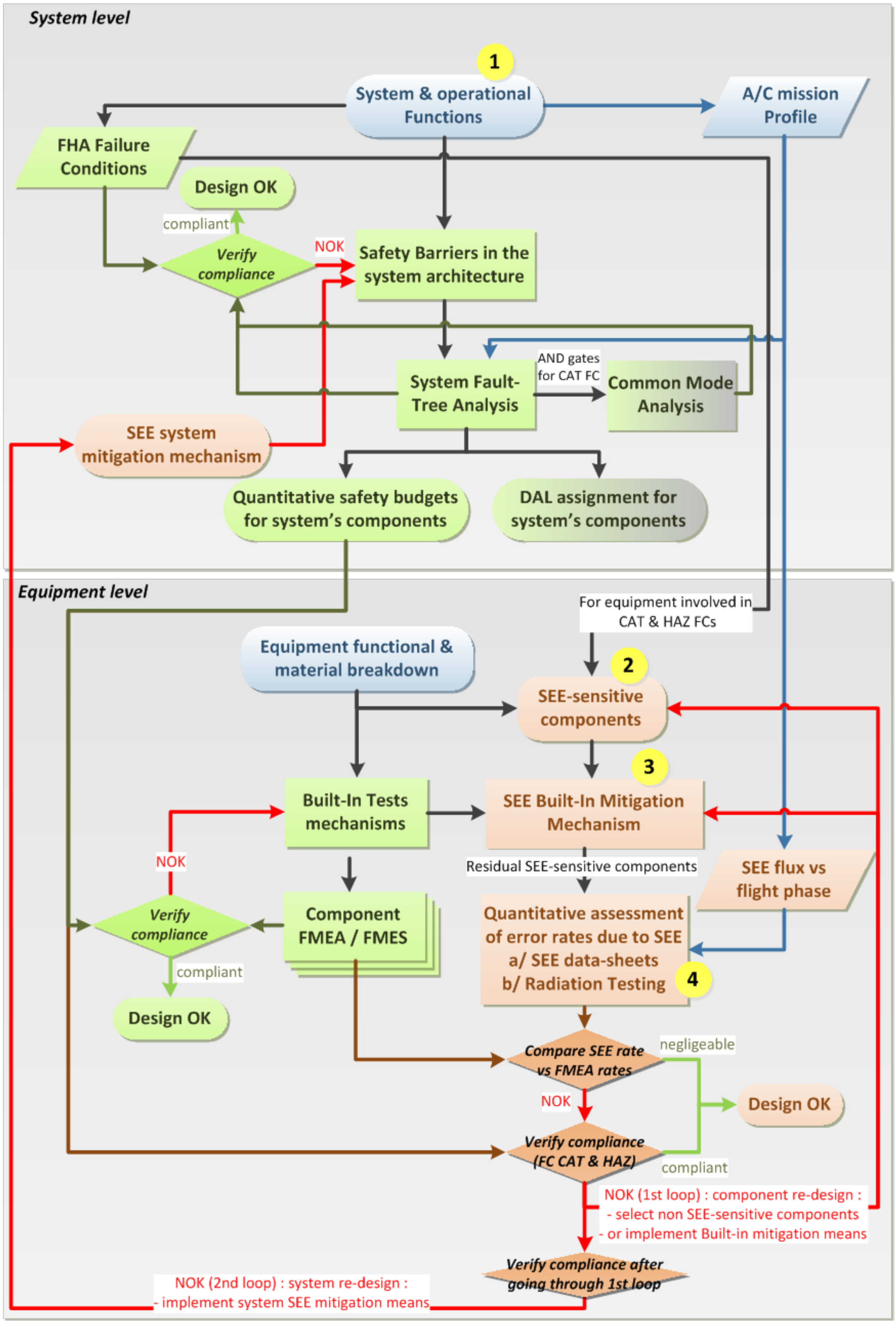

System level
1
System & operational Functions
A/C mission Profile
FHA Failure Conditions
Design OK
compliant
Verify compliance
NOK
Safety Barriers in the system architecture
AND gates for CAT FC
System Fault-Tree Analysis
Common Mode Analysis
SEE system mitigation mechanism
Quantitative safety budgets for system's components
DAL assignment for system's components
Equipment level
For equipment involved in CAT & HAZ FCs
Equipment functional & material breakdown
2
SEE-sensitive components
3
Built-In Tests mechanisms
SEE Built-In Mitigation Mechanism
NOK
Residual SEE-sensitive components
SEE flux vs flight phase
Verify compliance
Component FMEA / FMES
Quantitative assessment of error rates due to SEE
a/ SEE data-sheets
b/ Radiation Testing
4
compliant
Design OK
Compare SEE rate vs FMEA rates
negligeable
NOK
Design OK
Verify compliance (FC CAT & HAZ)
compliant
NOK (1st loop) : component re-design :
- select non SEE-sensitive components
- or implement Built-in mitigation means
Verify compliance after going through 1st loop
NOK (2nd loop) : system re-design :
- implement system SEE mitigation means

Figure 2. Proposed SEE safety analysis process

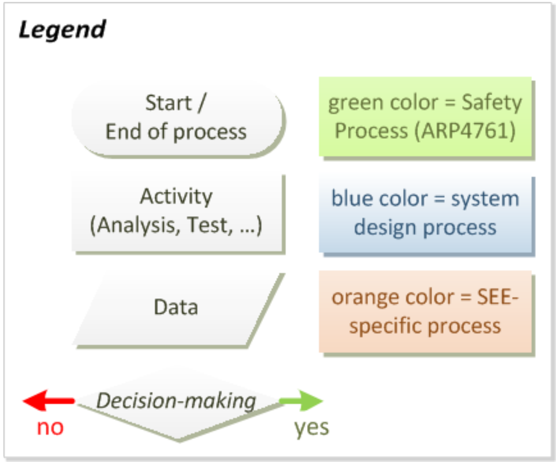


Figure 3. SEE safety process tags for the sample SSA and legend of figure 2

2.3 SYSTEM-LEVEL ANALYSIS

2.3.1 Overview

The FHA identifies FCs and associated safety objectives. The verification that the implemented system is compliant with these safety objectives is performed through the preliminary system safety assessment (PSSA) and SSA. The objective of the PSSA is to establish the system safety requirements and to determine that the proposed architecture can reasonably be expected to meet the safety objectives.

The verification against quantitative safety objectives is based on the system FTA. The FTA is also the input to the CMA that is performed for AND gates of CAT FCs, determination of the quantitative safety budgets, and determination of functional failure sets and associated DAL for each component of the system.

The PSSA FTA generally uses quantitative budgets for the system's components, which will be refined as safety objectives at equipment level. The SSA is based on PSSA FTA and uses the quantitative values obtained from the component's failure mode and effects summary (FMES) to verify the previous quantitative budgets in the FTA.

SEE-related demonstration activities are mainly performed at equipment level (see figure 2). In some cases, the SEE analysis will highlight the need for specific SEE mitigation techniques to be implemented at system level (which may also provide additional passivation means for intrinsic random failures of the components). These mitigation means must be reintegrated within the scope of SBs in the system architecture. Afterward, the verification against the safety objectives must be reassessed through a new FTA taking into account these new SBs.

The process at system level is illustrated in figure 4 below.

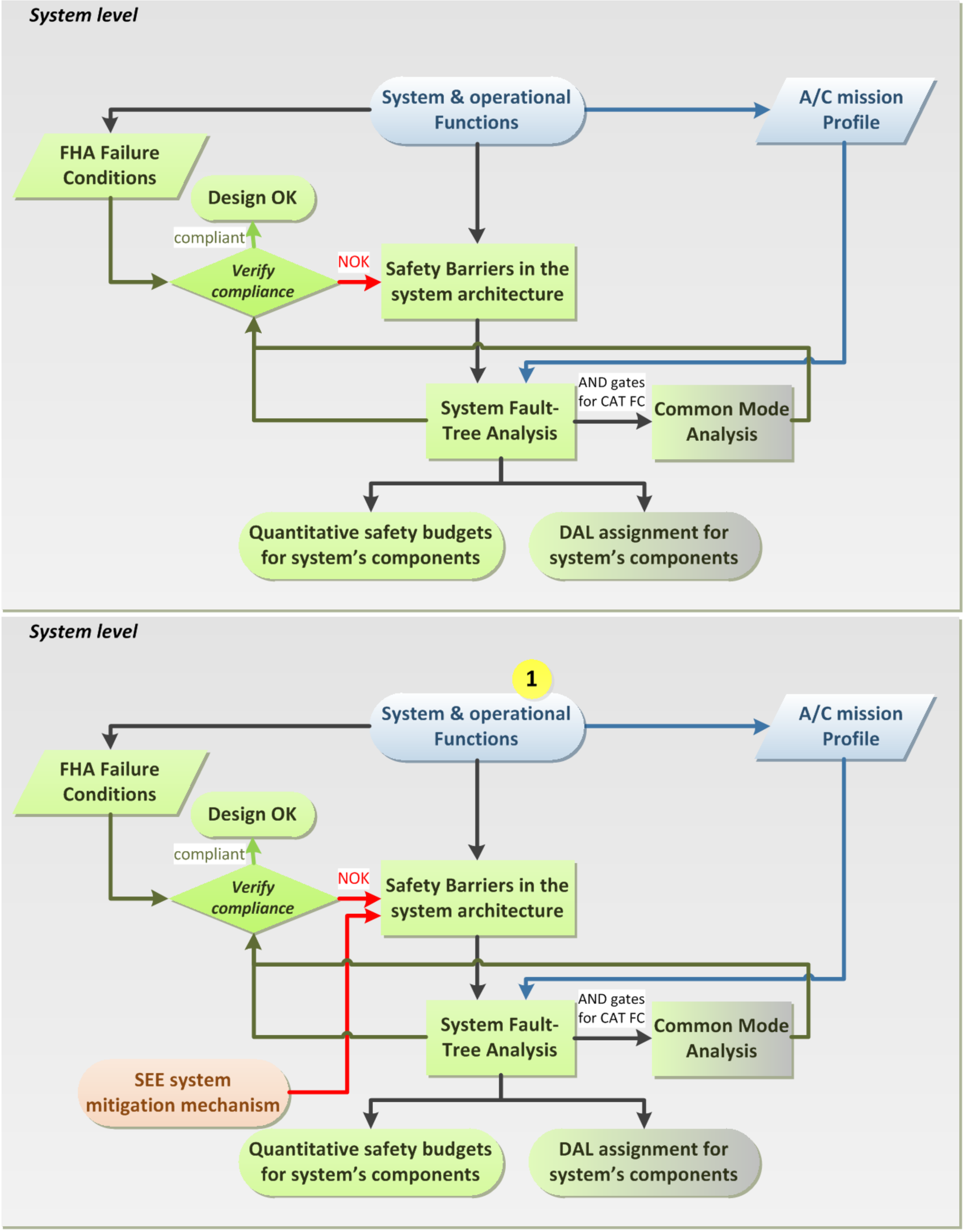

System level
System & operational Functions
A/C mission Profile
FHA Failure Conditions
Design OK
compliant
Verify compliance
NOK
Safety Barriers in the system architecture
AND gates for CAT FC
System Fault-Tree Analysis
Common Mode Analysis
Quantitative safety budgets for system's components
DAL assignment for system's components
System level
1
System & operational Functions
A/C mission Profile
FHA Failure Conditions
Design OK
compliant
Verify compliance
NOK
Safety Barriers in the system architecture
AND gates for CAT FC
System Fault-Tree Analysis
Common Mode Analysis
SEE system mitigation mechanism
Quantitative safety budgets for system's components
DAL assignment for system's components

Figure 4. Safety analysis process at system level (with/without SEE analysis)

Notes regarding the applicability of SEE analysis at system-level:

Because the effect of atmospheric radiation is one factor that could contribute to equipment loss or malfunction, SEE safety assessment is concerned only with quantitative assessments (FMEA/FMES and FTA) aiming to cover random failure effects [1].

This leads to three concerns:

1. EASA SEE Certification Memorandum (CM) [1] defines that the susceptibility to SEE should be assessed for systems or equipment capable of causing or contributing to CAT or HAZ FCs at aircraft level. However, IEC TS 62396-1 [3] considers that SEE assessment should be performed based on the DAL of the systems and with more rigor on the quantitative assessment for DAL A and DAL B systems.

The recommended criteria to select systems or equipment for which SEE safety analysis will be performed is their involvement in CAT or HAZ FCs rather than their DAL. This is for the following reasons:

- DAL levels aim to cover software and hardware systematic errors, whereas SEE results in stochastic events addressed by the system fault-tree analysis. The list of items involved in CAT or HAZ FCs is a direct outcome of the FTA.

- According to ARP4754A [5], DAL A to DAL C items may be involved in the functional failure sets of a CAT FC. A DAL C system contributing to a CAT FC will then be selected for SEE assessment with the recommended criteria (involvement in CAT FC), because it may be excluded with the DAL-based criteria.

Therefore, the criteria pointing to items involved in CAT or HAZ FCs, as determined by the FTA, is the more exhaustive and consistent with the nature of SEE events.

2. At system level, the CMA is not impacted by new SEE assessments. In fact, SEE effects due to normal atmospheric radiation levels could only contribute to random failures within a single equipment, and not concurrently affect several independent hardware equipment. Only extreme solar flare events, which produce additional neutrons within the atmosphere and thus increase the overall atmospheric neutron flux for short periods, may be susceptible to severely impact system architectural features, such as redundancy or monitoring. Therefore, CMA, which focuses on system mitigation means pertaining to common faults impairing independence mechanisms inside a system, will treat only solar flare impacts. To conclude, as recommended in reference [1], mitigation means against solar flare are implemented at an aircraft operational level and not at a system level.

3. Meanwhile, as the normal atmospheric radiation level effects (either for SEU or MBU types) are expected to be limited at one component perimeter, SEE effects that may propagate from one component to another will be passivated by safety mechanisms already implemented to cover functional effects of intrinsic random failures or errors. Therefore, no specific qualitative assessment of SEE effects propagation is required in the last update of reference [1].

2.3.2 SEE Impact on System, Operational Functions, and Mission Profile

What can be tolerated by the system, after one or several of its components has been impacted by single events, can be determined by answering the following questions about the expected system properties:

- Should the system design be tolerant to SEE?
- Should the system design be resilient to SEE?
- Is detection of the event sufficient?
- Is correction of the failure required?
- Is a preventive strategy required?

These characteristics will be passed to the equipment and component levels where they will orient toward specific families of mitigation techniques. Overestimating the needs is likely to result in overdesign with associated costs, but underestimating the needs could result in more-frequent failures than publicly announced.

Moreover, the selection of appropriate mitigation techniques is based on the operation of the device, not only in terms of reliability, but also in terms of availability, such as knowing whether the device’s operations can be interrupted.

The level of automation has an impact on the level of rigor to be applied when determining SEE error rates. When the crew is not part of the operational loop (i.e., not in the loop or on the loop), the consequences of SEE may be more severe More rigor in the determination of SEE rates should be applied, such as requiring testing to safety critical automated systems.

2.3.3 SEE System-Level Mitigation Mechanisms

The SSA requires the assessment of the SEE rate at the line replaceable unit (LRU) level. Typically, this value is the aggregate of SEE rates of all the SEE-sensitive components that are used in the LRU. At the system-level scale, the failure rates are expressed in terms of mean time between unscheduled removals (MTBUR) or mean time between failures (MTBF).

The increased complexity in the cockpit, brought in part by the significant increase of processed information, has evolved the execution of tasks from sequential to parallel. Such constructs increase the complexity of the assessment of SEE sensitivity to a point that it becomes code-dependent. Although the elemental sensitivity of the electronics remains a mandatory step, it may not provide sufficient coverage at the system level.

Another example of a system-level mitigation need can be found with built-in ECC based mitigations. Even if an ECC is implemented to correct a bit upset, it is still possible that—whereas a critical configuration bit upset is corrected—an error can propagate in the logic path. In particular, it is important to protect feedback or decision paths so that the device cannot be driven into an unintended mode prior to the correction of the upset configuration bit. To guarantee uninterrupted operation, hardware redundancy solutions are required. Moreover, the designer can add a device reset if the upset is detected in a critical configuration bit.

2.3.4 System-Level Redesign

The system level redesign may refer to the implementation of additional mitigation means not built-in at lower levels (the mitigations at equipment level are addressed in the equipment-level redesign). These mitigations are primarily architecture-based and can be based on redundancy if the penalties are acceptable (see section 2.4.3), external protection, or containment for destructive SEEs.

2.4 EQUIPMENT-LEVEL ANALYSIS

2.4.1 Overview

Each piece of equipment is described in terms of its function and materials. For CAT and HAZ FCs, an SEE safety analysis needs to be performed. SEE-sensitive components are identified as well as built-in mitigation techniques. From the aircraft mission profile description, the strategy to either fix the SEE (i.e., implement mitigation actions to remove the SEE) or continue flying without mitigating the SEE can be defined and input into the quantitative SEE safety assessment. This strategy must be defined in relation to the system safety objectives (e.g., privileging availability or integrity of the function).

Alongside the SEE safety assessment—taking into account built-in test mechanisms—the component-level FMEA is performed to verify the compliance of the equipment design with the derived safety objectives allocated to the equipment.

To verify the compliance of the design, including the SEE safety assessment results, the SEE rates resulting from the quantitative assessment are compared to the failure rates derived from the FMEA for a verified design. If the SEE rates are negligible, the design is compliant; if the SEE rates are not negligible, the compliance is verified with the top-level safety objectives resulting from the system-level quantitative safety assessment for CAT and HAZ FCs. The proposed criterion to determine whether the SEE rates are negligible is a difference of an order of magnitude, namely:

$$Error\ Rate\ (SEE) < \frac{Failure\ Rate\ (FMEA)}{10} \tag{1}$$

Note: Types of component technology used and previous “in-service” history may be taken into account to demonstrate compliance with SEE certification objectives for equipment previously used on certificated aircraft. If this is the case, this equipment may not be considered for the performance of the SEE quantitative safety assessment [1].

If there is compliance, the design is considered adequate. Otherwise, redesign needs to be considered either at system level (e.g., implementation of system-level, not-built-in mitigation techniques) or at component level (e.g., selection of component that is less SEE-sensitive or

SEE-immune, implementation of built-in mitigation techniques).

Figure 5 below illustrates the process at equipment level.

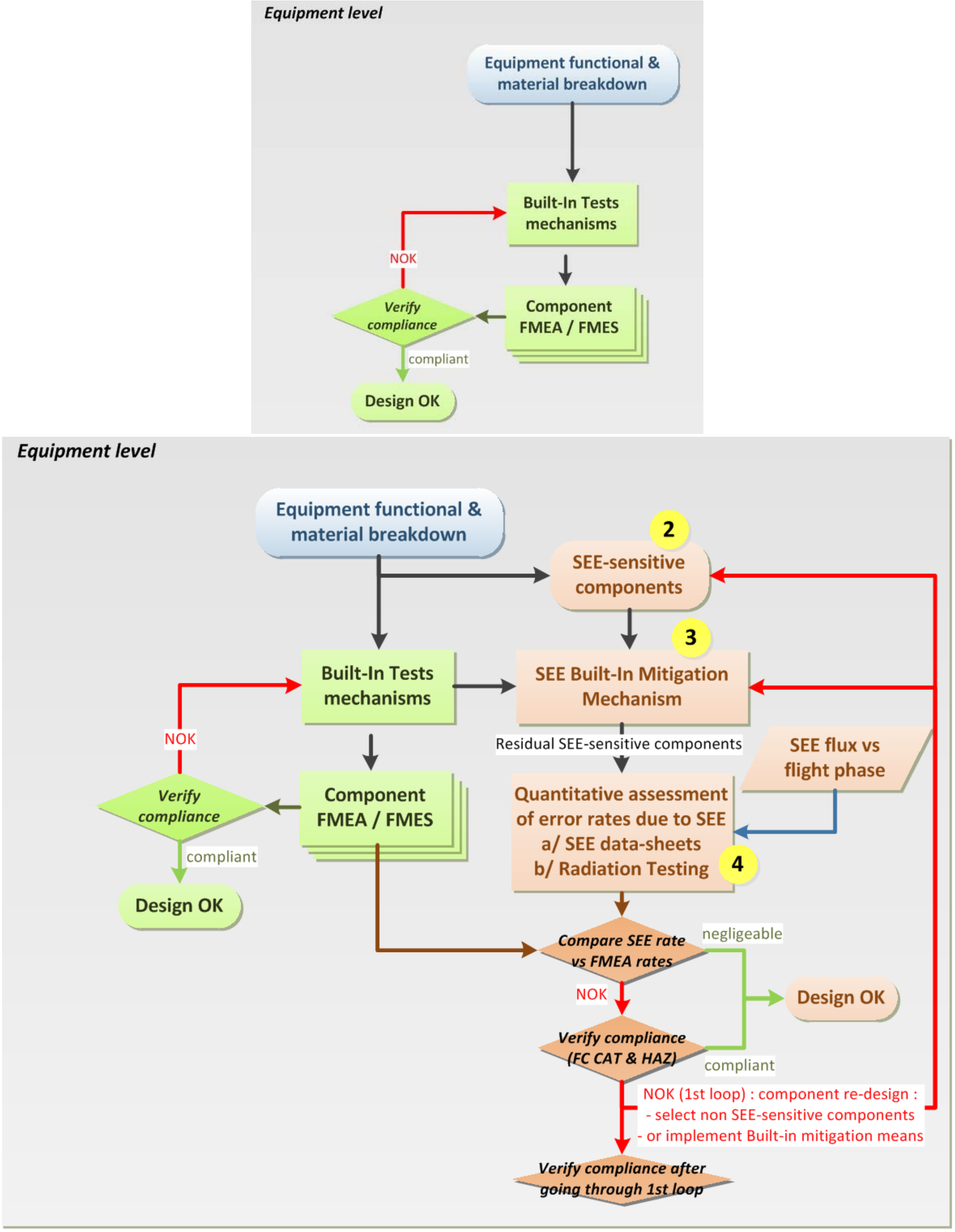

Equipment level
Equipment functional & material breakdown
Built-In Tests mechanisms
NOK
Verify compliance
Component FMEA / FMES
compliant
Design OK
Equipment level
Equipment functional & material breakdown
2
SEE-sensitive components
3
Built-In Tests mechanisms
SEE Built-In Mitigation Mechanism
NOK
Residual SEE-sensitive components
SEE flux vs flight phase
Verify compliance
Component FMEA / FMES
Quantitative assessment of error rates due to SEE
a/ SEE data-sheets
b/ Radiation Testing
4
compliant
Design OK
Compare SEE rate vs FMEA rates
negligeable
NOK
Design OK
Verify compliance (FC CAT & HAZ)
compliant
NOK (1st loop) : component re-design :
- select non SEE-sensitive components
- or implement Built-in mitigation means
Verify compliance after going through 1st loop

Figure 5. Safety analysis process at equipment level (with/without SEE analysis)

2.4.2 Determination of SEE-Sensitive Components

In a specific project, all components are listed in a bill of material (BoM) document. The scope of this research had no specific platform nor system defined in the early tasks; therefore, a methodology was proposed for a systematic approach:

- To support the most exhaustive review of all components and systems in a generic aircraft or rotorcraft platform.
- To perform a first-level filtering on the components and systems.

2.4.2.1 Equipment-Level Findings

The methodology supporting the review of all components and systems within an aircraft or rotorcraft consists of identifying the sensitivity within ATA chapters. The process for identifying a potential sensitivity to single events is defined within the filtering diagram of figure 6.

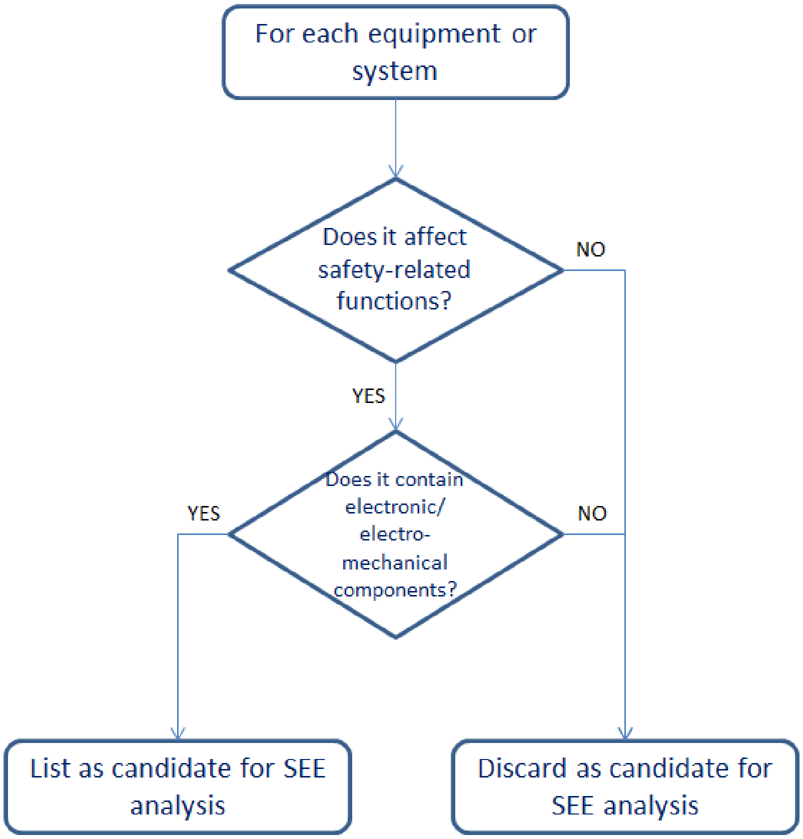

For each equipment or system
Does it affect safety-related functions?
NO
YES
Does it contain electronic/ electro-mechanical components?
YES
NO
List as candidate for SEE analysis
Discard as candidate for SEE analysis

Figure 6. SEE analysis selection criteria process

The main findings of this activity are summarized in table 3, where ATA chapters and sections hosting potentially sensitive components or systems are listed. The table also provides examples of such components and systems as well as the range of FCs (CAT, HAZ, major [MAJ], and minor [MIN]) associated with the systems in these sections.

Table 3. Synopsis of SEE-sensitive aircraft/rotorcraft systems and components

ATA chapter	Chapter name	Section	Examples	Class.
ATA 22	Auto-flight	-10 Auto-pilot -20 Speed-attitude correction -30 Auto-throttle -50 Aerodynamic load alleviating	AFGCS Flight Director Auto-throttle Gust alleviation system	Dependent on intended use; CAT CAT MIN
ATA 23	Communications	-10 Speech Communications -20 Data transmission and automatic calling -80 Integrated automatic tuning	HF radio VHF radio SELCAL HFDL RMP	Varied: MIN - MAJ
ATA 24	Electrical Power	-20 AC generation -30 DC generation -50 AC electrical load distribution -60 DC electrical load distribution	Generators Convertors Batteries Circuit breakers	Varied by system, up to MAJ and CAT for full fly-by-wire
ATA 26	Fire protection	-10 Detection	Fire Detector	Up to CAT
ATA 27	Flight controls	-10 Aileron and tab -20 Rudder/Ruddevator and tab -30 Elevator and tab -40 Horizontal stabilizer/stabilator -50 Flaps -60 Spoiler, drag devices, and variable aerodynamic fairings -70 Gust lock and damper -80 Lift augmenting	Stall warning Stick shaker Motors Actuators	CAT
ATA 30	Ice and rain protection	-50 Antennas and radomes -60 Propellers/rotors -80 Detection	Power sources	Up to CAT
ATA 31	Indicating/ recording systems	-10 Instrument and control panels -20 Independent instruments -40 Central computers -50 Central warning systems -60 Central display systems	Breakers CDS CWS CCR	Application dependent; MAJ for breakers; at least MIN
ATA 32	Landing gear	-30 Extension and retraction -40 Wheels and brakes -50 Steering -60 Position, warning, and ground safety switch	Motors Anti-skid control Actuators	Up to CAT

Table 3. Synopsis of SEE-sensitve aircraft/rotorcraft systems and components (continued)

ATA 34	Navigation	-10 Flight environment -20 Attitude and direction -30 Landing and taxiing aids -40 Independent position determining -50 Dependent position determining -60 Flight management computing	Air data computer Altimeter Pitot/Temp Speed warning Sideslip probe Gyroscopes AHRS VOR/DME receivers	Intended use dependent;
			ADF	MIN-MAJ
			ATCRBS	HAZ
			TCAS	MIN/MAJ
			Weather radar	MAJ
			TAWS	MAJ
			FMS	
ATA 42	Integrated Modular Avionics (IMA)		IMA	Dependent on hosted functions
ATA 46	Information systems	-20 Flight deck information systems	Aeronautical Databases	Varied
ATA 61	Propellers / propulsors	-20 Controlling -30 Braking	Motors, synchronizers, controls	Up to CAT
ATA 63	Main rotor drives	-20 Gearbox(es)	Accessory drives	Up to CAT
ATA 65	Tail rotor drive	-20 Gearboxes	Drives	Up to CAT
ATA 66	Rotor blade and tail pylon folding	-30 Controls and indicating	Control units	CAT
ATA 67	Rotors flight control	-10 Rotor control	Coupling and mixing unit	CAT
ATA 73	Engine fuel and control	-20 Controlling - governing -30 Indicating	Flowmeters	HAZ
			Manifold pressure instr.	MAJ
			Fuel/oil/ hydraulic pressure instr.	MAJ
ATA 77	Engine indicating	-10 Power -20 Temperature -40 Integrated engine instrument systems	Computers EICAS Displays	HAZ

AC = alternating current; AFGCS = auto-flight guidance and control system; AHRS = Attitude and Heading Reference System; ATCRBS = Air Traffic Control Radar Beacon System; CCR = central computing resource; CWS = central warning system; DC = direct current; DME = distance measuring equipment; EICAS = engine indication and crew alerting system; FMS = flight management system. HF = high frequency; HFDL = high frequency data link; RMP = radio management panel; SELCAL = selective calling; TAWS = terrain awareness and warning system; TCAS = traffic alert and collision avoidance system; VHF = very high frequency; VOR = VHF omnidirectional radio

Once the list of SEE-sensitive components is established, a more detailed analysis follows, based on the fact that not all electronic components are affected by all SEEs. It is therefore important to determine which SEE types are relevant in relation to the components in the system.

Table 4 associates the SEE types with the main functionalities of electronic components. This may help the system designer sub-select the sensitivity analysis to be performed based on the circuit functions and subsequently select appropriate mitigation techniques. This table is not exhaustive.

Table 4. Applicability of SEE to circuit types

	Non-Destructive SEE Categories						Destructive SEE Categories					
	SEU	MBU	MCU	SEFI	SET	SED	SHE	SEL	SESB	SEB	SEGR	SEDR
Memories	✓	✓	✓	✓	✓	✓	✓					
Logic (latches)	✓	✓	✓			✓	✓					
Logic (combination)				✓	✓	✓		✓				
Microprocessors	✓	✓	✓	✓			✓					
State controller				✓								
Analog or Mixed circuits					✓					✓		
Photonics					✓							
FPGA	✓	✓	✓	✓			✓	✓				✓
ASIC	✓	✓	✓	✓			✓	✓				
Power MOSFET									✓	✓	✓	✓
Power devices					✓			✓				
Converters	✓				✓			✓		✓	✓	

ASIC = application specific integrated circuit; FPGA = field programmable gate array

2.4.2.2 Challenges

The use of ATA chapters and sections in the absence of a BoM specific to a project allows a systematic and exhaustive review of all components and systems. Whereas some chapters are obviously hosting electronic components (e.g., avionics), the description of other chapters or even sections is not detailed enough to make a definite conclusion regarding the presence of electro-mechanical components (e.g., airframe group). The trend to integrate the drivers or controllers in the mechanical elements heightens this difficulty. In the end, the analysis of the BoM eliminates these uncertainties.

An SEE analysis need not be performed on all elements, but rather on the safety-critical ones. When performing the filtering process in the absence of a specific project that would indicate specific FCs, the difficulty originates from the fact that the safety criticality may be use-dependent. Current guidelines recommend performing an SEE safety analysis for systems involved in FCs of HAZ or CAT.

2.4.3 SEE Mitigation Mechanisms

2.4.3.1 Overall Trade Space

The fewer electronic components in a system, the less sensitivity to SEE achieved by construct. In assessing the need for radiation-tolerant versus radiation-hard electronic systems, the designer must consider the system-level mission requirements and their allocation to the equipment. Predicted MTBF, maintenance actions, and resets will contribute to the assessment of the best fitted mitigation technique against SEE.

All mitigation techniques generate a penalty. They are classified in three categories:

1. Speed penalty or delay
2. Area penalty or size
3. Power overhead

Speed penalty impacts the performance of the component, whether by the additional delay or by reducing the maximum achievable operating frequency. Area penalty directly translates into increased size, which ties to cost and sometimes manufacturing issues but can also result in a larger interconnection delay. Power overhead can be a consequence of a redundancy-based mitigation technique (because the number of components to be powered is multiplied); in this case, it accompanies any area penalty. Power overhead is also a direct consequence of design margins that are applied to mitigate destructive SEE. Increasing the acceptable power by a device has a cascading impact on other characteristics, such as the ability to dissipate heat. In some instances, the design margins applied to power force a replacement of the semiconductor itself.

2.4.3.2 Application of Mitigation Techniques

Mitigation techniques can be classified into three distinct groups:

1. Layout level techniques:

   - Modifications in the layout of transistors
   - Insertion of guard rings
   - Design of trench isolation

2. Circuit level techniques:

   - Use of hardened cell design
   - Design with spatial or temporal redundancy
   - Design with ECCs
   - Design margins

3. Technology changes:

   - Improvements in semiconductor materials

Layout-level techniques require the designer to control the manufacturing processes. Design margins are typically used for destructive SEE, such as SEB. The last category includes changes that are costly in terms of both the technology and manufacturing processes. The aeronautical market size is not yet sufficient to drive the cost of these improvements to an acceptable level.

Table 5 proposes a concise view of the applicability of categories of mitigation to SEE types. The table is not exhaustive but is sufficient to direct the system developer toward a family-type of mitigation to address certain SEEs.

Table 5. Most commonly used mitigation per SEE type

	Non Destructive SEE Categories						Destructive SEE Categories					
	SEU	MBU	MCU	SEFI	SET	SED	SHE	SEL	SESB	SEB	SEGR	SEDR
Board-level / current protection								X	X			
Horizontal mitigation	X		X					X	X			
Vertical mitigation								X	X			
Spatial redundancy	X				X	X	X					
Temporal redundancy	X				X	X						
Parity	X	X				X						
ECCs	X	X				X						
Scrubbing	X	X				X						
Interleaving			X									
Reset/ cycling				X				X	X			
External circuit protection										X	X	X
Design margins										X	X	X

2.4.3.3 Specific Implementations

The type of SEE and the impacts to be mitigated lead to different implementations of the same family of mitigation.

2.4.3.3.1 Protection Against Excessive Current

As shown in table 6, this mitigation will directly impact the availability of the circuit when the power is switched off. If loss of data is an issue when the power in the circuit is re-established, additional mitigation needs to be added to restore the data.

Table 6. Example implementations of protective circuitry against excessive current

SEE Type	Description of Mitigation	Cost/Penalty
SEL	Detection of excessive current in the board. The board is switched off and the current is later re-established	Loss of data
SEB	Protective circuitry external to the circuit for component with consistent response to SEB (e.g., MOSFET).	Availability
SEGR	Protective circuitry external to the circuit for component with consistent response to SEB (e.g., MOSFET).	Availability

2.4.3.3.2 Horizontal Hardening

Horizontal hardening techniques require collaborating with the manufacturer when the product is not off-the-shelf. Example techniques in table 7 carry an area penalty.

Table 7. Example implementations of horizontal hardening techniques

SEE Type	Description of Mitigation	Cost/Penalty
SEL	Guard rings	Area
MCU	Increase p-well distance	Area
MCU	Insert well-contact arrays between flip-flops or latches	Area
SET	Increase p-well distance	Area
SET	Place clock inverters adjacent to tap-cells	Area
SEU	Capacitive hardening of dynamic random access memory by inserting trench capacitors and transmission gates	Area, delay

2.4.3.3.3 Vertical Hardening

Similar to horizontal hardening, vertical hardening techniques require collaborating with the manufacturer when the product is not off-the-shelf. The example in table 8 carries a cost and performance penalty.

Table 8. Example implementation of vertical hardening technique

SEE Type	Description of Mitigation	Cost/Penalty
SEL	Insertion of silicon layer in the epitaxial	Cost, performance

2.4.3.3.4 Spatial Redundancy

Spatial redundancy provides reliability in the execution of instructions and computations because the operation is replicated and its result compared and (possibly) voted out. Therefore, this mitigation technique is best suited for computation-based applications. The examples in table 9 carry all types of penalties.

Table 9. Example implementations of mitigation using spatial redundancy

SEE Type	Description of Mitigation	Cost/Penalty
SEL	Insertion of silicon layer in the epitaxial	Cost, performance
SEU	Triple modular redundancy with single voter TMR with triple voter	Cost, area, timing, overhead
SEU	Double module redundancy with self-voting Duplication with comparison Double TMR	Cost, area, timing, overhead
SEU	Approximate logic circuit Partial logic masking	Cost, area, timing, overhead
SEU	BISER (duplicated) design for detection and correction of soft errors in latches, flip-flop, and combinatorial logic	Area
SEU	Dual interlock storage cell, heavy ion transient design, or single event resistant topology design with replicated critical storage nodes	Area
MCU	Redundancy of memories, error detection, and correction logic	Area

BISER = built-in soft error resilience; TMR = triple modular redundancy

2.4.3.3.5 Temporal Redundancy

Implementation of temporal redundancy implies a negligible or small timing penalty, which is an advantage over spatial redundancy. Temporal redundancy is well-suited for communication-based applications. Like all redundancy techniques, the examples in table 10 carry area penalty.

Table 10. Example implementations of mitigation using temporal redundancy

SEE Type	Description of Mitigation	Cost/Penalty
SET	Glitch filtering on the clock/reset trees	Area, timing
SET	Glitch protection using triple skewed clocks	Area, timing
SET	Glitch filtering on the asynchronous communication pipeline (see SEU protection)	Area
SEU	Asynchronous communications (replaces DMR on network/clocked logic)	Cost, area, overhead
SEU	BISER (with shifted output) design for detection and correction of soft errors in combinatorial logic.	Area, timing

BISER = built-in soft error resilience; DMR = double modular redundancy

2.4.3.3.6 Parity Bits

Parity bits provide error detection but no error correction, so the affected area may no longer be usable after detection. If the error detection is followed by a mechanism to recopy data, then the technique introduces a timing penalty. Table 11 provides an example in the communication domain.

Table 11. Example implementation of mitigation using parity bits

SEE Type	Description of Mitigation	Cost/Penalty
SEU	Parity bits in the handshake protocol of a synchronous communication pipeline	Overhead, timing

2.4.3.3.7 ECCs

Simple ECCs do not protect against MCU or MBU. Increasing MBU and MCU may lead to the increase in complexity of the codes to the point at which cost and noncompatibililty with memories requiring fast access become issues. Table 12 lists a simple and more complex ECC.

Table 12. Example implementations of mitigation using ECCs

SEE Type	Description of Mitigation	Cost/Penalty
SEU	Single error correction/double error detection codes	Timing
MBU	Double error correction/triple error detection codes	Timing, complexity

2.4.3.3.8 Scrubbing

Scrubbing is used for SEU/MBU in conjunction with ECCs or triple modular redundancy (TMR) to avoid an error accumulation beyond the capability of the mitigation technique.

2.4.3.3.9 Interleaving

Interleaving introduces complexity and delay in the circuit to a point at which the technique may not be compatible with access speed requirements. Table 13 lists a general interleaving example for MBU and a focused implementation targeting MCU, both carrying a time penalty.

Table 13. Example implementations of mitigation using interleaving

SEE Type	Description of Mitigation	Cost/Penalty
MBU	Interleaving	Timing, area
MCU	Interleaving focused on critical cells affecting the proper execution of instructions	Timing

2.4.3.3.10 Reset/Cycling

The circuit is no longer available during reset or power cycling. In addition, the frequency of reset/cycling should be compatible with the component (e.g., aging). As indicated in table 14, reset or power cycling is well-suited to mitigate SEL and SEFI at circuit level.

Table 14. Example implementations of mitigation using reset/power cycling

SEE Type	Description of Mitigation	Cost/Penalty
SEL	Switch off power supply for a pre-programmed time (alternative to hardening)	Availability
SEFI	Reset	Availability

2.4.3.3.11 Design Margins

The margins shown in table 15's examples are indicated in normative documents. However, despite the implementation of margins, SEB has been observed.

Table 15. Example rules for mitigation using design margins

SEE Type	Description of Mitigation	Cost/Penalty
SEB	Use of recommended derated power in the design: 50%–75% for MOSFET, 50% for insulated gate bipolar transistor (IGBT) and diodes	Cost, area
SEGR	Use of recommended derated power in the design: 50%–75% for MOSFET, 50% for IGBT and diodes	Cost, area

2.4.3.4 Effectiveness of Mitigation Techniques

The system level considerations of operational function and mission profile already direct the designer to the level of effectiveness that will be acceptable for the mitigation techniques. Tolerance to SEE indicates the capability of the equipment to recover from the SEE without exhibiting failure, whereas resilience allows for the function to continue performance in a degraded mode.

The selection of the techniques, when not imposed by the aircraft manufacturer in specification documents, depends on several factors, including:

- The prescribed or allocated failure rate (safety and reliability)
- The required detection time of events (may impact the device time performance)
- The means of detecting the event (may impact the device performance through penalties)
- The recovery time after event detection (considering sensitivity to disruption)
- The performance penalty, area penalty, and monetary cost for each of the mitigation solutions
- The overall system performance

- The implications of the mitigation implementation at system design level

Table 5 shows that the effectiveness of the mitigation is correlated with the type of SEE it is implemented against. To provide the relevant spectrum of protection, multiple mitigation techniques are likely to be required. Moreover, as for the system-level mitigation, the selection of appropriate mitigation technique(s) needs to take into account the operation of the device not only in terms of reliability but also in terms of availability, such as knowing whether the device operations can be interrupted.

2.4.4 Trade-Space and Limitations of Mitigation Techniques

As can be inferred from table 5, the solution to mitigate SEE is a combination of mitigation techniques to balance SEE-type coverage with safety objectives and penalties. The following sections recall a few commonly used combinations and tradeoffs.

2.4.4.1 Spatial Redundancy

The TMR is the most used mitigation techniqueand is highly efficient. However, its cost may limit its implementation to applications requiring high reliability. When the reliability requirements are lower, a mix of spatial redundancy and other techniques allow the penalties associated with TMR to be reduced.

Figure 7 shows a tradeoff that can be performed on the voter in a redundant architecture for which protection against voter fault is not warranted.

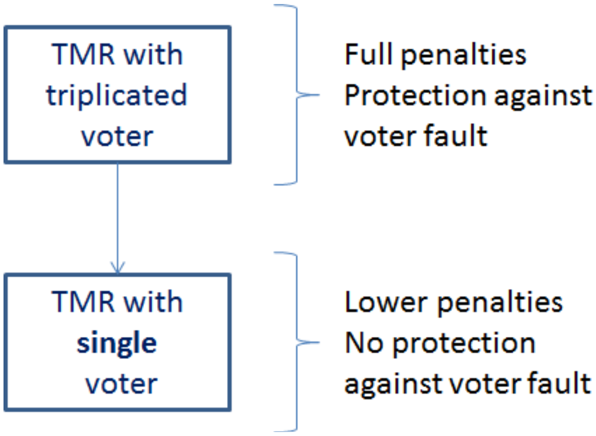

TMR with triplicated voter
Full penalties
Protection against voter fault
TMR with single voter
Lower penalties
No protection against voter fault

Figure 7. Tradeoff on TMR voter architecture

Figure 8 illustrates the tradeoff analysis that can be performed in FFs to alleviate penalties from a fully triplicated architecture. Two approaches are shown: one to reduce the redundancy from triplication to duplication and accepting to lose protection after one instance is faulty; the other to focus the protection on critical elements and not the full circuit. With the latter, the proportion of SET is going to increase and glitch filtering needs to be added.

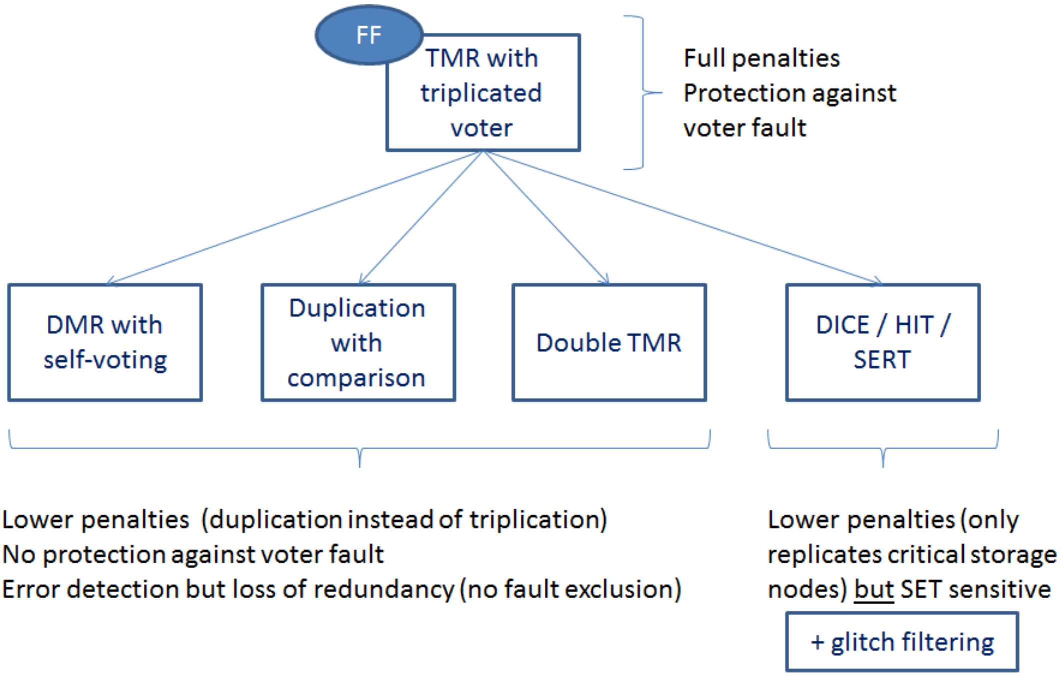

FF
TMR with triplicated voter
Full penalties
Protection against voter fault
DMR with self-voting
Duplication with comparison
Double TMR
DICE / HIT / SERT
Lower penalties (duplication instead of triplication)
No protection against voter fault
Error detection but loss of redundancy (no fault exclusion)
Lower penalties (only replicates critical storage nodes) but SET sensitive
+ glitch filtering

Figure 8. Tradeoff on spatial redundancy for FFs

Figure 9 illustrates the tradeoff that can be analyzed for logic circuit. The analysis consists of identifying parts of the circuit that can perform more than one function. It also requires access to circuit design.

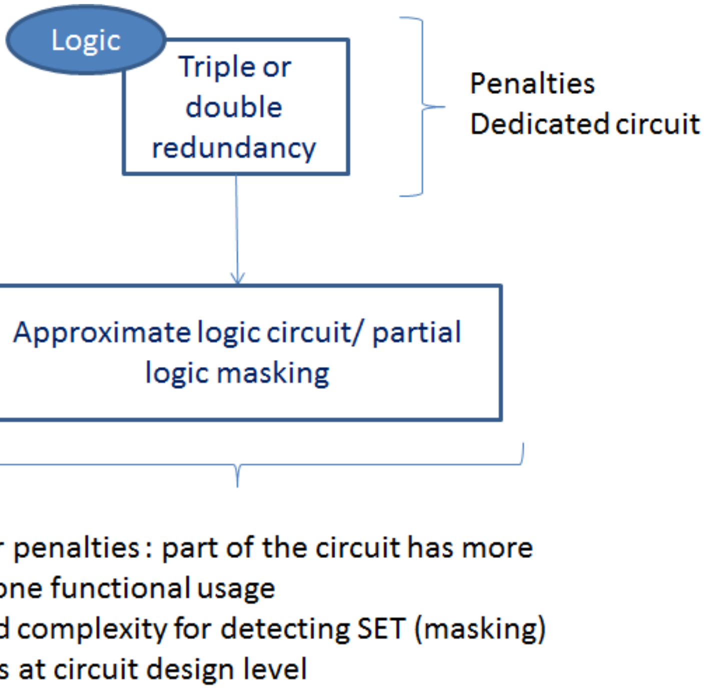

Logic
Triple or double redundancy
Penalties
Dedicated circuit
Approximate logic circuit/ partial logic masking
Lower penalties : part of the circuit has more than one functional usage
Added complexity for detecting SET (masking)
Access at circuit design level

Figure 9. Tradeoff on spatial redundancy for logic circuit

Figure 10 shows the tradeoff analysis that can be performed on asynchronous communication networks. The timing penalty is the key performance to be maintained, therefore the replacement of spatial redundancy by temporal redundancy. This introduces sensitivity in the handshake to SEU and SET, which will require additional protection.

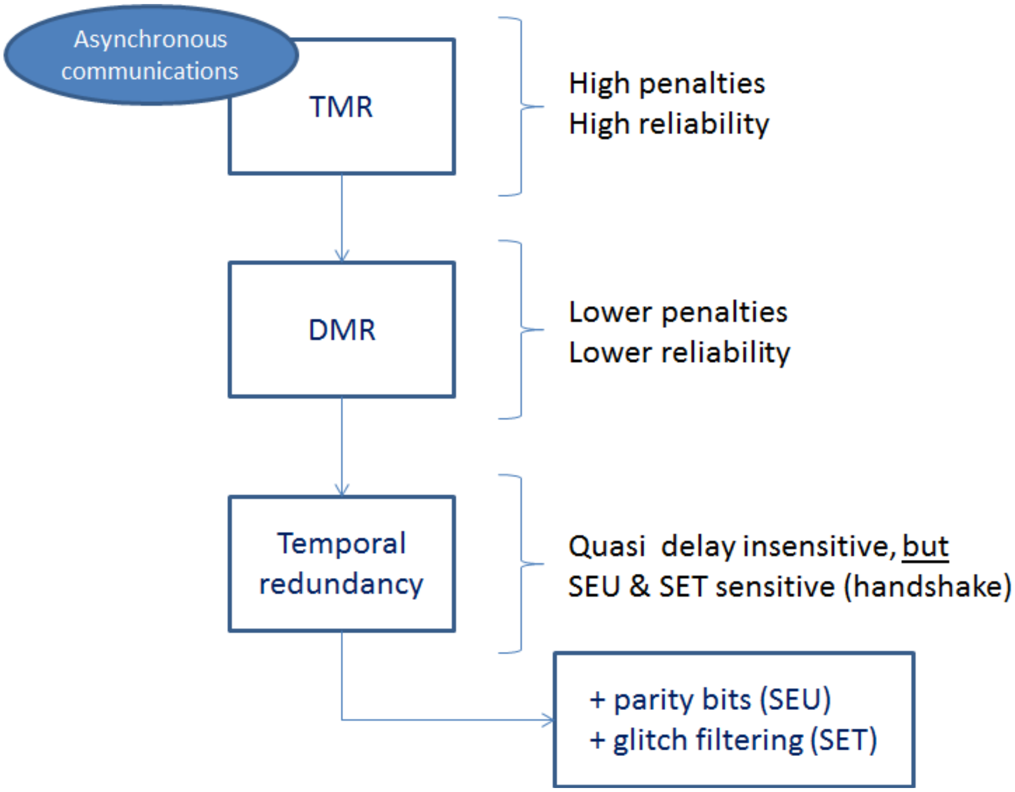


Figure 10. Tradeoff on spatial redundancy for communication network

2.4.4.2 Soft Error Protection

Figure 11 shows the tradeoff analysis that can be conducted on a memory cell to achieve a satisfactory error-correction level and extend the SEE coverage to MBU and MCU types.

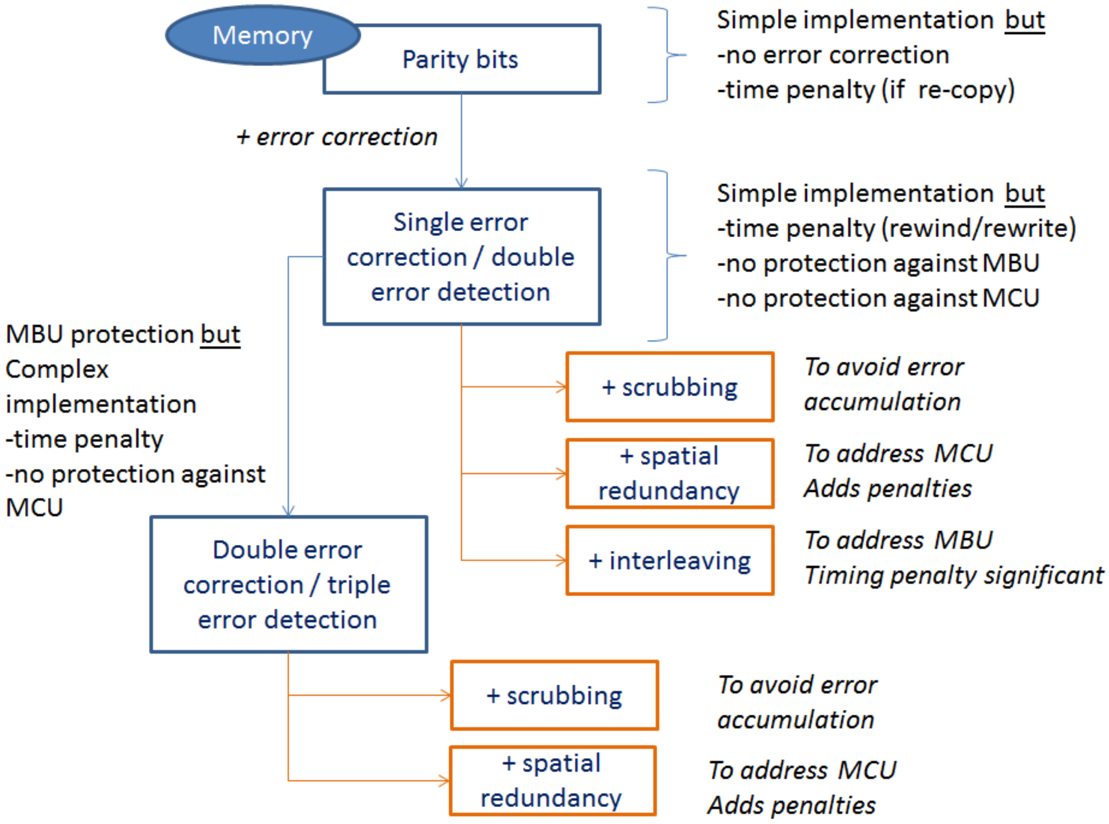

Memory
Parity bits
Simple implementation but
-no error correction
-time penalty (if re-copy)
+ error correction
Single error correction / double error detection
Simple implementation but
-time penalty (rewind/rewrite)
-no protection against MBU
-no protection against MCU
MBU protection but
Complex implementation
-time penalty
-no protection against MCU
+ scrubbing
To avoid error accumulation
+ spatial redundancy
To address MCU
Adds penalties
+ interleaving
To address MBU
Timing penalty significant
Double error correction / triple error detection
+ scrubbing
To avoid error accumulation
+ spatial redundancy
To address MCU
Adds penalties

Figure 11. Tradeoff on ECCs for memory cells

2.4.5 Determination of Radiative Flux

Predicting the atmospheric neutron flux is not an exact science. The level of fidelity in the neutron flux values need to be commensurate with the targeted use of the values. For a qualitative approach, a constant value representative of the entire flight envelope may be used. When refining the computations of SEE rates using a simulation, a tabulated model may be more appropriate. When higher fidelity is desired, actual measurements may be performed for the operating environment.

A rounded-up static conservative value for the integration neutron flux is 6,000 n/cm^2 per hour (corresponding to the integration of the neutron differential flux for energies greater than 10MeV at 40,000 ft/12.2 km and for latitude of 45º). This value is conservative by a factor of 2 compared to National Aeronautics and Space Administration (NASA) in-situ measurements performed in 1997 and by a factor of 300 when considering ground-level applications. Tabulated adjustments to this value exist for altitude and latitude from electronic components manufacturers [6]. Simplified models have been developed by aircraft manufacturers, such as The Boeing Company; more complex models have been generated by NASA Langley. The simplified model from Boeing is showing lower flux values at altitudes below 8000 ft and higher flux values at latitudes over 40º.

Manufacturers such as Xilinx launch in-situ measurement campaigns to collect real-time measurements of neutron flux at various locations (latitude, longitude, and altitude) to estimate the SEU cross-section of their devices. These data can be used to correct the atmospheric spectral model found in normative documents.

2.4.6 SEE Error Rates

To start the analysis with an initially conservative value, the SEE rate can be roughly estimated using the following equation:

$$\mathit{SEE\_rate} = \mathit{integrated\_atmospheric\_neutron\_flux} \text{ x } \mathit{SEE\_cross\_section} \qquad (2)$$

It is important not to start with an overly optimistic SEE rate value. Later, in the quantitative phase, actual SEE rates should ideally be provided by testing because analytical methods are unlikely to encompass all possible SEEs and some SEEs (e.g., SEL) are more difficult to predict.

The SEE neutron cross-section is the key parameter driving the probability that a component will interact with particles and, as a result, produce an SEE. The cross-section is a function of the feature size, which in turn depends on the technology. Section 8 and annex G of reference [3] provide guidance on the determination of a conservative cross-section per semiconductor components using data plots. The envelope of cross-section magnitude is, however, quite wide and datasheets from the manufacturers should be sought whenever possible.

A typical integrated circuit is composed of several distinct electronic components performing different functions and sensitive to different sets of SEEs. The circuit-level SEE rate will be the aggregate of SEE rates of all the SEE-sensitive semiconductor components.

2.4.6.1 Impacting Factors

An SEE rate can be affected by several factors, either connected to the semiconductor technology or circuit/equipment/system design, including the factors listed in table 16.

Table 16. Factors impacting SEE rate

Factor	Description of Impact
Feature size	All submicron integrated electronics devices are susceptible to SEEs; however, there is a correlation between the feature size and the occurrence of SEE errors. A commonly cited threshold value is approximately 90 nm.
Memory needs	Although mitigation and technology have made significant progress in reducing the rate of SEEs at the component level, the need for memory and performance has led to an increase in the number of components on a device; this increase has balanced and usually overpowered the gains on the cell.
Power consumption	The combination of lower power consumption and scaling requirements may initially result in increased bit error rates; this was the case with each SRAM generation. Even if it seems that the bit error rate has reached saturation with the deep sub-micron technology, the increase in memory density maintains the increase in system error rate.
Number of devices	If a single device has a MTBF of "Y" years and "N" devices are fielded, the aggregate MTBF is Y/N years.
DAL	The DAL indirectly impacts the determination of the SEE rates in the sense that the higher the DAL, the more rigorous the computation should be. For DAL A, testing is preferred to computations using datasheets.

2.4.6.2 Units of SEE Rates

For SEEs primarily affecting bits (e.g., SEU, MBU), the cross-section is expressed in cm^2/bit. For other SEEs, typically visible via the component response (e.g., SEL, SEFI, SET, SEB), the rate should be expressed in cm^2/device.

In the literature, some SEU rates are expressed in failure in time (FIT)/Mbit. Useful conversion factors include:

- 1 FIT = 1 failure in 10^9 device hours
- 1 cm^2/bit = $7.1E^{-17}$ FIT/Mbit[10]

Finally, at equipment level, SEE rates should be expressed in terms of MTBUR or MTBF.

[10] This factor is based on a high-energy neutron flux (E > 10MeV) of $13n/cm^2$.hr at New York City 74.

2.4.6.3 Establishing SEE Rates at Circuit Level

Once the SEE rates are established at the device level, the rate at circuit level needs to be determined. As before, the accuracy of the determination method needs to be adequate with the criticality level of the equipment.

The most conservative value for an aggregated SEE rate would be to multiply the bit (or device) level SEE rate by the number of bits (or devices). However, this computation may lead to over-specification and would not qualify for the required level of estimation method accuracy because not all bits (or devices) are created equal on an implementation.

Table 17 provides a list of the most used methods to estimate a less conservative aggregated SEE rate based on determining which bits are essential.

Table 17. Aggregated SEE rate using critical bits estimation methods

Criteria	Description of Use for Aggregated SEE Rate
Used resources	The assumption is that only those bits belonging to used resources are critical. The fraction of on-chip resources used within the LRU during the various avionics modes of operations should therefore be specified. A more precise estimation may be done via design tools (e.g., computer-assisted design or designer's netlist).
Generation of functional failure	The analysis attempts to qualify critical bits and quantify an architecture-dependent vulnerability factor based on the likelihood that a functional failure will be generated. Error injection methods belong to this analysis.
Derating factor	Another way to identify the probability that a bit flip will cause a failure is through the single event upset probability impact (SEUPI). The SEUPI is also known as the derating factor. The importance of appropriately derating the device can be understood from the following observation: on average, it takes between 10 and 100 upsets to actually generate a functional failure. In the absence of derating data, a conservative factor of 10 is therefore recommended.

2.4.6.4 Challenges

The main challenge is the quasi-absence of published SEE rates from the manufacturers. One reason is that SEE rates are probabilistic and vary with geographical location, altitude, and environmental conditions. However, even baseline information is not often accessible to the system designer. To compensate, airframe manufacturers have created simplified models that are applied across several vendors or technologies. These should be used only in the qualitative phase to provide an order of magnitude.

When considering the circuit level SEE rate for SEU in the configuration memory, an additional difficulty occurs because the rate is application dependent. Moreover, implementing the same algorithm using different methods and an Internet Protocol (IP) core may result in different system integrities.

2.4.7 Compendium of Methods to Determine SEE Error Rates

Several methods are proposed, ranging from radiation based to analytical. The choice of the method(s) should be commensurate with the factors defined in section 2.4.6.1 and the reasonableness of testing. In general, the process for determining the impact of neutron particle flux on avionics is a combination of analysis, simulation, and testing. The ratio of each is dependent on the criticality of the system.

2.4.7.1 In-the-Loop Testing

This method is recognized as the highest level of testing and is expected to provide the most accurate data for all SEE types. In this setup, the device under test (DUT)—the LRU—is subjected to a high energy neutron or proton beam. The LRU is connected to a simulator platform that supports its operation during exposure to the radiation and monitors/records its output.

2.4.7.2 LRU Irradiation

In this setup, the LRU is not operating in an active loop. The LRU is subjected to a high-energy neutron or proton beam similar to tests performed for space applications. Because the LRU is a larger size than the irradiating beam, the test objectives must include several target areas on the LRU and different width for the beam. This approach is relevant for identifying propagation of SEE in the LRU to functional interrupts, latch-up, or reboot.

2.4.7.3 Using Components Datasheet or Test Compendiums

Using existing data (from datasheets or radiation testing) for key devices in the LRU allows a static response to be built for each device for which the information is used. However, this does not take into account any dynamic propagation of SEE-induced errors inside the LRU.

This approach presupposes the setup and updating of a database, which to date remains limited. The content and status of existing databases is usually reported at the yearly Institute of Electrical and Electronics Engineers (IEEE) Radiation Effects Data Workshop (RADECS).

Irradiation data come from two types of experiments: neutron/proton testing and heavy ion testing. Most data from heavy ion testing are for space application parts and only a few are also targets considered for aircraft avionics. When applicable to aircraft avionics, the data from heavy ion testing cannot be used as they are for neutron cross-section and require a model-based transformation.

2.4.7.4 Using Generic SEE Data

This approach has the weakest technical basis because it does not use data for the specific SEE-sensitive components in an LRU, but instead uses generic SEE data. Like the previous approach, it relies on static responses to single events and ignores the dynamic response at the LRU level (e.g., error propagation). To compensate for the generality of the data, conservative margins may be added. However, the rationale for the determination of these margins could not be found in the literature. Therefore, this approach is not recommended.

2.4.7.5 Focused Laser Beam Stimulation

This approach uses a focused picosecond-pulsed laser beam to measure SEU cross-sections as a function of linear energy transfer (LET). Transfer functions convert the LET-based cross-section into SEU rates [7].

The approach can be used as a less-expensive alternative to neutron testing during both the initial estimation and monitoring phases. There are several problems with this method: it is relatively new compared to neutron testing, it uses aggregated data to indirectly obtain the SEU rate, and the data substantiating the correlation between LET cross-sections and SEU rates are quite limited.

2.4.7.6 Using In-Service Data

This approach is limited to components with SEE mitigation based on ECCs for which the erroneous bits are identified and recorded as part of in-service monitoring. The output is an SEU bit error rate that can be compared with the rates obtained from testing.

To provide actionable results, the processing of the in-service data must consider, at the very least, the following:

- The error may not be the sole result of atmospheric neutrons; other factors must be analyzed for exclusion, such as vibration transients and software issues.
- The number of SEU-susceptible bits should be known beforehand or have been reliably estimated.
- Circumstantial data supporting the characterization of the SEU must accompany the recording (e.g., altitude, latitude/longitude).
- The data storage recovery and cleanup/reset must be part of the airline’s regular maintenance program (including the fact that the process must be auditable).

2.4.7.7 Fault Injection Methods

Whereas the above methods present a direct way of testing, they might be expensive. Fault injection methods artificially flip bit(s) and can therefore be used to estimate soft error rates in a more economical manner. However, the efficiency of the method is directly related to its ability to reach all of the critical nodes (issue of accuracy of injection) and inject a fault.

2.4.7.8 Analytical Approaches

An analytical method to estimate SEE error rates is based on the generation of the individual and aggregate error rates from the netlist and, therefore, does not require an existing implementation. The main challenge of the analytical approaches is to remain efficient in the presence of mitigation (e.g., a feedback loop on the TMR voter) and, most often, layers of mitigation (e.g., TMR with scrubbing).

2.4.7.9 Considerations About Testing

Several factors influence the relevance of testing and the limitations that will accompany the test data. Table 18 summarizes the main questions a designer should consider before selecting testing as the method to obtain SEE error rates and defining a test plan.

Table 18. Factors influencing the relevance and limitations of testing

Factor	Discussion
Where to test?	When semiconductor manufacturer Xilinx tested its devices at several facilities, they discovered that, although the results were self-consistent from one visit to the next at the same facility, they yielded different cross-sections across facilities for the same part number and under the same testing conditions. The variations were as high as ±10%. The lesson learned from this observation is that manufacturers may have to use more than one facility to obtain their cross-section information or find a way to use one of their technologies as a benchmark to which others can be compared. For Xilinx, the results for the 150 nm technology are used as a gold standard for use in calibrating the results of other technologies subjected to the same beam.
How long to test?	As the hardness of semiconductor devices improves, whether through technology improvement or implementing mitigation techniques, the number of upsets occurring when subjected to the beam radiation is also reduced. As a consequence, for the same number of test hours, the accuracy of results is statistically less. Therefore, to maintain the level of statistical accuracy in the results, longer beam exposures are required.
When to test?	Only analytical methods are able to provide the designer with pre-design estimates. Depending on the qualitative results for the SEE rate, testing may not help prior to the implementation of the mitigation technique. A cost/benefit analysis can help rationalize testing at early or late stages in the design.
At what level?	There are many uncontrollable variables in SEEs, such that testing at chip level and aggregating for the number of chips might not capture the full range of effects or the real SEE rate. There is a lack of research in characterizing the correlation, or at least the trend, between an aggregated SEE rate obtained from chip-level testing and an SEE rate obtained from system or LRU level testing.
Testing or Simulating?	On commercial off-the-shelf complex integrated circuits, such as FPGAs and ASICs, the radiation hardness is difficult to estimate because of the challenge of identifying the source of the fault and in assessing the production means (i.e., separating faults from defects). The analysis of commercial FPGA components using computer models and simulations is not directly transferable to circuit level because of the intrinsic layers of protection and circuit management logic.

ASIC = application specific integrated circuit; FPGA = field programmable gate array

2.4.8 Component-Level Redesign

The component redesign may take different approaches:

- Add built-in mitigation techniques of higher level of protection (e.g., increase the level of an ECC)
- Add not built-in mitigation techniques (e.g., duplicate the circuit or the memory cells)
- Increase the level of protection of an existing, not built-in, mitigation (e.g., add a protection on the voter of a redundant circuit/device, add scrubbing to a TMR)
- Change the semiconductor component within the family (e.g., higher grade field programmable gate array [FPGA])
- Change technology (e.g., silicate-based semiconductors)

These strategies have associated costs and penalties to be balanced against programmatic (e.g., planning) and technical (e.g., design) constraints.

Of particular concern is the growing risk of MBU/MCU. The cost of ECC is rising with the complexity, such that other prevention techniques are being investigated, including semiconductor material improvement and introduction of field effect transistors (FETs) in the nanometer scale [8].

In the case of destructive SEE, such as SEBs, the choices in terms of technology are limited [9] for power components, so a system-level redesign is more likely.

3. DETAILED RESEARCH: IDENTIFICATION OF SEE-SENSITIVE AVIONICS SYSTEMS AND COMPONENTS

3.1 INTRODUCTION

The objective of this research is to identify safety critical avionics systems and components in transport aircraft and engines that may experience FCs as a result of a single event. The FCs include hazardously misleading information and other system failures.

The process for performing a safety analysis on SEE starts with the allocation of all systems and components to an SEE-sensitive or SEE-immune component list. Literature directly addresses the electronic component level, but does not associate in a systematic way, the aircraft system or component.

This section proposes a methodology that can be applied in a top-down approach not only to a list of aircraft systems and components to identify the SEE-sensitivity at the system level, but also to a BoM to identify SEE-sensitivity at the part-number level.

3.2 METHODOLOGY

The methodology supports a review of avionics systems and components as exhaustively as possible. To remain agnostic in terms of aircraft architecture and manufacturer customary bundling, the review will use ATA chapter numbering as a reference to show coverage, regardless of the aircraft make and model.

3.2.1 Overall Process

The process described in the following subsections is a generic version of the SEE safety analysis preparation phase, which results in a list of SEE-sensitive components and, by opposition, a list of SEE-immune components (see figure 12). The main differences are elicited in table 19.

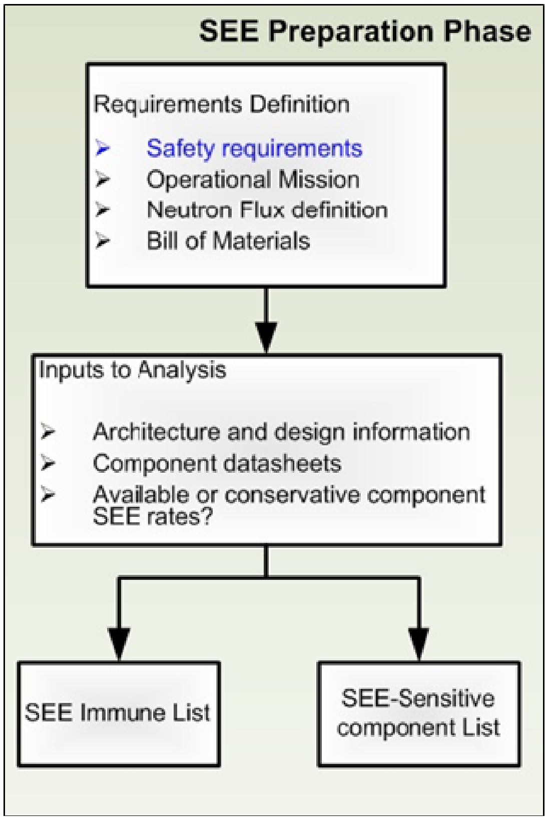


Figure 12. SEE analysis preparation phase flow diagram

Table 19. Comparison of the process with SEE safety analysis preparation phase

SEE preparation phase step	Implementation in this report
Requirements definition Safety requirements Operational mission Neutron flux definition BoM	The analysis is made outside of a particular project; therefore, safety requirements and operational mission are not available (typically customer dependent). Neutron flux definition can be defined as a maximum nominal neutron flux at any operational location by scaling the tables in annex D of IEC62396-1 [3]. BoM is replaced by the use of aircraft-agnostic ATA codes and avionics systems, and components are identified instead of part numbers.
Inputs to analysis Architecture & design info Components datasheets Available or conservative component SEE rates	The use of ATA codes replaces aircraft-specific architecture and design information. The systems and components are assigned to the SEE-sensitive list based on them typically embedding semiconductor components that are identified in the literature as SEE-sensitive.
SEE-sensitive component list	SEE-sensitive component list (aircraft-agnostic). Note that because the analysis did not make use of potentially available SEE rates for specific components, the list should be considered upper-bound.
SEE immune list	This list can be produced by referencing radiation tests performed on each component. The immunity is specific to manufacturers and part numbers; general considerations to claim immunity are included in the document in lieu of an actual list.

3.2.2 Filtering Process

From the requirement definition step to the determination of the SEE-sensitive component list, each avionics system is passed through a filtering process that determines the applicability of the analysis (and, therefore, the need to research analysis input information). The SEE analysis selection criteria process is illustrated in figure 13.

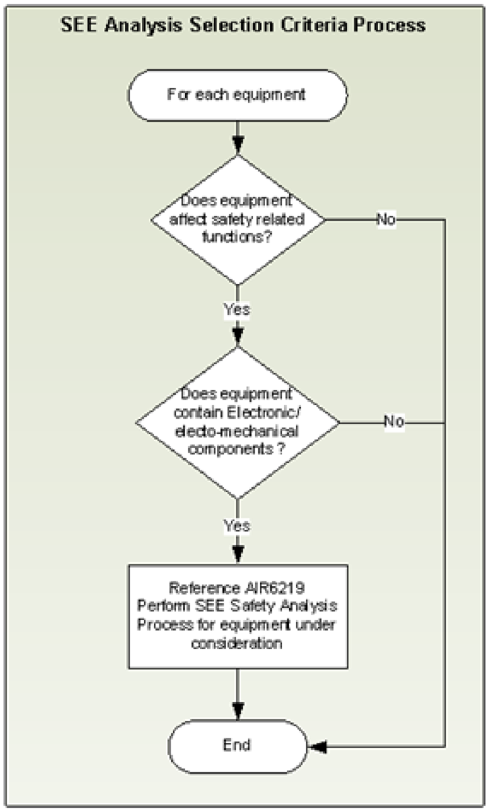

SEE Analysis Selection Criteria Process
For each equipment
Does equipment affect safety related functions?
No
Yes
Does equipment contain Electronic/ electro-mechanical components ?
No
Yes
Reference AIR6219 Perform SEE Safety Analysis Process for equipment under consideration
End

Figure 13. SEE analysis selection criteria process

3.3 APPLICATION OF METHODOLOGY TO GENERIC AIRCRAFT

This analysis is conducted on aircraft systems regardless of mitigations in place within the architecture (e.g., hardware redundancy). This will be addressed as part of the survey of mitigation techniques in section 4.

3.3.1 List of Aircraft Systems

Beginning with the list of ATA chapters from appendix A, the first filtering criteria to be applied is the determination of whether or not a system is safety critical. A quick glance through the various groups allows for coarse sorting:

- Aircraft (general) group: contains non-safety critical items, most external to the aircraft itself. This group is entirely filtered out.
- Airframe systems group: contains most of the avionics systems and will therefore play a central role in the analysis.
- Structure group: contains the aircraft’s structural elements in a strict sense. This group is entirely filtered out.
- Propeller/rotor group: contains not only the structure elements but also the units activating and driving them. Further analysis will separate the strictly structural/mechanical elements from elements containing electronic components.

- Power plant group: contains both the structural and mechanical elements and the means to control them. Further analysis is required

Applying this filter yields the list of systems in table 20.

Table 20. List of safety critical systems

ATA chapter	Chapter name
ATA 22	Auto-flight
ATA 23	Communications
ATA 24	Electrical power
ATA 26	Fire protection
ATA 27	Flight controls
ATA 30	Ice and rain protection
ATA 31	Indicating/recording system
ATA 32	Landing gear
ATA 34	Navigation
ATA 42	Integrated modular avionics
ATA 45	Diagnostic and maintenance system
ATA 46	Information systems
ATA 61	Propellers/propulsors
ATA 62	Main rotor(s)
ATA 63	Main rotor drive(s)
ATA 64	Tail rotor
ATA 65	Tail rotor drive
ATA 66	Rotor blade and tail pylon folding
ATA 67	Rotors flight control
ATA 73	Engine – fuel and control
ATA 76	Engine controls
ATA 77	Engine indicating

To refine the system selection, the extended list of ATA chapters in table 21 (ATA specification 2200), which introduces section numbers, is used. Relevant subcategories are presented in bold.

Table 21 Extended list of ATA chapters

ATA chapter	ATA chapter name	ATA section extension
ATA 22	Auto-flight	-00 General **-10 Auto-pilot** **-20 Speed-attitude correction** **-30 Auto-throttle** -40 System monitor (note 1) **-50 Aerodynamic load alleviating**
ATA 23	Communications	-00 General **-10 Speech communications** (note 2) **-15 Satcom** **-20 Data transmission and automatic calling** -30 Passenger address, entertainment, comfort -40 Interphone -50 Audio integrating -60 Static discharging -70 Audio & video monitoring **-80 Integrated automatic tuning**
ATA 24	Electrical Power	-00 General -10 Generator drive **-20 AC generation** **-30 DC generation** -40 External power **-50 Alternating current electrical load distribution** **-60 Direct current electrical load distribution**
ATA 26	Fire protection	-00 General **-10 Detection** -20 Extinguishing -30 Explosion suppression
ATA 27	Flight controls	-00 General **-10 Aileron and tab** **-20 Rudder/ruddevator and tab** **-30 Elevator and tab** **-40 Horizontal stabilizer/stabilator** **-50 Flaps** **-60 Spoiler, drag devices, and variable aerodynamic fairings** **-70 Gust lock and dampener** **-80 Lift augmenting**

Table 21 Extended list of ATA chapters (continued)

ATA chapter	ATA chapter name	ATA section extension
ATA 30	Ice and rain protection	-00 General -10 Airfoil **-20 Air intakes** -30 Pitot and static -40 Windows, windshields and doors **-50 Antennas and radomes** **-60 Propellers/rotors** -70 Water lines **-80 Detection**
ATA 31	Indicating/recording systems	-00 General **-10 Instrument and control panels** **-20 Independent instruments** -30 Recorders **-40 Central computers** (note 3) **-50 Central warning systems** **-60 Central display systems** -70 Automatic data reporting systems
ATA 32	Landing gear	-00 General -10 Main gear and doors -20 Nose gear and doors **-30 Extension and retraction** **-40 Wheels and brakes** **-50 Steering** **-60 Position, warning, and ground safety switch** -70 Supplementary gear
ATA 34	Navigation	-00 General **-10 Flight environment** **-20 Attitude and direction** **-30 Landing and taxiing aids** **-40 Independent position determining** (note 4) **-50 Dependent position determining** **-60 Flight management computing**
ATA 45	Diagnostic and maintenance systems (note 5)	-00 General **-05 through -19 CMS/aircraft general** **-20 through -44 CMS/airframe systems** **-45 Central maintenance system** **-46 through -49 CMS/airframe systems** **-50 through -59 CMS/structure** **-60 through -69 CMS/propellers** **-70 through -89 CMS/power plant**

Table 21 Extended list of ATA chapters (continued)

ATA chapter	ATA chapter name	ATA section extension
ATA 46	Information systems	-00 General -10 Airplane general information systems **-20 Flight deck information systems** -30 Maintenance information systems -40 Passenger cabin information systems -50 Miscellaneous information systems
ATA 61	Propellers/propulsors	-00 General -10 Propeller assembly **-20 Controlling** **-30 Braking** **-40 Indicating** -50 Propulsor duct
ATA 62	Main rotor(s)	-00 General -10 Rotor blades -20 Rotor head(s) -30 Rotor shaft(s)/swashplate assembly(ies) **-40 Indicating**
ATA 63	Main rotor drive(s)	-00 General **-10 Engine/gearbox couplings** **-20 Gearbox(es)** -30 Mounts, attachments **-40 Indicating**
ATA 64	Tail rotor	-00 General -10 Rotor blades -20 Rotor head **-40 Indicating**
ATA 65	Tail rotor drive	-00 General -10 Shafts **-20 Gearboxes** **-40 Indicating**
ATA 66	Rotor blade and tail pylon folding	-00 General **-10 Rotor blades** **-20 Tail pylon** **-30 Controls and indicating**
ATA 67	Rotors flight control	-00 General **-10 Rotor control** **-20 Anti-torque rotor control (yaw control)** **-30 Servo-control system**

Table 21 Extended list of ATA chapters (continued)

ATA chapter	ATA chapter name	ATA section extension
ATA 73	Engine fuel and control	-00 General -10 Distribution **-20 Controlling – governing** **-30 Indicating**
ATA 76	Engine control	-00 General **-10 Power control** **-20 Emergency shutdown**
ATA 77	Engine indicating	-00 General **-10 Power** **-20 Temperature** -30 Analyzers **-40 Integrated engine instrument systems**

Note 1: The system monitor package is not selected as safety critical because the systems it contains provide a separate or external monitoring or remote readout for maintenance purposes and are not directly related to the internal system monitoring for a system integrity/crew warning.

Note 2: The speech communications package also includes inflight telephones, which are not considered safety critical. Only the high frequency (HF), very high frequency (VHF), and ultra-high frequency (UHF) radio communication equipment is sub-selected.

Note 3: The central computers package includes non-safety critical components, such as checklists, procedures, and company regulations. The digital core avionic system is the sub-element selected for the analysis.

Note 4: The independent position determining package also includes basic instruments, such as sextants/octants, which are not selected for this analysis.

Note 5: The diagnostic and maintenance systems package (ATA 45) covers units, components, and associated systems interfacing with multiple aircraft systems and performing checkout and fault-isolation procedures using a central computer complex or standard fault isolation procedures to locate a single system or component malfunction. Because the primary use of the information is maintenance, it is not clear whether the package would qualify as safety critical for the analysis.

3.3.2 SEE-Related Inputs to Analysis

In this section, specific information related to SEE is collected to match against the list of aircraft equipment to produce the list of SEE-sensitive systems.

3.3.2.1 SEE Types

SEE is the term used to describe the interaction of neutron particles with the molecular structure of semiconductor components (e.g., with silicon). This interaction results in an electronic disturbance in the component due to the deposited energy by a single ionizing particle. The disturbance in the energy level of the molecular structure in the semiconductor can translate into a temporary or permanent change of state at the component level. This change may or may not cascade to the device and the system.

Whereas the result of SEE is the same, several types of SEE have been identified. The list of events considered for this analysis, their definition, and the type of semiconductor with which they are associated are listed in table 22.

Table 22. SEE types and effects

SEE Type	Effect	Applicability (examples)
SEU	A change of state in a memory or latch	Random Access Memory (RAM), microprocessor cache memories and registers, FPGA
MCU	Bit upsets in more than one physically adjacent bit	RAM, microprocessor cache memories and registers, FPGA
MBU	Bit upsets in more than one bit in the same logical word	RAM, microprocessor cache memories and registers, FPGA
SET	A spurious signal or voltage propagating through a circuit path during a single clock cycle	Analog and digital devices
SEFI	Corruption of the control path of a complex device so that the circuit no longer performs its function properly	Control registers in RAM, microprocessors, FPGA
SEL	Loss of gate or device function or control	Control registers in RAM, microprocessors, FPGA, Programmable Logic Device
SEB	Device destruction	High voltage components, such as MOSFET and IGBT

IGBT = insulated gate bipolar transistor

In short, all integrated circuits should be considered for SEE analysis, as well as high-voltage components (>200V) for SET and SEB.

3.3.2.2 Determination of SEE Immunity

It is possible that a semiconductor component, when interacting with high-energy neutrons, will not induce a failure as a result of an SEE. This immunity is determined via testing (direct and inferred) and is specific to the integrated circuit and semiconductor component. The acceptable testing methods to determine immunity are presented below.

Any semiconductor component that cannot be demonstrated as SEE-immune must be listed in the SEE-sensitive category.

3.3.2.2.1 Heavy Ions Testing

The immunity to SEE can be determined by subjecting the semiconductor component to heavy ions and measuring the LET. The LET is a measure of the energy that can be deposited per unit path length divided by the density; it is expressed in MeV-cm^2/mg. In the case of SEE, the interaction with high-energy neutrons generates secondary particles and recoils that act as heavy ions. In silicon, the SEE-induced highest possible LET is approximately 15MeV-cm^2/mg. Therefore, any semiconductor component tested with heavy ions and exhibiting an LET greater than the 15MeV-cm^2/mg threshold can be declared SEE-immune [10].

3.3.2.2.2 High-Energy Neutrons Testing

This is direct testing of the semiconductor component with high-energy neutrons and observing the absence of SEE.

3.3.2.2.3 Inferred Arguments and Technology-Related Rationales

Other rationales can be used to declare a component SEE immune, such as:

- A similar related part of the same technology and feature size from the same manufacturer was successfully tested using the methods in sections 3.3.2.2.1 and 3.3.2.2.2.
- Older nonvolatile memories, such as electrically erasable programmable read-only memories (EEPROMs) and flash memories with larger feature sizes, have generally been considered SEE immune.
- Advanced alternative memory technologies, such as ferro-magnetic random access memory (RAM) or magneto-resistive RAM, have, respectively, exhibited low SEU sensitivity and SEU immunity [11].

3.3.3 SEE-Sensitive Components

3.3.3.1 General Considerations

Certain classes of semiconductor components are known to be SEE sensitive. A non-exhaustive list includes:

- Memories (e.g., various types of RAM, application-specific integrated circuits (ASICs), and flash memory).
- Microprocessors.
- FPGA, programmable logic device (PLD).
- Complementary metal-oxide semiconductor (CMOS) and MOSFET.
- High-current, high-voltage semiconductors (e.g., diodes; gate-turnoff and integrated gate-commutated thyristors; and insulated gate bipolar transistor [IGBT]).

For SEU-types, the sensitivity increases with the component density and the use of lower voltages. In the deep sub-micron (DSM) feature sizes (e.g., 22–28 nm), it was observed that MBU tend to diminish as SEU increases. This is because these components are more sensitive to protons (typically generating MBU) than neutrons (generating more SEU) [12].

For SEB-types, the sensitivity is a function of the direct current (DC) voltage; it decreases with temperature and increases with altitude [13].

3.3.3.2 Impact of Functional FC Classification

The EASA CM on SEE [14] envisions recommending the performance of SEE analysis only for systems, LRUs, or items with a functional failure classification of CAT, HAZ, or MAJ. Systems, LRUs, or items with functional failure classification of MIN or no safety effect (NSE) would not need to be considered for SEE analysis.

When considering the ad-hoc correspondence between functional failure classification and DAL, this recommendation would translate into considering systems, LRUs, or items with DAL A, B, and C for SEE analysis.

In addition, according to SAE ARP-4754A [5], items with functional failure classification of MAJ (or DAL C) would not require a risk analysis, .

3.3.3.3 SEE-Sensitivity in Auto-Flight Systems (ATA 22)

The auto-pilot package (ATA 22-10) contains systems that use radio/radar signals, directional and vertical references, air data (pitot static), computed flight path data, or manually induced inputs to automatically control the flight path of the aircraft. This package includes power source devices, interlocking devices, and amplifying, computing, integrating, controlling, actuating, indicating, and warning devices that are candidates for the SEE-sensitive component list. Representative equipment is the Auto-Flight Guidance and Control System (AFGCS), which includes such equipment as autopilot (aircraft/rotorcraft), yaw damper, flight director, and autothrust/autothrottle. There is no standard minimum functional FC classification for an AFGCS because it depends on the intended use [15]. However, the highest failure classification is CAT with an equivalent DAL A.

The speed-attitude correction package (ATA 22-30) contains systems that automatically maintain safe flight conditions by correcting for effects of speed and out-of-trim conditions by such means as automatic trim, Mach trim, or speed stability and Mach feel. This package includes sensing, computing, actuating, indicating, internal monitoring, and warning devices that are candidates for the SEE-sensitive component list.

The auto-throttle package (ATA 22-30) contains systems that automatically control the position of the throttles to properly manage engine power during all phases of flight/attitude. The package includes engaging, sensing, computing, amplifying, controlling, actuating, and warning devices that are candidates for the SEE-sensitive component list. The AFGCS in reference [15] includes autothrust/autothrottle. Although there is no minimum functional failure classification, the highest level is CAT, which is associated with a DAL A.

The aerodynamic load-alleviating package (ATA 22-50) contains systems that automatically correct or provide for such factors as gust loading or upset, aerodynamic augmentation/alleviation/suppression, and ride control.

The package includes sensing, computing, actuating, indicating, internal monitoring, and warning devices that are candidates for the SEE-sensitive component list. As an example, FC classification for the stall warning system is at least MIN.

3.3.3.4 SEE-Sensitivity in Communications Systems (ATA 23)

The speech communication package (ATA 23-10) contains systems that use voice-modulated electromagnetic waves to transmit and receive messages from air-to-air or air-to-ground installations.

The package includes HF, VHF, and UHF communication equipment, which can be candidates for the SEE-sensitive component list. The functional FC classification for VHF radio is MAJ [18] whereas the FC classification for HF radio is MIN [17], which corresponds to DAL C and DAL D, respectively.

The satellite communications (Satcom) package (ATA 23-15) contains Satcom systems that can be candidates for the SEE-sensitive component list. However, Satcom equipment is not mandatory and, therefore, is not considered in this analysis.

The data transmission and automatic calling package (ATA 23-20) contains systems that present information derived from pulse-coded transmissions. Some items included in the package are a teleprinter, selective calling, and an aircraft communications addressing and reporting system (ACARS).

The SELCAL and ACARS sub-systems should be considered for the SEE-sensitive component list. The functional FC classification for SELCAL is MIN [18], which corresponds to a DAL D. Because the main use of ACARS is the oceanic and AOC link, equipment implementing a high frequency data link (HFDL) can be used for the FC classification of at least MIN [19] with ATC communications MAJ, which corresponds to DAL D/C, depending on the application.

The integrated automatic tuning package (ATA 23-80) contains systems that maintain integrated control of the operating frequencies of the communication and navigation transmitters/receivers after either a manually inserted command or preprogrammed integrated flight system command.

The package includes integrated frequency selector panels, integrated frequency display panels, and digital frequency control computers. The last item (i.e., the Radio Management Panel) can be a candidate for the SEE-sensitive component list.

3.3.3.5 SEE-Sensitivity in Electrical Power Systems (ATA 24)

The alternating current (AC) generation package (ATA 24-20) contains systems generating, regulating, controlling, and indicating AC electrical power.

The package includes inverters, AC generators/alternators, control and regulating items, and components that can be candidates for the SEE-sensitive component list (mostly SET and SEB).

The DC generation package (ATA 24-30) contains systems generating, regulating, controlling, and indicating DC electrical power. The package includes such items as generators/alternators, transformers, rectifiers, batteries, and control and regulating components, which can be candidates for the SEE-sensitive component list (mostly SET and SEB).

The AC electrical load distribution package (ATA 24-50) contains systems connecting AC power to consumer systems. The package includes such items as the AC main and secondary buses, main circuit breakers, and power system devices. The last two components can be candidates for the SEE-sensitive component list. Certain types of circuit breakers have an FC classification of MAJ [20], corresponding to a DAL C.

The DC electrical load distribution package (ATA 24-60) contains systems connecting DC power. -. The package includes items such as the DC main and secondary buses, main circuit breakers, and power system devices. The last two components can be candidates for the SEE-sensitive component list.

There is no minimum functional FC classification because it depends on the intended use. Several Technical Standard Orders (TSOs) cover systems in this package, including batteries, inverters, current generators, and DC converters. If an aircraft is full fly-by-wire, the FC classification of the electrical systems is CAT.

3.3.3.6 SEE-Sensitivity in Fire Protection Systems (ATA 26)

The detection package (ATA 26-10) covers fixed and portable systems used to sense and indicate the presence of overheating, smoke, or fire. There are several types of fire-protection systems, one of which includes power and RF components denoted as a fire-detectors-radiation sensing type. The associated TSO-C79 [21] does not provide a minimum FC classification, only the expected performance requirements. In the specific case of a dual-engine aircraft, for which an engine fire is combined with the extinction of the wrong engine, the FC classification is CAT.

3.3.3.7 SEE-Sensitivity in Flight Controls Systems (ATA 27)

The aileron and tab package (ATA 27-10) and rudder/ruddevator and tab package (ATA 27-20) contain mechanical components that control the position and movement of the ailerons/elevons and rudder/ruddevator, respectively (e.g., wheels, cables, linkages, control surfaces, and pedals). These elements can embed smart actuators, which are electronic devices. Therefore, elements in this package can be candidates for the SEE-sensitive component list.

The elevator and tab package (ATA 27-30) contains systems controlling the position and movement of the elevator/elevon and tabs. The package contains such items as the control column, stick-shaker units, automatic stall recovery devices, tab control wheels, cables, boosters, linkages, control surfaces, position indicators, and stall warning systems. The stick-shaker unit, stall recovery device, and stall warning systems may contain semiconductor components that qualify them as candidates for the SEE-sensitive component list.

The horizontal stabilizer package (ATA 27-40) contains systems controlling the position and movement of the horizontal stabilizer/canard. The package includes such items as control handle, cables, jackscrews, motors, warning systems, linkages, control surfaces, and position indicators. The motors and warning systems can be candidates for the SEE-sensitive component list.

The flaps package (ATA 27-50) contains systems controlling the position and movement of the trailing edge flaps. The package includes items such as the control handles, cables, actuators, warning systems, linkages, control surfaces, and position indicators. The actuators and warning systems can be candidates for the SEE-sensitive component list.

The spoiler, drag devices, and variable aerodynamic fairings package (ATA 27-60) contains systems controlling the position and movement of the spoilers, drag devices, and variable aerodynamic fairings. The package includes such items as the control handles, cables, warning systems, linkages, spoilers, drag devices, and position indicators. The warning systems can be candidates for the SEE-sensitive component list.

The gust lock and damper package (ATA 27-70) contains systems protecting the control surfaces from being moved by wind while the aircraft is on the ground, with the exception of a flight control boost system. Although SEEs on the ground have a lower occurrence rate by a factor of approximately 300, they do occur, Therefore, based on environment, the package cannot be disregarded for use at this stage. It is further assumed that gust lock and damper systems are active protection means and contain electronic components. Based on the above assumptions, the protection systems qualify for the SEE-sensitive component list.

The lift-augmenting package (ATA 27-80) contains systems controlling the position and movement of variable opening wing slots, leading-edge wing flaps, and other similar auxiliary devices used for increasing aerodynamic lift. The package includes such items as control handles, cables, actuators, linkages, warning systems, control surfaces, and position indicators (with the exception of training edge flaps covered in ATA 27-50). The actuators and warning systems can be candidates for the SEE-sensitive component list.

The FC classification for flight controls is CAT.

3.3.3.8 SEE-Sensitivity in Ice and Rain Protection Systems (ATA 30)

The air intake package (ATA 30-20) contains systems used to eliminate or prevent the formation of ice in or around air intakes, including the power plant cowling anti-icing. There is no integrated circuit in the system that would indicate a potential SEE-sensitivity.

The antennas and radomes package (ATA 30-50) contains systems used to eliminate or prevent the formation of ice on antennas and radomes. The power components can be candidates for the SEE-sensitive component list.

The propellers/rotors package (ATA 30-60) contains systems used to eliminate or prevent the formation of ice on propellers or rotors, excluding the rotating assembly. The power components can be candidates for the SEE-sensitive component list.

The detection package (ATA 30-80) contains systems used to detect and indicate the formation of ice. The sensory and warning components can be candidates for the SEE-sensitive component list.

The FC classification for an anti-icing system can be as high as CAT when considering severe icing conditions combined with the loss of the anti-icing function.

3.3.3.9 SEE-Sensitivity in Indicating/Recording Systems (ATA 31)

The instrument and control panels package (ATA 31-10) covers all panels, fixed or movable, with their replaceable components, such as instruments, switches, circuit breakers, fuses, and other panel accessories. The circuitry in the components makes them candidates for the SEE-sensitive component list. Certain types of circuit breakers have an FC classification of MAJ [20], corresponding to a DAL C.

The independent instruments package (ATA 31-20) contains instruments, units, and components that are not related to specific systems (e.g., inclinometers, clocks). Although not all would qualify as safety critical, they contain circuitry that can make them candidates for the SEE-sensitive component list.

The central computers package (ATA 31-40) contains systems and components used for computing data from a number of different sources without a preponderance of functions in any one system (e.g., a digital core avionic system), which can make it a candidate for the SEE-sensitive component list. There is no minimum FC classification because it depends on the intended (final) use of the data.

The central warning systems package (ATA 31-50) contains systems and components providing audible or visual warnings of conditions in unrelated systems. The package includes master warning or flight warning systems (FWSs), central instrument or caution and warning systems, tone generators, and annunciators, which can be candidates for the SEE-sensitive component list. A standard FC classification is at least MIN.

The central display systems package (ATA 31-60) contains systems and components providing a visual display of conditions in unrelated systems. The current display technology and the move towards “smart displays” make the package a candidate for the SEE-sensitive component list. There is no standard minimum FC classification because it depends on the intended use of the equipment in a specific aircraft [22].

3.3.3.10 SEE-Sensitivity in Landing Gear Systems (ATA 32)

The landing gear systems package (ATA 32) covers units and components furnishing a means of supporting the steering of aircraft on the ground or water and making it possible to retract and store the landing gear inflight. These units and components are active or in use at lower altitudes or on the ground or water, where the irradiation by neutrons is weaker by a factor of approximately 300. With the development of increased electric control of the landing gear system, the elements may remain active during all phases of flight, which would change the argument that they are less SEE-sensitive based on reduced exposure time and lower altitude.

The main gear (ATA 32-10), nose gear/tail gear, doors package (ATA 32-20), and supplementary gear—skis, float package (ATA 32-70)—contain the mechanical elements and are not considered for the SEE-sensitive component list.

The extension and retraction package (ATA 32-30) contains systems used to open/close the landing gear doors and extend/retract the landing gear. The package includes such items as actuating mechanisms, bogie trim, bungees, latches, operating controls, valves and motors, cables, wiring, and plumbing. Most of these elements can be candidates for the SEE-sensitive component list.

The wheels and brakes package (ATA 32-40) contains systems used to roll and stop the aircraft while on the ground and to stop wheel rotation after gear retraction. The package includes items such as bearings, tires, valves, de-boosters, swivel glands, anti-skid devices, pressure indicators, and plumbing. Anti-skid devices and pressure indicators can be candidates for the SEE-sensitive component list.

The steering package (ATA 32-50) contains systems controlling the direction of movement of the aircraft on the ground. The package includes such items as actuating cylinders, controls, and bogie swivel unlock. These components can be candidates for the SEE-sensitive component list.

The position, warning, and ground safety switch package (ATA 32-60) contains systems used to indicate and warn of the position of the landing gear/doors. The package includes such items as switches, relays, lights, indicators, horns, and wiring. The switches, relays, and indicators can be candidates for the SEE-sensitive component list.

The FC classification is CAT when considering the undetected loss of wheel-braking function.

3.3.3.11 SEE-Sensitivity in Navigation Systems (ATA 34)

The flight environment data package (ATA 34-10) contains systems that sense environmental conditions and use these data to influence navigation. The package includes air data computers, pitot/static systems, air temperature, rate-of-climb, airspeed, high-speed warning, altitude and altitude reporting, the altimeter correction system, air disturbance detection, and warning systems. The air data computer, air data sensors, and warning systems can be candidates for the SEE-sensitive component list. Several TSOs cover equipment in this package (e.g., C10b for altimeter, C16a for Pitot systems, C43c for temperature instruments, C46a/C101 for high speed warning, C87a for radio altitude, C88b for pressure altitude, C106 for air data computer). There is no standard minimum FC classification because it depends on the intended use.

The attitude and direction package (ATA 34-20) contains systems using magnetic or inertia forces to sense and display the direction or attitude of the aircraft. The package includes components for sensing, computing, and indicating and warning—such as magnetic compasses, vertical and directional references, magnetic heading systems, attitude director systems, symbol generators, turn and bank, rate of turn, amplifiers, indicators, and the flight director if it is not integral with the auto-pilot computation. All the elements of this package can be candidates for the SEE-sensitive component list. Several TSOs cover equipment in this package (e.g., C3e for turn and slip instruments, C4c for bank and pitch instruments, C5f/C6e for direction instruments, C7d for magnetic compass, and C201 for Attitude and Heading Reference System [AHRS]). There is no standard minimum FC classification because it depends on the intended use.

The landing and taxiing aids package (ATA 34-30) contains systems providing guidance during approach, landing, and taxiing (e.g., localizer, glide slope, instrument landing system, markers, and para-visual ground guidance system). These systems are used at lower altitudes, where the irradiation by neutrons is weaker by a factor of approximately 300. The SEE likelihood is greatly reduced but not totally eliminated, so these systems can be candidates for the SEE-sensitive component list.

The independent position-determining package (ATA 34-40) contains systems providing information to determine position independently from ground installation or orbital satellites. The package includes such items as inertial guidance systems, weather radar, Doppler, proximity warning, collision avoidance, and star tracker, which can be candidates for the SEE-sensitive component list. The FC classifications for the weather radar are MIN/MAJ, depending on the equipment class [23]. The FC classification for a Traffic Alert and Collision Avoidance System (TCAS II) is HAZ [24]. The FC classifications for a Terrain Awareness and Warning System (TAWS) are MAJ (HMI) and MIN otherwise [25], and a helicopter TAWS FC classification is MAJ [26].

The dependent position determining package (ATA 34-50) contains systems providing information to determine position, depending mainly on ground installation or orbital satellites. The package includes such items as distance measuring equipment (DME), VHF omnidirectional radio (VOR), automatic direction finder (ADF), OMEGA, LORAN, transponders, radio compass, and global navigation satellite systems, which can be candidates for the SEE-sensitive component list. The FC classification for an Air Traffic Control Radar Beacon System (ATCRBS) is MIN [27]; an ATCRBS mode select has FC classifications of MAJ for altitude and MIN otherwise [28].

The flight management computing package (ATA 34-60) contains systems combining navigational data to compute or manage the aircraft's geographical position or theoretical flight path. The package includes such items as course computers, flight-management computers, performance data computers, and associated control display units (DUs) and warning annunciators. These systems can all be candidates for the SEE-sensitive component list. The FC classifications for a flight management system (FMS) using multiple inputs is MAJ for Required Navigation Performance (RNP) ≥ 0.3 (with MIN for loss of vertical guidance function) and HAZ for RNP < 0.3 (with MIN for loss of vertical guidance function) [29]. A different TSO addresses other navigation modes (lateral navigation [LNAV]/vertical navigation [VNAV], localizer performance [LP], or localizer performance with vertical guidance [LPV]), and indicates the FC classification for standalone navigation equipment with Satellite Based Augmentation as MAJ for LNAV/VNAV, MAJ for LP/LPV (loss of function), and HAZ for LP/LPV (malfunction) [30]; we will retain a MAJ for en route navigation.

3.3.3.12 SEE-Sensitivity in Integrated Modular Avionics Systems (ATA 42)

Integrated modular avionics (IMA) systems can be candidates for the SEE-sensitive component list. TSO-C153 [31] indicates that the FC classification is dependent on the functions that will be loaded onto the IMA platform and determined via performance of a safety assessment conducted as part of the installation approval.

3.3.3.13 SEE-Sensitivity in Information Systems (ATA 46)

The flight deck information systems package (ATA 46-20) contains components furnishing a means to store, update, and retrieve digital information to support the flight deck systems, flight deck crew, and flight operations. The mass storage media is a candidate for the SEE-sensitive component list.

3.3.3.14 SEE-Sensitivity in Propellers/Propulsors (ATA 61)

The controlling package (ATA 61-20) contains systems controlling the pitch of the propeller blades. The package includes such items as governor synchronizers, switches, wiring, cables, levers, and all units and components supporting the propulsor vector drive system, such as flight deck control, drive motors, gearboxes, drive shafts, and synchronizing shafts. Electronic components are found in the synchronizers, switches, and controls and motors, which can be candidates for the SEE-sensitive component list.

The braking package (ATA 61-30) contains systems used to decrease run-down time or stop the propeller rotation during engine power-off conditions and includes brake mechanisms, levers, pulleys, cables, switches, wiring, and plumbing. Most of the items are mechanical; however, depending on implementation, brake mechanisms may include electronic components that could make them a candidate for the SEE-sensitive component list. An undetected loss of braking function can have an FC classification of CAT.

The indicating package (ATA 61-40) contains systems used to indicate operation or activation of the propeller/propulsor systems. The package includes such items as light, switches, and wiring. The switches can be candidates for the SEE-sensitive component list.

3.3.3.15 SEE-Sensitivity in Main Rotor(s) (ATA 62)

The main rotor(s) package (ATA 62) contains rotor head assemblies (ATA 62-20 and 62-30) and rotor blades (ATA 62-10), which are mainly mechanical items. Therefore, these sub-packages are not candidates for the SEE-sensitive component list.

The indicating package (ATA 62-40) contains systems used to indicate the operation of activation of the rotor systems. The package includes such items as lights, gauges, switches, and wiring. The switches can be candidates for the SEE-sensitive component list.

3.3.3.16 SEE-Sensitivity in Main Rotor Drive(s) (ATA 63)

The engine/gearbox couplings package (ATA 63-10) covers the drive shafts between engines and main gear boxes and, if applicable, clutch and free wheel. The package is mainly composed of mechanical items and is not considered for the SEE-sensitive component list. However, if microcontrollers are embedded in these elements, these microcontrollers would be on the SEE-sensitive list.

The gearboxes package (ATA 63-20) contains systems driving the rotors. The package includes the mechanical power take-off, accessory drives (but not the accessories themselves), the gearbox lubricating systems, and the rotor brakes (if integrated in the gearbox). The accessory drives can be candidates for the SEE-sensitive component list. The FC classification is CAT. If microcontrollers are embedded in the mechanical elements, then they should be included in the SEE-sensitive list.

The indicating package (ATA 63-40) contains systems used to indicate operation or activation of the rotor systems. The package includes such items as lights, gauges, switches, and wiring. The switches can be candidates for the SEE-sensitive component list.

3.3.3.17 SEE-Sensitivity in Tail Rotor (ATA 64)

The tail rotor package includes assembly that rotates in a plane nearly parallel to the symmetry plane and delivers a thrust opposing to the main rotor torque to ensure yaw control. The package includes rotor blades (ATA 64-10) and rotor head (ATA 64-20), both mechanical components not to be considered for the SEE-sensitive component list.

The indicating package (ATA 64-40) contains systems indicating operation or activation of rotor systems. The package includes items such as lights, gauges, switches, and wiring. The switches can be candidates for the SEE-sensitive component list.

3.3.3.18 SEE-Sensitivity in Tail Rotor Drive (ATA 65)

The gearboxes package (ATA 65-20) covers the intermediate and tail gearbox, which can be a candidate for the SEE-sensitive component list. The FC classification is CAT.

The indicating package (ATA 65-40) contains systems used to indicate operation or activation of the rotor systems. The package includes such items as lights, gauges, switches, and wiring. The switches can be candidates for the SEE-sensitive component list.

3.3.3.19 SEE-Sensitivity in Rotor Blade and Tail Pylon Folding (ATA 66)

The rotor blades package (ATA 66-10) contains systems ensuring rotor blade folding and spreading, including the mechanical, hydraulic, and electrical means permanently fitted on the aircraft. The nature of these means is not causing sensitivity to SEE, so the package is not a candidate for the SEE-sensitive component list.

The tail pylon package (ATA 66-20) contains systems ensuring tail pylon folding and spreading, including the mechanical, hydraulic, and electrical means permanently fitted on the aircraft. The nature of these means is not causing sensitivity to SEE, so the package is not a candidate for the SEE-sensitive component list.

The controls and indicating package (ATA 66-30) contain systems controlling the folding/spreading sequences and/or indicating the system’s operation. The control units can be candidates for the SEE-sensitive component list. The FC classification is CAT.

3.3.3.20 SEE-Sensitivity in Rotors Flight Control (ATA 67)

The rotor control package (ATA 67-10) contains systems controlling the attitude of the helicopter by the angle of attack of the rotor blades. The package includes such items as a collective pitch lever, a cyclic pitch stick, corresponding linkage and cable controls, coupling and mixing units, an artificial feel unit system, and a control position indicating system. Whereas the indicating system’s implementation is considered not to use SEE-sensitive components, the coupling and mixing units and artificial feel unit can be candidates for the SEE-sensitive component list. The FC classification for flight controls is CAT.

The yaw control package (ATA 67-20) contains systems controlling the direction of the helicopter. The package includes such items as tail rotor control pedals, associated linkage and cable controls, bell-cranks on the yaw control channel, and the control position indicating system. It is considered that the implementation of the systems does not use SEE-sensitive components.

The servo-control system package (ATA 67-30) covers the distribution from a power source to the rotor servo-control. Because the package only addresses distribution, it is not considered a candidate for the SEE-sensitive component list.

3.3.3.21 SEE-Sensitivity in Engine (fuel and control) Systems (ATA 73)

The controller-governing package (ATA 73-20) covers the main fuel control, which meters fuel to the engine and the thrust augmentor. The package includes fuel control unit components, such as hydro-mechanical or electronic fuel control, levers, actuators, cables, pulleys, linkages, sensors, and valves. The sensing and control items, when electronic, can be candidates for the SEE-sensitive component list.

The indicating package (ATA 73-30) contains systems used to indicate the flow rate, temperature, and pressure of the fuel. The package includes such items as transmitters, indicators (when not part of an integrated engine instrument system), and wiring. The first two elements can be candidates for the SEE-sensitive component list.

As an examples of equipment in this package, the FC classification for fuel flow meter is HAZ [32]: the classification for manifold pressure instrument [33] and fuel, oil, and hydraulic pressure instruments [34] is MAJ.

3.3.3.22 SEE-Sensitivity in Engine Controls Systems (ATA 76)

The engine controls systems package (ATA 76) covers components providing means to control the operation of the engine and the interconnected components for emergency shutdown. Therefore, its components—such as linkages, cables, levers, and pulleys—are mostly mechanical. The units themselves are not included. This package is not considered a candidate for the SEE-sensitive component list.

3.3.3.23 SEE-Sensitivity in Engine Indicating Systems (ATA 77)

The power package (ATA 77-10) contains items directly or indirectly indicating power or thrust, such as brake mean effective pressure, pressure-ratio, and rotations per minute. These sensors can be candidates for the SEE-sensitive component list.

The temperature package (ATA 77-20) contains items indicating temperature in the engine, such as the cylinder head and exhaust. These sensors can be candidates for the SEE-sensitive component list.

The integrated engine instrument systems package (ATA 77-40) covers systems in an integrated concept receiving several or all engine-operating parameters and transmitting them to a central processor for crew presentation. The package includes such items as DUs (e.g., engine indication and crew alerting system [EICAS]), transmitters, receivers, and computers, which can be candidates for the SEE-sensitive component list.

The FC classification for engine indicating systems is HAZ.

3.4 CONCLUSION ON SEE-SENSITIVE AVIONICS SYSTEMS AND COMPONENTS

The objective of the research was to develop a methodology to identify SEE-sensitivity in avionics systems and components. The proposed approach was, in the absence of a specific project with a BoM, to use ATA chapters to identify groups of systems and components as SEE-sensitive.

The main findings were that aircraft systems and components potentially sensitive to SEE belong in majority to the airframe system group, but components in the propeller/rotor group and power plant group need to be analyzed. All integrated circuits and high-voltage components should be considered for SEE analysis. Most of the time, the FC classification is dependent on the intended use of the function. Therefore, an integrated circuit may be mitigated differently on different avionics components.

To conclude, the proposed methodology applied to a specific BoM showing all part numbers and with identification of the associated system provides the adequate context for determining an SEE-sensitive component list. In the absence of a specific project, the ATA chapters and sections listed in table 23 provide a starting point for the identification of SEE-sensitive components on a generic aircraft/rotorcraft.

Table 23. Synopsis of SEE-sensitve aircraft/rotorcraft systems and components

ATA chapter	Chapter name	Sections	Examples	Class.
ATA 22	Auto-flight	**-10 Auto-pilot** **-20 Speed-attitude correction** **-30 Auto-throttle** **-50 Aerodynamic load alleviating**	AFGCS, Flight Director, Auto-throttle, Gust alleviation system	Dependent on intended use; CAT CAT MIN
ATA 23	Communications	**-10 Speech communications** **-20 Data transmission and automatic calling** **-80 Integrated automatic tuning**	HF radio, VHF radio, SELCAL, HFDL, RMP	Varied: MIN–MAJ
ATA 24	Electrical Power	**-20 AC generation** **-30 DC generation** **-50 AC electrical load distribution** **-60 DC electrical load distribution**	Generators, Convertors, Batteries, Circuit breakers	Varied by system, up to MAJ and CAT for full fly-by-wire
ATA 26	Fire protection	**-10 Detection**	Fire Detector	Up to CAT
ATA 27	Flight controls	**-10 Aileron and tab** **-20 Rudder/Ruddevator and tab** **-30 Elevator and tab** **-40 Horizontal stabilizer/stabilator** **-50 Flaps** **-60 Spoiler, drag devices, and variable aerodynamic fairings** **-70 Gust lock and damper** **-80 Lift augmenting**	Stall warning, Stick shaker, Motors, Actuators	CAT
ATA 30	Ice and rain protection	**-50 Antennas and radomes** **-60 Propellers/rotors** **-80 Detection**	Power sources	Up to CAT

Table 23. Synopsis of SEE-sensitve aircraft/rotorcraft systems and components (continued)

ATA chapter	Chapter name	Sections	Examples	Class.
ATA 31	Indicating/ recording systems	**-10 Instrument and control panels** **-20 Independent instruments** **-40 Central computers** **-50 Central warning systems** **-60 Central display systems**	Breakers, CDS, CWS, CCR	Application dependent; MAJ for breakers; at least MIN
ATA 32	Landing gear	**-30 Extension and retraction** **-40 Wheels and brakes** **-50 Steering** **-60 Position, warning, and ground safety switch**	Motors, Anti-skid control, Actuators	Up to CAT
ATA 34	Navigation	**-10 Flight environment** **-20 Attitude and direction** **-30 Landing and taxiing aids** **-40 Independent position determining** **-50 Dependent position determining** **-60 Flight management computing**	Air data computer, Altimeter, Pitot/Temp, Speed warning, Sideslip probe, Gyroscopes, AHRS, VOR/DME receivers, ADF, ATCRBS, TCAS, Weather radar, TAWS, FMS	Intended use dependent; MIN–MAJ HAZ MIN/MAJ MAJ MAJ
ATA 42	Integrated Modular Avionics		IMA	Dependent on hosted functions
ATA 46	Information systems	**-20 Flight deck information systems**	Aeronautical Databases	Varied
ATA 61	Propellers/ propulsors	**-20 Controlling** **-30 Braking**	Motors, synchronizers, controls	Up to CAT
ATA 63	Main rotor drive(s)	**-20 Gearbox(es)**	Accessory drives	Up to CAT
ATA 65	Tail rotor drive	**-20 Gearboxes**	Drives	Up to CAT
ATA 66	Rotor blade and tail pylon folding	**-30 Controls and indicating**	Control units	CAT
ATA 67	Rotors flight control	**-10 Rotor control**	Coupling and mixing unit	CAT

Table 23. Synopsis of SEE-sensitve aircraft/rotorcraft systems and components (continued)

ATA chapter	Chapter name	Sections	Examples	Class.
ATA 73	Engine fuel and control	**-20 Controlling - governing** **-30 Indicating**	Flowmeters, Manifold pressure instr., Fuel/Oil/ Hydraulic pressure instr.	HAZ MAJ MAJ
ATA 77	Engine indicating	**-10 Power** **-20 Temperature** **-40 Integrated engine instrument systems**	Computers, EICAS Displays	HAZ

CCR = central computing resource; CWS = central warning system

4. DETAILED RESEARCH: IDENTIFICATION OF CURRENT PRACTICES AND METHODOLOGY FOR SEE MITIGATION TECHNIQUES

4.1 INTRODUCTION

The objective of this research was to compile and present a compendium of SEE mitigation techniques applicable to aerospace applications. Mitigation techniques are often combined to benefit from their individual performance on specific aspects of the design or specific types of SEE-sensitivity. The content presents the basic techniques and most commonly used combinations.

Radiation effects are to be considered in the design of safety-critical systems' embedded electronic components. Radiation to which the electronic components are subjected consists of different particles, including electrons, neutrons, protons, helium nuclei, and heavy ions. The effects are classically divided into two groups: total ionization dose (TID) and SEE. For aircraft systems with shorter exposure times to radiation, SEEs are the focus whereas design of space systems need to address both TID and SEE.

The SEE consequences can be the destruction of the electronic component or an error state from which one can recover or not recover. The mitigation techniques for destructive SEE are more limited in nature and different than mitigation techniques for non-destructive SEE. The former is primarily based on safety margins applied at design. Non-destructive SEEs are observed as soft-errors that have been historically mitigated using redundancy approaches. These approaches are highly reliable but bear a significant cost. Therefore, other approaches have been developed that apply from the cell design to the circuit. In parallel, the semiconductor technology is evolving to integrated SEE-sensitivity considerations in the material and/or layout.

This section is organized as follows: section 4.2 provides background information on SEE types and affected electronic components. The section also indicates the high-level tradeoff considerations that impact the selection of mitigation techniques. Section 4.3 presents the overview of most commonly used mitigation techniques at cell, circuit, and system levels. Specific components are highlighted, including memory cells (the most common element in electronic systems) and FPGAs/ASICs (an example of systems). SEFIs are treated separately as potentially being built from other SEE-types and being component-specific in their manifestations. Finally, mitigation approaches to SEB and SEGR are described to reflect the techniques applied to destructive SEE in power elements.

4.2 SEE FOR ELECTRONIC SYSTEMS

4.2.1 Types of SEE

The SEEs can be classified in two categories: destructive SEE and non-destructive SEE [35].

4.2.1.1 Descriptions of SEE

4.2.1.1.1 The SEU

An SEU causes a change of state in a storage cell. The SEU affects memory devices, latches, registers, and sequential logic. Depending on the size of the deposition region and amount of charge deposited, a single event can upset more than one storage cell (i.e., the charge is collected by multiple transistors); the effect is called an MCU. For example, an MCU can be caused by a parasitic bipolar effect when a particle-hit generates a perturbation in the well potential.

4.2.1.1.2 MBU

An MBU is defined as a single event that causes more than one bit to be upset during a single measurement. During an MBU, multiple bit errors in a single word can be introduced as well as single bit errors in multiple adjacent words. The failure rate is further accelerated by reduced power supply voltage, increased clock frequency, crosstalk, and electro-migration effects.

4.2.1.1.3 SEFI

The loss of functionality (or interruption of normal operation) in complex integrated circuits due to perturbation of control registers or clocks is called an SEFI. An SEFI can generate a burst of errors or long duration loss of functionality (e.g., lockup). In general, an SEFI is not accompanied by a high current condition associated with an SEL or SESB. The functionality may be recovered either by cycling the power, resetting, or reloading a configuration register. The SEFIs are reported in flash non-volatile memories, synchronous dynamic random access memory (DRAM), SRAM FPGA, microprocessors, and microcontrollers.

4.2.1.1.4 The SET

An SET is a short (transient) impulse generated in a gate resulting in the wrong logic state at the combinatorial logic output. The wrong logic state will propagate if it appears during the active clock edge. The pulse may eventually be latched in a storage cell (e.g., a latch or FF). However, three types of masking can limit the propagation down to an error and be the basis for mitigation techniques: logic masking (with which SET affects a non-sensitized path), latch window or timing masking (with which SET affects elements outside their latching time window), and electrical masking (with which SET is attenuated by subsequent logic gates until filtered out). The pulse widths are important parameters to characterize SET impact as a function of the component feature size [36].

4.2.1.1.5 The SED

The class of SEE that describes the transient unstable state of an SRAM cell is an SED. This unstable SRAM state will eventually reach a stable state and the characterization will fall under SEU. Because the unstable state of the cell can be long enough that read instructions can be performed and soft errors generated, SEDs are separately identified. By extension, any device accessible during a transient state can be susceptible to an SED [37].

4.2.1.1.6 The SHE

An SHE is used to highlight the fact that the neutron-induced upset (e.g., SEU, MBU) is not recoverable. For example, when a particle-hit causes damage to the device substrate in addition to the flipping bit, an SHE is declared in lieu of an SEU.

4.2.1.1.7 SEL

In a CMOS, an SEL occurs when the energized particle activates one of a pair of the parasitic transistors, which combines into a circuit with large positive feedback. As a result, the circuit turns fully on and causes a short across the device until it burns up or the power is cycled. The effect of an electric short is potentially destructive and results in overheating of the structure and localized metal fusion.

An SEL exhibits a sharp increase in current resulting from turning on a parasitic PNPN[11] structure (equivalent to a thyristor). An SEL has a temperature dependency for whichthe SEL threshold LET decreases while the cross-section increases with temperature. Therefore, some components might not display SEL vulnerability during testing at room temperature, but are more likely to be affected at elevated temperatures.

4.2.1.1.8 SESB

SESBs are a subtype of SEL and, like SEL, they exhibit a high current-consuming condition in the affected device. Unlike an SEL, however, SESBs do not require a parasitic PNPN structure; SESBs can be induced in N-channel MOSFETs switching large current. When the energized particle hits near the drain, an avalanche multiplication of the charge carriers is created. The transistor is open and remains that way (the reason for the reference to a latch-up condition) until the power is cycled (when the device snaps back).

4.2.1.1.9 SEB

An SEB can cause device destruction due to a high current state in a power transistor, and the resulting failure is permanent. SEB susceptibility has been shown to decrease with increasing temperature. SEBs include burnout of power MOSFET, gate rupture, frozen bits, and noise in charge-coupled devices. An SEB can be triggered in a power MOSFET biasin the OFF-state when a heavy ion deposits enough energy to turn the device on.

4.2.1.1.10 The SEGR

The SEGR is caused by particle bombardment that creates a damaging ionization column between the gate oxide and the drain in power components. It typically results in leakage currents at the gate and drain that exceed the normal leakage current on a non-exposed device. SEGR may have destructive consequences.

[11] A PN junction is a formation of two types of semiconductors, called p-type and n-type. Semiconductor architectures are described as a combination of p-type and n-type, such as NPN or PNPN.

4.2.1.1.11 The SEDR

The SEDR has been observed in testing but not in space-flight data. Therefore, it is presently considered mostly an academic curiosity. An SEDR is identified from a small permanent jump in the core power supply current. A currently observed SEDR in an FPGA has been attributed to an antifuse-rupture.

4.2.1.2 Criteria for Determining SEE-Sensitivity

The probability of an SEE occurring depends on the amount of energy deposited on the semiconductor material. For short segments of high-energy particle tracks, the energy deposited by a single event is proportional to the chord length of the sensitive material. Therefore, the device shape and size is critical for determining the SEE-sensitivity [38] and the smaller the feature size, the higher the sensitivity to radiation. A criterion for the design of potentially sensitive semiconductor components is the amount of LET defined as the energy deposited per traversing length per material specific density and is expressed as MeV.cm^2/mg.

4.2.1.3 Synopsis of SEE-Types, Effects, and Impacted Electronic Components

Table 24 provides a summary view of the types of SEE, the visible effect, and the types of electronic components sensitive to the SEE-type [39].

Table 24. Overview of SEE

SEE type	Effect	Affected Electronics
SEU	Corruption of the information stored in a memory element	Memories, latches in logic devices
MBU	Corruption of several memory elements in a single hit	Memories, latches in logic devices
SEFI	Loss of normal operation	Complex devices with built-in state/control sections
SET	Impulse response of certain amplitude and duration	Analog and mixed-signal circuits, photonics
SED	Momentary corruption of the information stored in a bit	Combinatorial logic, latches in logic devices
SHE	Unalterable change of state in a memory element	Memories, latches in logic devices
SEL$^{(*)}$	High-current conditions	CMOS, BiCMOS devices
SESB$^{(*)}$	High-current conditions	N-channel MOSFET
SEB$^{(*)}$	Destructive burnout	Bipolar junction transistors, N-channel power MOSFET
SEGR$^{(*)}$	Rupture of gate dielectric	Power MOSFETs
SEDR$^{(*)}$	Rupture of dielectric	Non-volatile NMOS structures, FPGA, linear devices

$^{(*)}$ = potentially destructive SEE-types, BiCMOS = bi-complementary metal oxide semiconductor; NMOS = n-metal oxide semiconductor

4.2.2 Affected Electronic Components

In general, SEE susceptibility at the system level originates from susceptibilities at the component level; therefore, the SEE analysis will always start at the most elemental component. The following subsections present the most common electronic components that are used in avionics and affected by SEE. These components range from elemental semiconductors to electronic circuits of various complexities. The thematic grouping provides an agglomerated view.

An SEE occurs when the carrier's charge liberated by an ionizing particle and collected at a sensitive node of an electronic component is greater than the electric charge carrying elementary information in the component. A sensitive node is defined as one in an electronic circuit whose electrical potential can be modified by internal injection or collection of electrical charges. Sensitive elementary semiconductors include PN junctions (junctions formed from p-type and n-type semiconductor materials) and elementary metal-oxide semiconductor (MOS) transistors. At the cell level, sensitive components include gates, FFs, registers, and memory cells. Analog components using CMOS or bipolar technologies are also susceptible and include operational amplifiers (OpAmps), regulators, comparators, and oscillators.

More detailed information regarding the electronic components definition, architecture, and usage can be found in appendix H.

4.2.2.1 Elemental Sensitivity

The basic component of all electronic components is the transistor. Sensitive regions to SEE are primarily the junctions between two of the three transistor regions. There are two types of transistors: bipolar transistors with base-collector-emitter terminals and field-effect transistors with gate-source-drain terminals. All types of transistors are sensitive to SEE.

The IGBTs are sensitive to SEB and SEGR, similar to power MOSFET, because they share the parasitic NPN transistor structure. High-voltage diodes are less sensitive but not immune.

4.2.2.2 Linear and Analog Devices

These devices can hold functions such as voltage regulators and amplifiers. They all contain transistors and/or MOSFETs. Representative topologies for amplifiers include two-stage OpAmp with Miller compensation, Telescopic OpAmp, fully cascaded two-stage OpAmp, and current mirror OpAmp [40], which are all sensitive to SET. Power amplifiers are implemented with bipolar junction transistors (BJTs) and MOSFETs, which are sensitive to SEB. A voltage regulator can be implemented with resistor(s), diode(s), and a transistor, and can be complemented by an OpAmp.

4.2.2.3 Logic Element

Logic elements are built from transistors and diodes sensitive to parasitic bipolar effect, observable as SET or MCU, and resulting in potential flip of logic gates. The most used logic element types are NOT AND (NAND) gates, inverters (INVs), and comparators. When considering comparators, SEL is the primary sensitivity.

4.2.2.4 Memories

Memories are classified into volatile and non-volatile types. Volatile memory is associated with RAM, which comes in three types: SRAM, DRAM, and phase-changed random access memory (PRAM). The basic storage element in SRAM is an FF, or a latch, implemented using bipolar transistors, an inverter, NOT OR (NOR), or NAND gates. The most common architecture of an SRAM cell encompasses six transistors (6T-SRAM). A DRAM cell is formed using a transistor-capacitor pair.

Content addressable memory (CAM) is used for high-speed searching applications (e.g., database engines) and built from SRAM.

Non-volatile memory types include read-only memory (ROM), flash, and EEPROM. The ROM is quickly becoming obsolete. Flash memories are built from logic NAND or NOR gates. These memories can also be built from MOSFETs or floating-gate transistors.

4.2.2.5 Power MOSFET

N-channel MOSFETs contain parasitic NPN transistor structures and are susceptible to SEGR and SEB. For power MOSFETs, technology plays a significant role in the level of SEB sensitivity; silicon-based n-channel MOSFETs are more sensitive than silicon-carbide-based MOSFETs and p-channel MOSFETs are practically immune.

The vulnerability is associated with the possibility that neutron radiation turns on the parasitic transistor. There is little published literature on the impact of SEE on power MOSFETs. However, these components are increasingly present in avionics because of the development of fly-by-wire and the trend toward a more electric aircraft, whereas the sensitivity is directly connected to an increase in operational voltages.

4.2.2.6 Power Devices

These devices include switches and regulators (e.g., the step-down switching regulator, the low dropout regulator, and the switching regulator) and are sensitive to SET and SEL because of their use of transistors.

4.2.2.7 Converters

Analog-to-digital converters (ADCs) and digital-to-analog converters (DACs) contain at least one comparator, which makes them sensitive to SEL. When they integrate registers and clocked gate elements, the associated sensitivity to SEU and SET carries over.

AC-DC converters use MOSFETs or BJT and can be sensitive to SEL, SEGR, SET, and SEB.

4.2.2.8 Application Specific Integrated Circuit (ASIC)

An ASIC is an integrated circuit designed for a specific application; it contains microprocessor(s) and memory block. Because of their composition, they are sensitive to SEU in registers and memory cells.

4.2.2.9 FPGA

The FPGAs can be manufactured as SRAM, Flash and antifuse. Although FPGAs are hardware logic devices, they are sensitive to radiation because of their internal electrical architecture that makes extensive use of logic gates and memory elements. A keen knowledge of the FPGA device is required to select the appropriate part number.

The SEE-sensitivity to SEL and SEU of FPGA has different sources:

- For SRAM-FPGAs, the hardware configurations are realized by the internal SRAM elements, which are SEE-sensitive.
- For Flash-FPGAs and Antifuse-FPGAs, the hardware configuration is realized by non-volatile hardware elements, but these components use volatile memory to save temporal status information during the transient phases in the clock cycle.

Antifuse-FPGAs are implemented with TMR on memory elements and a voting scheme. These are highly reliable and specially designed with aerospace applications and a radiation environment in mind; however, they are expensive, face restrictions from import/export regulations, and cannot be reprogrammable.

4.2.2.10 Summary Technology Table

Extensive testing of several key electronic components has been performed to characterize SEE-sensitivity [41–43]. Table 25 gives a non-exhaustive overview of electronic components associated with the most commonly used technology in avionics systems and their SEE-susceptibility.

Table 25. Overview of SEE-sensitive electronic components

Component type	Technology	Primary SEE-Sensitivity
250V n-type power MOSFET	Trench	SEB
200V n-type power MOSFET	VDMOS	SEGR
Positive low drop-out voltage regulator	Bipolar	SET
Dual Hi-Speed/Low Power Op Amplifier	Bipolar	SET
Comparator	BiCMOS	SEL
N-channel DMOS switch	CMOS	SET
Step down switching regulator	BiCMOS	-N/A
Step down switching regulator	Bipolar	SET
Low dropout regulator	BiCMOS	SET
Switching regulator	CMOS	SEL
Type-A MOSFET	Polysilicon	SEB, SEGR
IGBT	Silicon	SEB, SEGR
8-bit signal conditioning ADC	Bipolar	SEL-immune
12-bit Successive Approximate Register ADC	CMOS	SEL
12-bit ADC	XFCB	SEL-immune
14-bit ADC	CMOS	SEL
DAC	BiCMOS	SEL
4 Gb NAND	CMOS (73nm)	SEL, SEU, SEFI
8 Gb NAND	CMOS (50nm)	SEU, SEFI
16 Gb NAND	CMOS (42nm)	SEU, SEFI
4 Gb NAND Flash	CMOS	SEFI
Dual ASICs	CMOS	High current event
DC-DC converter	Bipolar/MOS	SEB, SEGR
Triple channel DC-DC converter	Hybrid	SEL, SEGR, SEB
FPGA	Antifuse	SEL, SEU
FPGA	CMOS	SEL, SEU
Microprocessor	CMOS	SEFI
DSP	CMOS	SEFI
EEPROM	CMOS	SEFI
DRAM	CMOS	SEFI

BiCMOS = bi-complementary metal oxide semiconductor

4.2.3 Application of Mitigation Technique(s)

4.2.3.1 Tradeoff Between Hardware and Software

In general, a system implemented using software can be potentially affected by SEE based on its use of the electronic components described in section 4.2.2. Conversely, a mechanical/hardware system is immune to SEE. Therefore, a first step in assessing radiation-tolerant or radiation-hard electronic systems is to categorize the functionalities of these systems into the ones that can temporarily be affected by radiation in a soft-error manner and the ones that cannot fail during the whole mission lifetime. The former can be implemented with software, but the latter should extensively use hardware systems.

Whereas the tradeoff analysis between software and hardware might be clearer for space systems, it is more complex for aircraft systems. This is true regarding both destructive and non-destructive SEE based on the shorter expected lifetime of the electronic components.

4.2.3.2 Penalties Generated by Mitigation Techniques

Mitigation techniques generate three types of penalties:

1. Speed penalty or delay
2. Area penalty or size
3. Power overhead

Speed penalty impacts the performance of the component, whether by the additional delay or by reducing the maximum achievable operating frequency. Area penalty directly translates into increased size that ties to cost and sometimes manufacturing issues, but it can also result in a larger interconnection delay.

Power overhead can be a consequence of a redundancy-based mitigation technique because the number of components to be powered is multiplied; in this case, it accompanies any area penalty. Power overhead is also a direct consequence of design margins that are applied to mitigate destructive SEE. Increasing the acceptable power by a device has a cascading impact on other characteristics, such as its ability to dissipate heat. In some instances, the design margins applied to power force a replacement of the semiconductor itself.

4.3 MITIGATION TECHNIQUES

Mitigation techniques can be classified into three distinct groups:

1. Layout level techniques: layout transistors, guard rings, and trench isolation.
2. Circuit level techniques: hardened cell design, modular redundancy (double and triple), and ECCs.

3. Expensive technology changes: the improvements on semiconductor materials (see section 4.3.3.9.1) are costly in terms of both the technology and manufacturing processes. The aeronautical market size is not sufficient to drive the cost of these improvements to an acceptable level.

This research focuses on the first two groups. Another classification scheme for mitigation techniques separates preventive techniques (e.g., cell design and circuit layout) from corrective techniques (e.g., ECCs).

4.3.1 Radiation Hardening

This approach is favored by space electronics, for which the mission lifetime requirements are more demanding than for the aerospace industry and is often referred to as either radiation hardened by process (RHBP) or radiation hardened by design (RHBD). Because RHBP dedicated processes for space are no longer affordable for a single industry, some approaches are likely to be common between both industries for the very high-tolerance levels. As a consequence of RHBP affordability and because the RHBD techniques carry penalties, RHBD components are said to be radiation tolerant and not truly radiation hardened.

The type of technique depends on the electronic component technology, intended use, and SEE-type [39]. The process for radiation hardening is illustrated in figure 14.

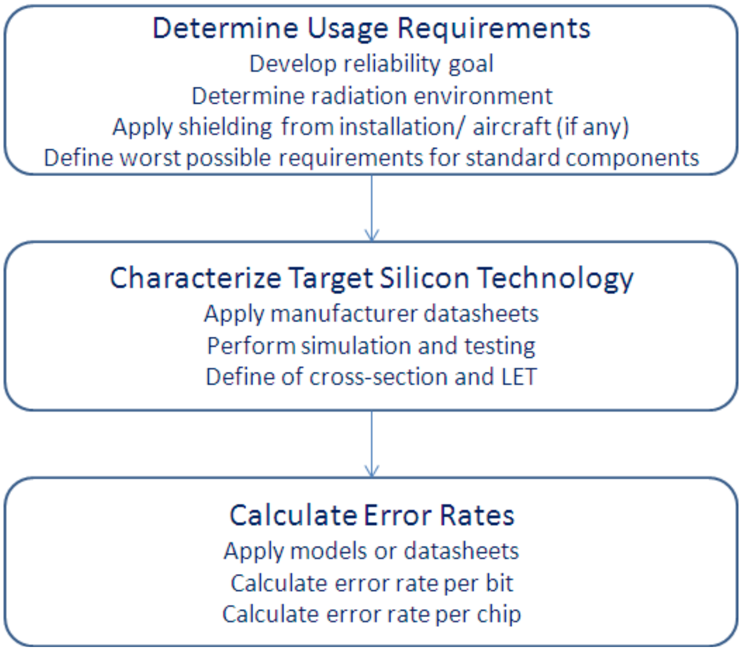

Determine Usage Requirements
Develop reliability goal
Determine radiation environment
Apply shielding from installation/ aircraft (if any)
Define worst possible requirements for standard components
Characterize Target Silicon Technology
Apply manufacturer datasheets
Perform simulation and testing
Define of cross-section and LET
Calculate Error Rates
Apply models or datasheets
Calculate error rate per bit
Calculate error rate per chip

Figure 14. SEU hardening approach

4.3.1.1 Layout-Based Hardening Mitigations for SEL

The SEL mitigation techniques can be classified into three main groups: board-level current detection, horizontal mitigation, and vertical mitigation.

4.3.1.1.1 Board-Level Current Detection

The board-level current detection technique uses board-level current sensors to detect the excessive current resulting from the latch-up. The power supply of the affected device is switched off and later re-established . However, the logical state in which the circuit was prior to the SEL is typically lost and cannot be recovered.

4.3.1.1.2 Horizontal Mitigation

Horizontal mitigation is implemented by using guard rings that break the parasitic bipolar transistor structure. This mitigation is effective but carries a significant area penalty.

4.3.1.1.3 Vertical Mitigation

Vertical mitigation is implemented by introducing a silicon layer in the thickness of the epitaxial layer and reducing the resistivity of the well. These modifications are costly and may impact the circuit performance (e.g., breakdown voltage).

4.3.1.2 Layout-Based Hardening Mitigations for MCU and SET

An MCU is caused by charge sharing and parasitic bipolar effects; its rate depends on the cell distance and well-contact density. In addition, the parasitic bipolar effect influences the probability of occurrence of an SEU and the pulse width of an SET. To reduce the sensitivity, a horizontal mitigation approach can be used, whereby each potential target transistor is implanted on different p-well regions or is separated by at least 1.1μm. Latest tests show that the MCU rates can be significantly reduced by inserting well-contact arrays between FF at supply and ground rails or between latches [44].

Using the same principles, the circuit layout can be adapted to limit the bipolar effects generating the SET carrying damaging pulse width distributions. Research suggests that placing clock inverters adjacent to tap-cells (<5μm) [44] as an SET on a clock tree may simultaneously flip several storage cells, which in turn is more likely to affect proper chip operation.

4.3.1.3 Capacitive Hardening

Other (proprietary) techniques propose capacitive hardening, either via trench capacitors (e.g., embedded DRAM cells) to minimize the area penalty or via transmission gates that cut-off the feedback during write cycles to reduce the speed penalty.

4.3.1.4 Glitch Filtering

Glitch filtering can be used on clock/reset trees. Implementations include filters enhanced with weak keepers on the output node to prevent a floating state, as shown in figure 15.

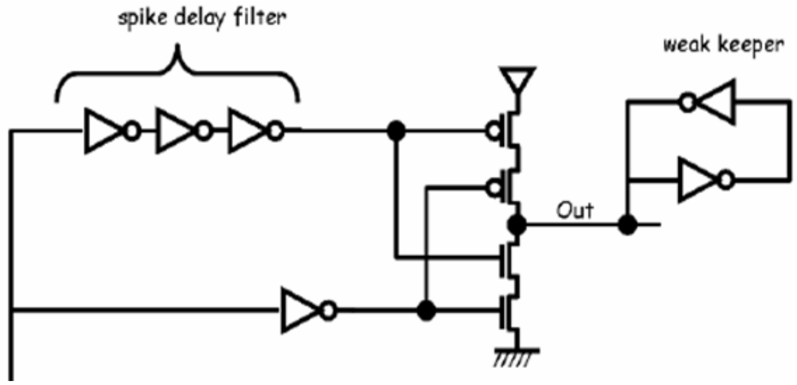


Figure 15. Glitch filtering implementation

4.3.1.5 Issues With Hardening: Impact of Requirement Capture

The primary risk is running into a design that is too expensive or complex with respect to the process or design. This issue can be triggered at an early stage in the project when requirements are captured:

- If the requirements are unclear, the radiation analysis might be incomplete; in a worst case scenario, the radiation analysis might be completely overlooked.
- Uncertainty typically leads to over-conservatism in the design.
- The system design may become unfeasible or no longer affordable.

4.3.2 Redundancy Mitigations for SEU and SET

Redundancy techniques are the most widely used. They are highly efficient but very costly and should be reserved for situations for which high reliability is targeted. A lower level of redundancy can be combined with other techniques to reduce the penalties while accommodating the desired level of reliability.

4.3.2.1 Exact Spatial Hardware Redundancy

The most common mitigation techniques are the double modular redundancy (DMR) and TMR:

- TMR with single voter: when no hardened library is available, TMR is applied to the standard FFs of the commercial library. Each of the FFs receives the input data at the same time and their output is majority-voted (see figure 16). The area penalty on the FFs exceeds a factor of 3 but costs little in combinatorial logic (compared to the factor of 2 penalty on area and speed for hardened library). However, the implementation fails in case of a faulty voter.

- TMR with triple voting logic: to mitigate a faulty voter, also known as full TMR. Each of the three voters receives outputs from all three memories. The penalties of full TMR are higher than TMR with single voter.

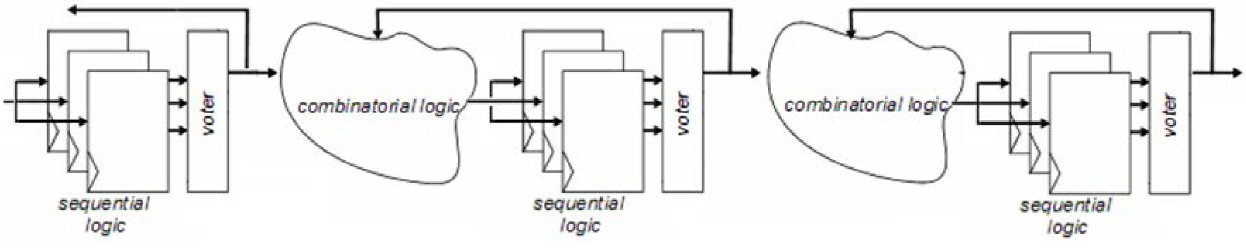


Figure 16. TMR with single voter

To mitigate a glitch, TMR can be complemented by other techniques: For example, TMR with a triple skewed clock. This is where the skewed clocks allow latching an SET—at most—in one of the three FFs, as shown in figure 17. The majority voter on the output of the FFs therefore remains at the correct value.

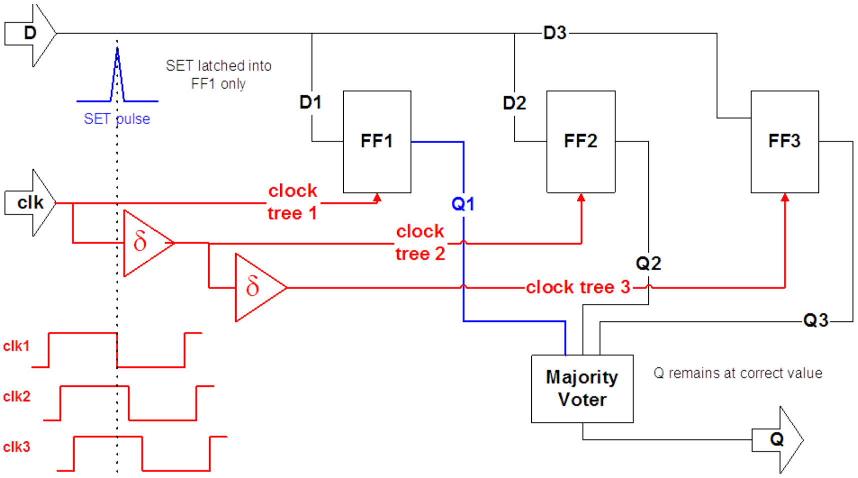


Figure 17. Skewed TMR implementation

When there is a need to reduce the TMR-induced overhead while still complying with reliability requirements, DMR with self-voting, duplication with comparison (DWC), or double-triple modular redundancy (DTMR) techniques can be used.

4.3.2.2 Approximate Logic Circuits

To address the significant area of overhead from hardware redundancy (see section 4.3.2.4.1), partial logic masking can be achieved by implementing hardware redundancy with only a partial replication of the logic. To further reduce the performance penalty, other approaches include the use of implications [45] or approximate logic circuits [46].

An approximate logic circuit is a circuit that performs a closely related function with respect to the original circuit, such that it can be used for error detection or error masking on the overlapping functions. It is different from a replicated or triplicated circuit used in DMR and TMR, respectively, for which exact copies of the original circuit are used. The error-detection and error-correction schemas found in DMR/TMR/DTMR are, however, reproducible using approximate logic circuits.

4.3.2.3 Temporal Redundancy

This mitigation technique is particularly useful to mitigate SEU sensitivity of asynchronous networks-on-chip and can replace spatial redundancy such as DMR (see section 4.3.2.1). Between the limitation of clock scaling on DSM technologies and the need for high frequencies, circuit design has evolved from global clocking to globally asynchronous locally synchronous implementations, for which locally clocked logic is interconnected through asynchronous communications. This asynchronous logic is quasi delay insensitive (QDI) for delay-variation sources, such as process, voltage, temperature, or crosstalk; it is, however, sensitive to bit flips within the logic, especially when they result in the corruption of the handshake of the asynchronous pipeline (observable as a corrupted data value but also as a handshake protocol deadlock). To increase the robustness of the asynchronous pipeline, fault-tolerant mechanisms are applied to the delay-insensitive code to go beyond synchronous design techniques, such as parity bits or glitch filtering [47].

Temporal redundancy consists of encoding the current data token with its previous value by using a higher order delay-insensitive code.

Asynchronous QDI data links are implemented with pipelines built with asynchronous registers (using SEU and SET-sensitive C-elements) and completion detectors (SET-sensitive). When these data links are implemented with 1-of-n encoding, an SEE (SEU or SET) can affect the always-excited state of registers in the pipeline differently, depending on its timing (e.g., by generating new data from the spacer held in the register or clearing the data in the register). The results can be valid corrupted data (VCD) when the data generated by the SEE have valid 1-of-n encoding or invalid corrupted data (ICD) created by an SEU or unexpected spacer/unexpected data created by an SET during the delayed Ack. When QDI encodings are implemented using m-of-n pipelines (*m*>1), the SEE-sensitivity is most reduced (i.e., the SEE is no longer able to create or clear data in a register if the data are not already switching because there are at least m-bits between the spacer and the data encodings and the completion detection circuit needs at least m inputs to switch). Compared to the 1-of-n pipeline, an SEU will no longer be able to cause a VCD during the data delay, but rather incomplete data (ID), and the only time a VCD can be generated is during the data skew, which can be prevented by ensuring at design that the data skew window is small.

The application of temporal redundancy allows one to address the remaining sensitivity of m-of-n pipelines to ICD. A temporally redundant delay-insensitive code communication system starts with a regular delay-insensitive 1-of-n encoding that is converted into a temporally redundant 2-of-n+1 encoding. The encoding is then transmitted along a QDI data link to the receiver, where it is decoded and eventually corrected using a double-check scheme.

The temporal redundancy scheme in this section is designed to provide a multi-bit correction on the receiver side of a QDI data link while keeping the communication pipeline throughput close to the original 1-of-n encoding. This scheme does not add any token to the communication link and is therefore relevant for communication-based designs. Any spatial redundancy scheme carries a delay penalty and is designed to prevent errors in the result of computation or logical operations by replicating them. Therefore, in general, computation-based designs are better suited to spatial redundancy, whereas temporal redundancy should be favored for communication-based designs.

4.3.2.4 Issues With Redundancy Techniques

4.3.2.4.1 Area and Speed Penalties

Hardware redundancy naturally increases the complexity by adding to the number of cells and nodes, translating into area and speed penalties such that TMR/DMR or hardened cells are larger and slower than soft FF. Area overhead for DMR/DWC is 100% and 200% for TMR.

4.3.2.4.2 Impact of Hardware Redundancy in the ASIC Design Flow

When designing the ASIC with tools, it can generate inefficiencies, such as increased runtime, but can also fight timing optimization options and even make the design tool crash. Moreover, when using synthesis tools with sequential logic optimization, registers can be modified because these tools were designed to remove redundancy.

4.3.2.4.3 Impact in the Verification Process

The TMR impacts the verification processes and affects the testability in scan testing mode. Indeed, defects in redundant structures do not appear in TMR simulation, even when only two of the three flows are correct. Recommendations include performing the verification of the proper implementation of the TMR protection at the NETLIST level (parsing), using formal verification tools, implementing fault simulation and injection, and performing ground radiation testing.

4.3.3 Protection of Memory Blocks

The mitigation techniques in this section apply to SRAM blocks. Traditionally, memory cells have been satisfactorily protected by corrective techniques.

4.3.3.1 Parity Bits

Parity bits have been employed for a long time within the computer industry. When an error is detected, the pipeline is flushed, the instruction queue is cleared, and execution restarts from the last committed instruction or there is a complete reload/reboot by the hardware state machine or software (see figure 18). However, unless redundant data are available elsewhere in the system, the restart/reboot usually results in the loss of data; in this scenario, parity provides error detection but does not support it.

Duplicated memories can be implemented using cache (duplicates in external memory) or locally duplicated memories.

Parity does not generate timing penalty unless an error is detected and the data need to be copied from the replica before the processing can continue.

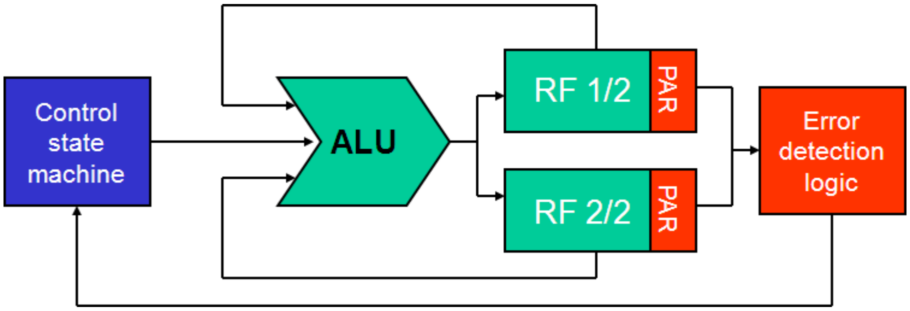


Figure 18. Parity bit implementation for memory cell

ALU = arithmetic logic unit; RF = reference frame; and PAR = parity

4.3.3.2 Built-in Soft Error Resilience

Built-in Soft Error Resilience (BISER) is an architecture-aware circuit design technique for correcting soft errors in latches, FF, and combinatorial logic [48].

In latches (or FF), the output of redundant latches is fed to a comparator with weak keeper, as shown in figure 19. Any error in either latch will result in a situation in which the output will not agree in the C-element and the error will not be propagated further, but the correct value stored in the keeper during normal operations will be retained.

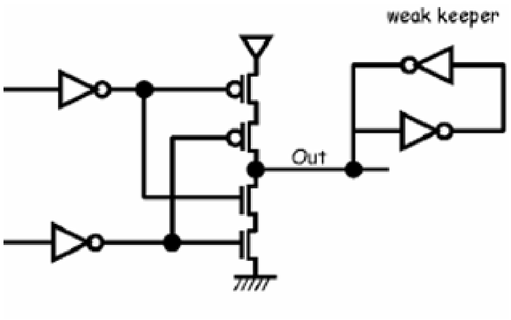


Figure 19. The BISER architecture for FF

Protection of combinatorial logic is based on error correction using duplication (duplicated combinatorial logic) fed to each of the duplicated latches connected to the C-element (see previous paragraph). To avoid the penalty area from duplicated logic and to take advantage of the fact that soft errors in combinatorial logic manifest as glitches, its output can be time-shifted so that the direct output can be fed to one latch and the time-shifted output to the other.

4.3.3.3 Dual Interlocked Storage Cell, Heavy Ion Transient, and Single Event Resistant Topology

The dual interlock storage cell (DICE) mitigation technique belongs to spatial redundancy type, but, contrary to TMR, it replicates only critical storage nodes (latch/FF) and uses feedback to recover the correct value after an upset (see figure 20). Similar techniques used to design SEU-tolerant cells include the heavy ion transient (HIT) technique [49], shown in figure 21, and the single event resistant topology (SERT) technique [50].

Note that the use within logic gates of the DICE latch in clocked storage cells results in the dominance of SET in the circuit. To further increase the robustness of SET, DICE can be combined with delay filtering (to filter out transients) to address both SEU and SET sensitivity [51] at the input signal.

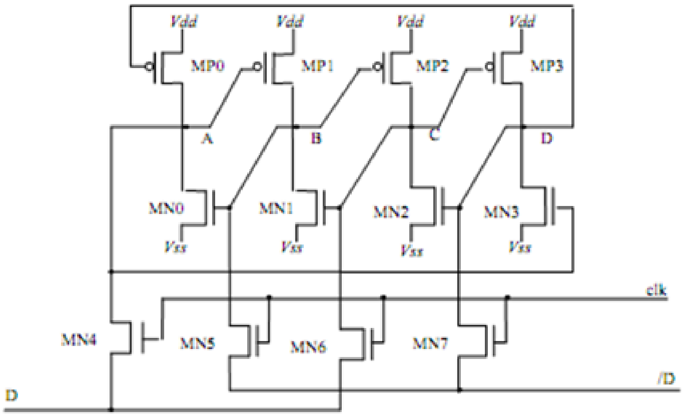


Figure 20. DICE implementation

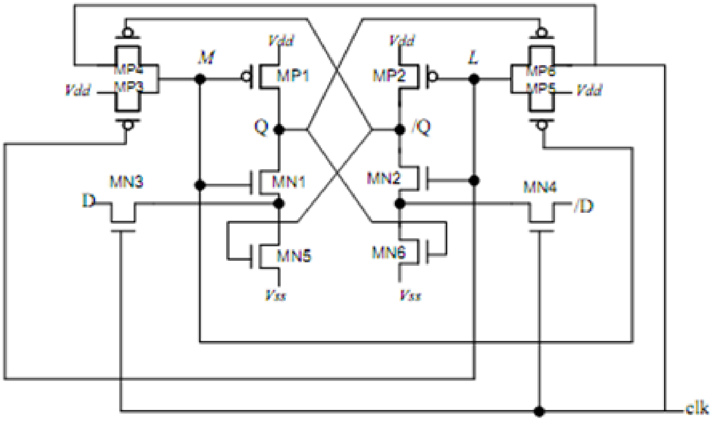


Figure 21. HIT cell implementation

4.3.3.4 The ECC and Error Detection and Correction

The ECC and error detection and correction (EDAC) mitigation techniques use hamming codes to correct single bit flips per word and require scrubbing to prevent error accumulation, as shown in figure 22. The control state machine rewrites the corrected data. There is a timing penalty associated with EDAC as the processing starts on uncorrected data and needs to be aborted with the pipeline rewind in case of error. Note that redundancy (of memories and EDAC logic) is necessary to protect against SEL and that a simple ECC/EDAC circuit cannot mitigate an MCU.

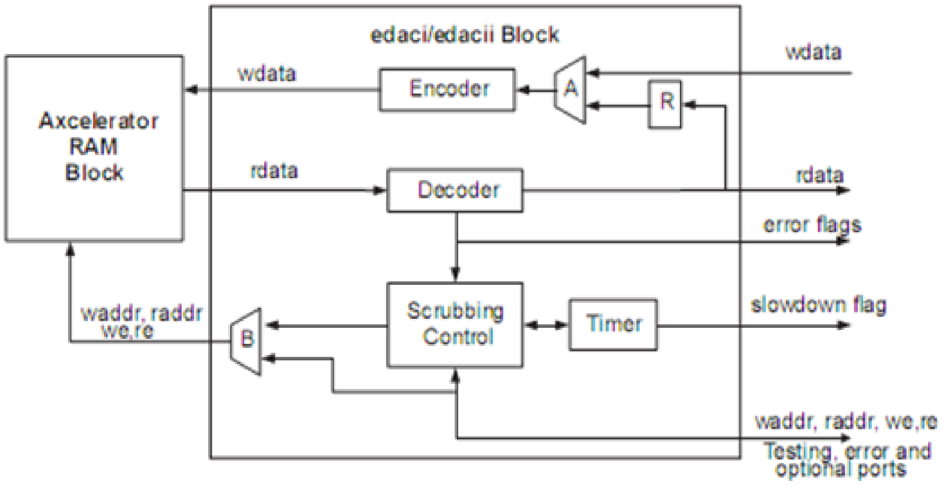


Figure 22. EDAC implementation

Finally, ECC is traditionally limited to the protection of the main memory and memory caches with access speed slower, by a factor of 10, or higher (consistent with the timing penalty incurred with the ECC) than other caches.

4.3.3.4.1 Advanced ECC to Protect Against MBU

Advanced ECC—such as double error correction, triple error correction, or error-locality-aware coding—have been shown to be effective against MBU in SRAM. The drawback is the significant area overhead due to the check-word generation and computational complexity. The latter even prohibits the use of these ECCs for extremely fast CAM/RAM arrays operating at clock speed.

Interleaving is the most commonly used technique to protect SRAM cells against MBUs. Interleaving encompasses the creation of logical check-words from physically dispersed locations in the memory array, forcing MBUs to appear as multiple single bit errors instead of a single multiple-bit error. It uses powerful ECCs, so it is not applicable to fast CAM/RAM arrays.

4.3.3.5 Scrubbing

Data scrubbing is an error-correction technique based on a background task that periodically inspects the memory for errors and then corrects them using a copy of the data.

Periodic scrubbing is recommended to reduce the multi-bit error rate in caches. Because scrubbing reuses information that is replicated in higher levels of memory, it can be applied only to cache hierarchies and not to in-core memory arrays.

4.3.3.6 Interleaving to Protect Against MBU

The vulnerability-based interleaving (VBI) mitigation technique interleaves individual bit cells based on their probability of affecting instruction execution. With VBI, the position of certain bit lines (columns of a memory array) are rearranged in the stored word because important bit lines are usually adjacent, which is a cause of the MBU-vulnerability of a memory array. Added resiliency of the design is created by physically dispersing critical bit lines and protecting only the bit lines with selective parity. Because of the use of parity, which does not offer error correction, this technique does not need ECC protection.

In a typical information layout of an instruction queue, bits cover characteristics, such as validity, issuance, location in memory, instruction operands, and predicted branch location. Not all these bits, if corrupted, will impact the correct execution of the instruction (e.g., validity and issuance are more critical to the proper execution than the instruction location in memory). The VBI method ensures more critical bits are spread throughout the word to minimize the probability that an MBU affects more than one of them [52].

4.3.3.7 Spatial Redundancy

The memory can be tripled (i.e., TMR). Scrubbing is also required in the background using the spare port of a dual-port memory. This technique bears a huge area overhead and, additionally, remains inefficient against configuration upsets.

Another implementation of spatial redundancy of data includes the inclusion of four extra transistors in the SRAM cell to prevent any change in value caused by an SEU [53]. This implementation has a significant area penalty due to well-to-well spacing requirements and a power penalty because it changes the source voltage.

4.3.3.8 Temporal Redundancy

The temporal redundancy mitigation technique is implemented by inserting a resistor in the most effective place in the circuit. Specific proposals point to the use of poly-silicon resistors that delay the transient, so that it decays substantially before the SEU. This proposal runs into the issue of a complex manufacturing process: the process control problem of laying a large resistance, sensitivity of poly-silicon to doping concentration, and poly-silicon structure and grain sizes that are sensitive to thermal processing steps [54].

4.3.3.9 Other Memory Cell Design Approaches

With the growing probability of errors in more than one bit, the cost (brought about by the combination effects from changes in area, speed, and power) of ECCs to protect the entire memory cell is rising. Therefore, mitigation and/or prevention techniques different from hardware redundancy (DICE being the most often used) can be adjunct. Some of the techniques below can be found in the category of hardened cell design (see “hardening” in section 4.3.1).

4.3.3.9.1 Semiconductor Material Improvement

Improvements focusing on the transistor itself include finding better doping profiles or using silicon on insulator (SOI) devices with a thinner silicon layer. However, the manufacturing process is more complex, the yield is lower, and the substrate is more expansive, which limits the manufacturing of SOI chips.

4.3.3.9.2 Introducing FET Components

Scaling in bulk CMOS and MOSFET technology increases the sensitivity to SEE. To reduce the sensitivity, replacement of bulk devices by double gate FinFET structures is currently the most promising approach in the nanometer scale. FinFET technology has its roots in the 1990s when DARPA searched for a potential successor to the planar transistor; the FinFET technology refers to multi-gate thin-body MOSFET. Several topologies of double gate FinFET constituting a 6-transistor SRAM cell have been compared. A 6T-SRAM is described by its basic parts: pull-up (PU), pull-down (PD), and pass-gate (PG). A double gate FinFET consists of a front gate and aback gate. The topologies are obtained from the way the back gate PU, PD, and PG are biased. Of the 10 topologies tested, the results concluded that the flexible pass-gate (FLEX-PG, figure 23) and the flexible pass-gate-opposite storage node (FLEX-OSN, figure 24) are the best topologies [55].

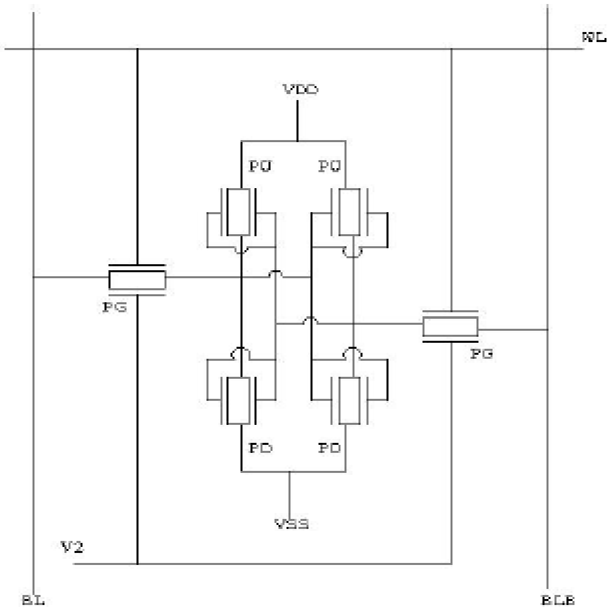


Figure 23. Double gate finFET FLEX-PG topology

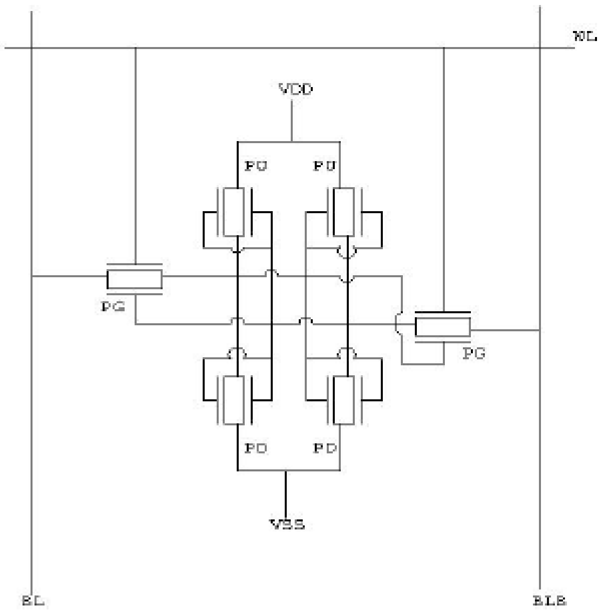


Figure 24. Double gate finFET FLEX-OSN topology

4.3.3.9.3 Increasing Storage Node Spacing

By increasing the spacing between storage nodes, an SEU caused by the collection of charge at several closely spaced nodes can be prevented. By design, this solution carries a significant area and power penalty; it also generates interconnect delays. Knowledge of the SRAM layout is critical to the assessment of risk for MCU [56].

4.3.3.9.4 Preventing Transient Propagation

Hardened memory cells can be implemented using transistors that block the feedback loop to prevent the propagation of the transient along the loop. However, this design has limitations in terms of recovering the initial voltage level at circuit nodes following a strike, and the hardened cell also requires periodic refresh pulses [57].

4.3.3.9.5 Circuit-Level Filtering

At the circuit level, filtering can be implemented using multiple pass transistors to reduce the magnitude of a transient pulse. These transistors are always on and act as low-pass filters [58]. This technique reduces, but does not eliminate, the sensitivity to upset and bears a speed penalty (i.e., a delay).

4.3.3.9.6 Combinations

An SEU-robust design not using poly-silicon combines several of the previously described mitigation techniques, making the best use of their benefits while being less penalized by their limitations. The design in reference [59] combines filtering with transistor-based spatial redundancy, although not requiring separate well and periodic refresh pulses.

4.3.4 SEU Protection in SRAM and Reprogrammable FPGA (RFPGA)

Based on its properties, there is an increased interest in SEU protection in SRAM-reprogrammable FPGA (RFPGA) devices:

- Non-recurring cost is lower than that for an ASIC.
- Holds the capability to be reconfigured in flight.
- High-performance and complexity supports system-on-FPGA design.

Protection against SEU is important for this component because an SEU in the configuration memory not only affects the user data or component state but can also alter the functionality of the circuit or turn the direction of the input/output (I/O) pins.

The ECC-type protection techniques that are successfully applied at memory cell level cannot be applied to FPGAs without major modification of the chips' architecture. Therefore, mitigation techniques for SEU-protection of SRAM-RFPGA are different and include:

- Configuration scrubbing or read-back and partial reconfiguration.
- TMR (registers with combinatorial logic and voters).
- Redundancy of user memory.
- Voting schemes (on logical feedback paths on output).
- Triplication of I/Os.

4.3.4.1 Configuration Scrubbing

Scrubbing is used to continuously clean the configuration bitstream and repair SEU soft errors. The scrubbing prevents the potential accumulation of configuration upsets and works upstream to reduce the likelihood that two upsets manage to overcome the TMR implementation [60].

4.3.4.2 TMR Implementation for SRAM-FPGA

The SRAM-FPGA flow typically implements sequential and combinatorial logic. A standard TMR implementation with single voter would only triplicate the sequential logic elements and process their output through the single voter. This implementation is not suitable for SRAM-FPGA. Instead, the full chain of sequential and combinatorial logic elements need to be triplicated, as shown in figure 25. This can be implemented in the hardware description source code (i.e., functional TMR) or design tool (e.g., Xilinx TMR tool).

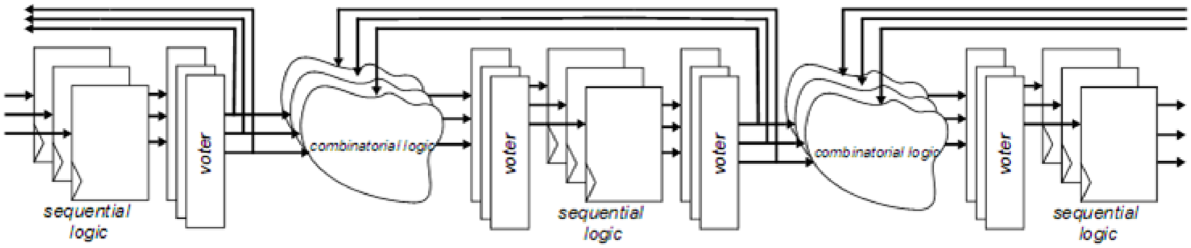


Figure 25. TMR implementation on FPGA

Note that TMR with scrubbing is an efficient but costly method, including an area penalty. Therefore, other techniques focus on the lower cost and smaller systems, but, thus far, they have not been used in aerospace applications. Such techniques include the use of an auxiliary FPGA, storing all user bits and implementing a cyclic redundancy code (CRC) as an ECC.

4.3.4.3 Dedicated FPGA Design for Radiation Hardening

Some hardened RFPGAs are available from several vendors, such as ATMEL, XILINK, and ACTEL. The designs are typically proprietary and a significant amount of test data are not available.

4.3.5 Fault-Tolerant ASIC Design

To counteract the cost issues associated with radiation-hardened technologies, research efforts focus on the usability of commercial ASIC technologies for space and safety-critical applications. One of the main issues is the absence of a standard integrated framework of circuit design techniques to provide simultaneous mitigation of SEU, SET, and SEL; therefore, the fault-tolerance design is achieved by combining and integrating various techniques [61].

4.3.5.1 The SEL Protection Switch

This element is introduced in a standard cell to control its supplied current as an alternative to the layout-based mitigations described in section 4.3.1.1. When excessive current is detected, the SEL protection switch (SPS) will switch off the power supply. The SPS circuit schematic is centered on a current sensor/driver transistor. The transistor provides enough current during normal operations when its function is a driver and must survive a potential latch-up as a current sensor.

The duration of the protection phase is programmed in the logic, so that once that phase is completed, the power network controller sends a pulse that reinitializes the SPS circuit.

4.3.5.2 Combination of TMR and SPS

As explained before, redundancy is the most frequent approach to mitigation of SEUs and SETs. Redundancy needs to be combined with the SPS design to adequately cover ASIC's SEE vulnerabilities. This combined level of protection generates significant modifications to the standard TMR/DMR circuit designs. The protection provided by TMR is applied to the power domain of the ASIC.

Once an SEL condition occurs in one of the triplicated power domains, the SPS switches off the line while the other two domains continue in normal operations, and the circuit now operates as a DMR circuit for as long as the SPS is active.

4.3.5.3 Combination of DMR and SPS

The DMR mitigation technique is typically chosen over the TMR mitigation technique to reduce the overhead but keep the reliability level high by using a self-voting scheme. When the SPS breaks off the circuit line affected by an SEL, the redundancy is lost for the entire duration of the protection.

The next difficulty to address is the intrinsic high sensitivity of this setup to SET. If an SET occurs during the clock transition (e.g., near the active clock edge), the setup/hold time margins can be violated, resulting in the FF being uncertain about the correct output state. When the FFs are in different logic states, an SEU occurs and propagates through the logic to causation of a system failure. One solution that has been verified by fault-injection is a modification of the feedback line of the self-voter. Classical self-voting is derived from a three-input majority voter scheme in which the inputs are the two external input values and the voter’s own output. The proposed modification to the feedback line of the voter is to integrate a multiplexer so that the logic value of the FF data input is used as the third voter during the hold time and then back to the voter output when the hold is passed. When the clock transition occurs, a pulse controls the multiplexer and the FF data input is connected to the third voter input. If an SET occurs during that short amount of time, the third voter receives the correct logic value, regardless of the potentially wrong state at the FF output. By design, this solution is limited to transient pulses (e.g., a few hundredths of a picosecond) and by the FF hold time.

4.3.6 Protection Against SEFI

The SEFIs have distinct signatures depending on the electronic component they affect [62]. However, in all cases, SEFIs most likely disappear with resetting; therefore, the most used mitigation technique for SEFI is to implement a watchdog to detect an SEFI that will trigger a reset command to reinitialize the board.

Some SEFIs are caused by an SEU in a sensitive area of the board. The current approach is to characterize as an SEFI any situation for which the root cause of the upset is not determined (e.g., no bit error found). When the root cause is identified, SEFIs are likely to be recast in other types of SEEs (e.g., SEU, SEL, and SESB).

4.3.6.1 DRAM-Type Components

The SEFIs observed in DRAM-type components cause the inadvertent execution of the built-in test mode. In this mode, the device no longer responds to the write or read commands. The device stays in the test mode until either further irradiation affects it by returning to normal operation mode or a termination signal is sent. Note that an SEFI is not observed in DRAM without the test mode implemented.

4.3.6.2 EEPROMs

The SEFI can manifest itself in at least three observed types of errors. The first type is the appearance of repeated errors every few cycles, combining MBUs with increased bias current during the read cycle. In the absence of power cycling, the next read cycle shows the same configuration of MBU with increased bias current. When the power is cycled, the device returns to normal operations. The second type of error manifested with “00” in all address locations and the inability to read the device. As previously experienced, normal operations resume after power cycling. The third type manifests itself as an occasional (i.e., once over many cycles) error in a byte.

4.3.6.3 Microprocessors

The most observed SEFI causes the inadvertent execution of the “HALT” instruction. This error can be the consequence of an SEU in the program counter that sends the execution into different areas of the memory. This type of error is detectable via noticing alterations in the address bits. An SEFI can, however, occur in the absence of errors in the program counter. A reset is required to resume normal operations.

4.3.7 Example of SEE Sensitivity at Equipment Level

The increased complexity in the cockpit, brought about in part by the significant increase of processed information, is illustrated by the trend to replace central processing units (CPUs) by a graphics processing unit (GPU) to achieve high-performance parallel computing that processes a large amount of data, whereas a CPU is simpler and dedicated to a single threat of execution.

The internal structure of a GPU is different from that of a CPU. A GPU is designed to accomplish several elementary tasks in parallel, rapidly manipulating a high number of memory locations, whereas a CPU is optimized to sequentially execute complex tasks.

Memory elements in the GPU (e.g., registers and shared memory) can be affected by an SEU or MCU; the logic resources are vulnerable to SET. However, because of the construct of the equipment, a corruption might not be observable at the output. Specifically, a corrupted register might not be in use, the stored data in the register may be obsolete, affected shared memory bits might not be critical in the computation, or errors in logic elements might be masked. Because of this dependence on the code, the assessment of the SEE-sensitivity at the system level is specific and cannot be generalized to other applications [63]. A starting point, however, is found with the analysis of the elemental resources in the system.

4.3.8 SEB and SEGR Protection of Power Electronics

Protection against SEB and, to a lesser extent, SEGR, is different than protection against SEU in the sense that SEB and SEGR can result in the destruction of the electronic component; therefore, mitigations for SEB and SEGR are focused on external protections at circuit level and margins on the maximum tolerable power in the design (also determined as voltage stress: ratio of applied voltage to breakdown voltage).

Factors affecting the SEB sensitivity include: device rated voltage, percentage of voltage stress, chip size, temperature, technology, altitude (possibly latitude and time of year), and shielding. The higher the voltage, the higher the sensitivity to SEB will be. Higher rated voltage devices will require smaller voltage stress. However, the relationship between SEB-sensitivity and stress voltage is highly non-linear.

4.3.8.1 Safety Margins: Derated Power for MOSFETs

Margins in the design or selection of the component include considering its performance in derated power conditions compared to the component maximum (breakdown) voltage level. Recommended safety margins for power MOSFETs normally require a derating to at least 50% [64] or 75% (MIL-STD-975 [65] is more conservative).

4.3.8.2 Safety Margins: Derated Power for IGBTs and Diodes

Margins for high-voltage diodes and IGBT are recommended to at least 50% [66] because diodes have a lower susceptibility to SEB than do MOSFETs or IGBTs; therefore, by applying design recommendations (e.g., phase-shifted bridge) to diodes, the resulting susceptibility will be even lower.

4.3.8.3 Protective Circuitry

One approach to mitigating destructive SEE in power electronics is to protect the circuit with a protective resistance. The protective circuitry can prevent a rapid CAT FC to occur while still allowing SEB pulses that are characterized as an arrested burnout [67]. It has been shown that in the absence of the series resistor, power MOSFET’s typical response to a neutron hit is to trigger destructive avalanche energy. However, for IGBTs, the impact is less clear because the impulse response amplitudes varied, sometimes reaching destructive levels. In any case, current leakage ensues [68].

4.3.8.4 Technology Evolution

The objective of technology evolution is to reduce the specific on-resistance and increase the breakdown voltage of the power MOSFET. Examples of developing technologies include the silicon super junction (SJ) and silicon-carbide (SiC) power MOSFET. This evolution shows promise, but large costs and limited testing prevent these technologies from being deployed in avionics systems at the present time. In some reports, limited tests show that the sensitivity of SJ MOSFETs to SEB and SEGR is not improved compared to the traditional technologies [68]; initial tests of SiC MOSFETs show improved robustness to SEB [69].

4.3.8.5 Issues

Factors affecting SEB are significant and dominate the technology and the voltage stress, therefore limiting the options for mitigation [69]. A circuit designer will typically not have the choice of technology for the power components, so the main actionable mitigation is on the voltage stress using margins.

However, SEBs have been observed even though the device is operating under the derated voltage, including when safety margins are at the conservative recommendation of 75%. Values of maximum voltage stress can be as high as 85% for target failure rates of 0.1% system failure per year [70].

4.4 CONCLUSION ON SEE CURRENT PRACTICES AND METHODOLOGY

The objective of this research was to develop a compendium of mitigation techniques and document their application, effectiveness, and limitations. The approach was to select key mitigation types through a review of existing literature.

Overall, the findings highlighted that all electronic components implementing transistors can be sensitive to SEEs. At a first level, destructive SEEs are mitigated in a specific way that includes significant safety margins on the design. Mitigation techniques for non-destructive SEE can be implemented at layout level and circuit level and have a preventive or corrective action. This research presents a portfolio of solutions, such that mitigations at circuit levels are typically a combination of techniques to minimize the penalties and meet the reliability target at the same time.

In 1998, it was estimated that in commercial avionics, approximately 20% of all “could-not-duplicate” issues were due to SEU. Recent evaluations of C-17 avionics systems conducted at the Boeing Radiation Effects Lab have concluded that:

- SEUs in main memory are well protected by EDAC.
- SEU in cache memory protected by parity bit may result in a reconfiguration need approximately once every 2–3 hours.
- SEU in unprotected devices, such as FPGA and microprocessors, may result in a reboot need once in approximately 200–300 hours (cumulative).
- Flight controls appear to be adequately protected by a combination of EDAC and redundancy.

However, the technology trends for semiconductor elements used (or to be used) in avionics, such as the size reduction and power increase, support an increase in SEE-related no-fault-found. This increase will eventually result in the mitigation technique(s) no longer adequately addressing the allocated safety objective. Either new mitigations will have to be found (e.g., at semiconductor substrate level, higher order ECCs) or new combinations of built-in and not-built-in mitigations will need to be proposed.

There are still large uncertainties regarding the response of some systems to radiation that can only be reduced by testing and provision by the manufacturers of error rate curves. More complex SEEs, such as SEFIs, may be attributed in the end to other types once the root cause is better understood. Finally, the work on new material yields components that need further testing and characterization before they can be accepted for aerospace applications.

5. DETAILED RESEARCH: EXPLORATION OF SEE MITIGATION TECHNIQUES, NOT-BUILT-IN AVIONICS SYSTEMS OR COMPONENTS

5.1 INTRODUCTION

Based on the compendium of mitigation techniques for SEE applicable to avionics systems, this research focuses on the next step of the SEE analysis methodology currently being drafted (i.e., the qualitative and quantitative SEE assessment and applying it to not-built-in mitigation techniques).

The information presented in the following subsections highlights the challenges the designer faces not only when selecting the mitigation technique(s) but also when substantiating the selection based on reliability information. The avionics market is still conservative with respect to the selection of mitigation techniques. Despite the significant penalties, hardware redundancy is the most commonly used not-built-in technique and is required by aircraft manufacturers for safety-critical systems. Therefore, the method selected for this investigation is TMR/DMR implemented on device logic paths and configuration memory cells. The selected examples involve the DAL A flight control computer (FCC) with analysis made at two different levels: the semiconductor device and the LRU.

Before the analysis can be performed, reliability information must be obtained. There is a surprising lack of available data from the manufacturers and a similar lack of transparency at the aircraft level when reliability and implementation solutions are prescribed to the system supplier. This report tries to identify the pitfalls when substantiating the use of reliability data for SEE because it forms the input to the SEE safety analysis process.

This section is organized mainly around the major phases of the SEE safety analysis preparation to the SSA. Section 5.2 summarizes the SEE safety assessment processes covered under this report. Section 5.3 focuses on the collection of input information to build the quantitative reliability value and indicates what challenges the designers face at each step. Section 5.4 collects the various adjustments that can be made to the raw quantitative values to obtain an accurate aggregated failure rate and not be overly conservative. Section 5.5 compiles the various methods for testing the failure rate from chip level to LRU level, their applicability, their limitations, and what factors can drive the designer to select a particular method. Finally, section 5.6 uses real-life implementations to analyze the determination of failure rates for an FCC at the device and LRU level using testing and manufacturer data. The section also provides lessons learned, which highlight factors coming to play when determining failure rates.

5.2 SEE ASSESSMENT PROCESS

Figure 26 shows the steps in the SEE safety assessment that will be taken into account in the SSA. The entry condition is the classification of the avionics components into SEE sensitive and SEE immune. The objective is the development of SEE failure rates.

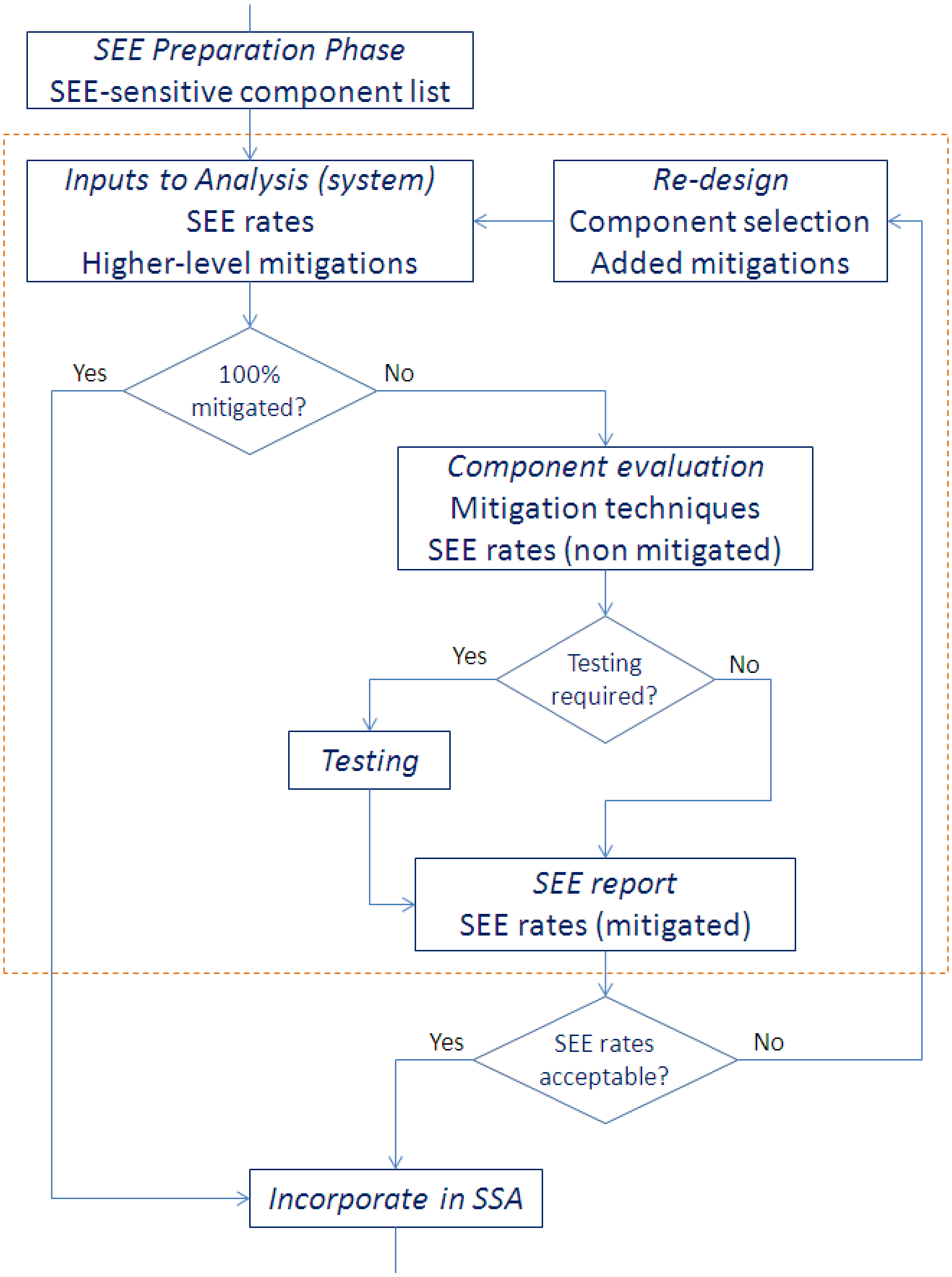


Figure 26. Component assessment process

The input information to the analysis are the SEE rates and implementation at a higher level (e.g., architecture) of mitigations that impact the effective SEE rates to take into account at component level. If the output of this preliminary analysis is that the SEE sensitivities are fully mitigated, then the next step is to integrate this result into the SSA. If the level of mitigation is not 100%, then the analysis at component level starts.

Depending on the level of accuracy of the data collected and the requirement for testing, the following steps can be classified as qualitative or quantitative. The output of the analysis is the consideration of whether the mitigated SEE rates meet the acceptability level. If they do not, a redesign should be envisioned whereby either the selection of the component itself is revisited or additional mitigations are implemented. If the mitigated level is acceptable, the findings are incorporated in the SSA.

5.3 INPUTS TO THE COMPONENT EVALUATION

Fault rates can be hard or soft; both types should be considered. Moreover, some soft errors can be recovered after cycling power (e.g., SEFI, SEL) or be transient in nature (e.g., SET). Because some soft errors can be recovered by automatic or crew-initiated reset, they may not constitute an equipment fault. The SSA requires the assessment of the SEE rate at the LRU level. Typically, this value is the aggregate of the SEE rates of all the SEE-sensitive components that are used in the LRU.

5.3.1 Determination of SEE Rates at Device-Level

The SEE rates can be determined by calculation or provided by the aircraft manufacturer. For the sake of this investigation, consider the SEE rates to have not been provided by the aircraft manufacturer. To start the analysis with an initially conservative value, a method to roughly estimate SEE rates is proposed. It is indeed important to not start with an overly optimistic SEE rate value. Later, in the quantitative phase, actual SEE rates should ideally be provided by testing because analytical methods are unlikely to encompass all possible SEE and some SEE (e.g., SEL) are more difficult to predict.

In general, a single event will occur each time a particle penetrates the sensitive surface, *S*, of the DUT. The global sensitive surface can be further modeled as *N* sensitive volume of surface σ in interaction with neutron flux. The relationship between the SEE cross-section and the SEE rate is given by the equation (3)

$$\sigma = \frac{R_{SEE}}{\Phi_a \times N} \tag{3}$$

Where R_{SEE} is the SEE rate per unit of time and Φ_a the neutron beam flux per unit of time and surface. When *N* is unknown, the cross-section is indicated per bit or per device. Equation (3) is most often used in the form of:

$$SEE\_rate = integrated\_atmospheric\_neutron\_flux \text{ x } SEE\_cross\_section \tag{4}$$

5.3.1.1 Integrated Neutron Flux

Predicting the atmospheric neutron flux is not an exact science. For example, according to recognized references, such as reference [71], the neutron flux can be modeled as a function of latitude and altitude; moreover, the recommendation in reference [3] is to use 6000 n/cm^2 per hour for the rounded up conservative value of the integrated neutron flux (corresponding to the integration of the neutron differential flux for energies greater than 10MeV at 40,000 ft/12.2 km and for a latitude of 45º). Using a single value over the entire flight envelope may be too generic. To obtain a value of the integrated neutron flux that is adjusted with respect to specific altitude and latitude, annex D of reference [3] provides scaling parameters to be applied to the rounded conservative value of 6000 n/cm^2 per hour (see figures 27 and 28). To provide an order of magnitude, this value is conservative by a factor of 2 compared to ER-2 measurements performed in 1997 and by a factor of 300 when considering ground-level applications.

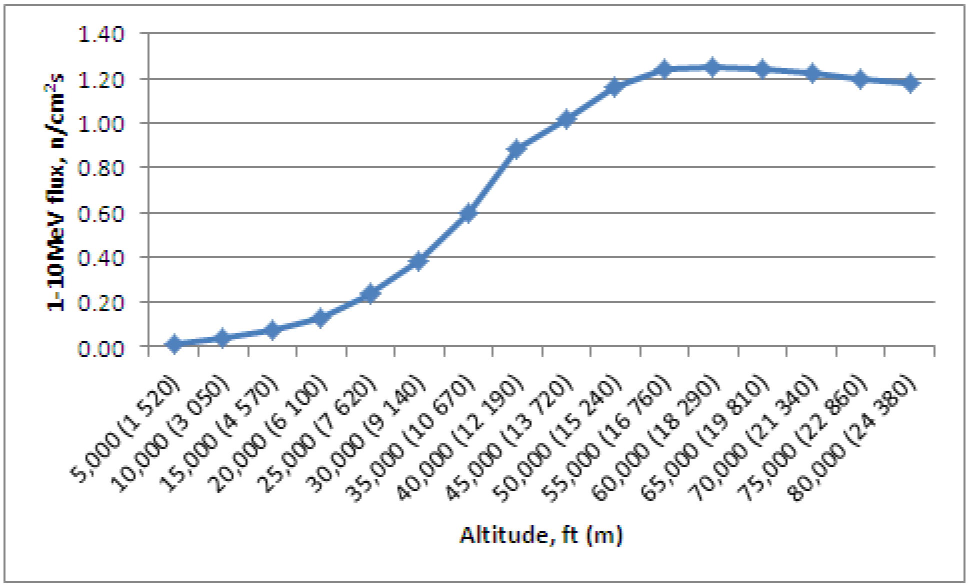


Figure 27. Variation of neutron flux with altitude

Note that this plotted fit (figure 27) is based on Boeing's simplified model, which diverges from the more rigorous AIR model from NASA Langley for altitudes lower than 8000 ft (Boeing's flux values are approximately 7% lower).

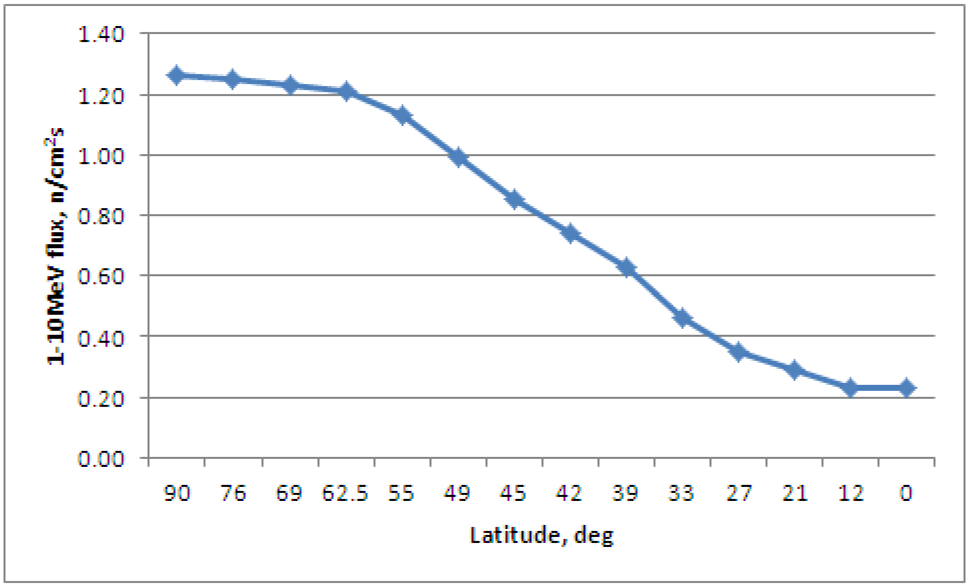


Figure 28. Variation of neutron flux with latitude

The simplified Boeing model (figure 28) indicates higher flux values than the more rigorous AIR model from NASA Langley for latitude above 40º (up to 3% higher at the pole).

However, when semiconductor manufacturer Xilinx launched its Rosetta experiment to collect real-time measurements of neutron flux at various locations (latitude, longitude, altitude) to estimate the SEU cross-section of its devices, the measurements did not match the expected results from applying the model-based methodology described in the normative reference [72]. The norm was later corrected (version A) along with the atmospheric spectral model. The corrections included the following elements:

- Realization that the proton flux is substantial and, for example, can account for an additional 7% in San Diego and as much as 35% for Hawaii's Mauna Kea.
- Reference [72] addresses terrestrial level measurements. However, the attenuation factor because of the building was not accurately accounted for. For example, up to 28% of the flux can be lost to the ground floor of a typical two-storied concrete building in the Silicon Valley

5.3.1.2 SEE Cross-Sections

The SEE neutron cross-section is the key parameter driving the probability that a component will interact with particles and, as a result, produce an SEE. The cross-section is a function of the feature size, which in turn depends on the technology.

Section 8 and annex G of reference [3] provide guidance on the determination of a conservative cross-section per semiconductor components using data plots. The envelope of cross-section magnitude is quite wide and datasheets from the manufacturers should be sought whenever possible.

5.3.1.3 Units of SEE Rates

For SEE primarily affecting bits (e.g., SEU, MBU), the cross-section is expressed in cm^2/bit. For other SEEs, typically visible via the component response (e.g., SEL, SEFI, SET, SEB), the rate should be expressed in cm^2/device.

In the literature, some SEU rates are expressed in FIT/Mbit. An FIT is equivalent to one failure in 10^9 device hours. To convert to cm^2/bit, the conversion factor of $7.1E^{-17}$ Mbit.cm^2/(FIT.bit) should be used. This factor is based on a high-energy neutron flux (E > 10MeV) of 13n/cm^2.hr at New York City [72].

Finally, at system level, SEE rates are no longer the appropriate metrics and should be replaced with MTBUR or MTBF.

5.3.1.4 Challenges

The main challenge is the quasi-absence of published SEE rates from the manufacturers. One reason is that SEE rates are probabilistic and vary with geographical location, altitude, and environmental conditions. However, even baseline information is normally not accessible to the system designer. To compensate, airframe manufacturers have created simplified models that are applied across several vendors and technologies. These should be used only in the qualitative phase to provide an order of magnitude.

5.3.2 Impacting Factors

Factors impacting the determination of SEE rates, primarily via the methodology used to obtain numerical value (unmitigated or mitigated), are of two natures:

- Indigenous when they relate to the selected technology
- Exogenous when they relate to the avionics system design and the system's intended use

Section 5.3.2.1 below presents a key example of the indigenous factor whereas the others focus on exogenous factors.

5.3.2.1 Impact of Feature Size and Memory Needs

All submicron integrated electronics devices are susceptible to SEEs; however, there is a correlation between the feature size and the occurrence of SEE errors. A commonly cited threshold value is approximately 90 nm.

Although mitigation and technology have made significant progress in reducing the rate of SEEs at the component level, the need for memory and performance has led to the increase in the number of components on a device; this increase has balanced and, in most cases, overpowered the gains on the cell. To provide an order of magnitude, table 26 indicates SRAM-based FPGA characteristics for some highly integrated systems adequate for ASIC-required performance [73] found in military/aerospace safety-critical applications [74].

Table 26. Comparison of high-integration SRAM-FPGAs

FPGA model	Spartan-6	Artix-7	Kintex-7	Virtex-7
Feature size (technology)	45 nm	28 nm	28 nm	28 nm
Number of logic cells	150,000	215,000	480,000	2,000,000
RAM Block	4.8 Mb	13 Mb	34 Mb	68 Mb

These characteristics are common to all types of RAM. Direct RAM technology has regularly improved the bit error rate by a factor of 4 or 5 with each generation. However, the DRAM system error rate has remained unchanged because of the concurrent increase in memory density.

For the SRAM technology, it is the combination of lower power consumption and scaling requirements that initially resulted in increased bit error rates with each SRAM generation. Even if it seems that the bit error rate has reached saturation with the DSM technology, the increase in memory density maintains the increase in system error rate [75].

5.3.2.2 Impact of DAL

The DAL indirectly impacts the determination of the SEE rates, in the sense that the higher the DAL, the more rigorous the computation should be. It is therefore recommended that for DAL A, the determination include testing at component and LRU level. For DAL B equipment, the computation should use testing data on similar parts, and for DAL C equipment, an SEE fault model can be used [3]. SEE screening is typically not required for DAL D and E equipment.

5.3.2.3 Impact of Automation Level

When the crew is not part of the operational loop (i.e., not in the loop or on the loop), the consequences of SEE may be more directly serious. More rigor in the determination of the SEE rate should be applied to safety-critical automated systems, such as requiring testing (e.g. DAL A Type I systems, such as fly-by-wire).

5.3.3 Orders of Magnitude

5.3.3.1 The FIT

Orders of magnitude can be found in the literature. For example, hard-reliable mechanisms (e.g., gate-oxide breakdown, metal electro-migration) have a typical failure rate of 1–50 FITs. When considering that only half of these mechanisms degrade the integrated circuit performance, the overall failure rate is typically 5–150 FITs. On the end of the scale, without any mitigation, error rates can be as high as 50,000 FITs per chip [75]. ASIC below 90 nm have exhibited 1000 FIT/million gates and 1000 FIT/million memory bits [76].

5.3.3.2 The MTBF

Hard failures due to mechanical mechanisms (as opposed to destructive SEE) are generally in the order of 100–1000 FITs (10^{-6} to 10^{-7} failure/device.hour) for avionics [77]. Let’s take the example of a microprocessor with a FIT rate of 600 at sea level in New York City and consider the impacting factors of the number of devices (see table 27) and altitude (see table 28):

Table 27. Impact of number of devices on MTBF

Characteristics	Impact on MTBF
600 FIT rate at sea level/NYC	MTBF: 190 years
1000 microprocessors fielded in system	Combined MTBF: 70 days

Table 28. Impact of altitude on MTBF

Characteristics	Impact on MTBF
600 FIT rate at sea level/NYC	MTBF: 190 years
= 367,200 FIT rate at 40K ft/pole	MTBF: 110 days (for one unit)
100 microprocessors fielded in system	MTBF: 1 day

5.4 BUILDING SEE RATES

Once the device level SEE rate is established, the robustness (e.g., FIT) at circuit level needs to be established. The accuracy of the estimation method needs to be adequate for the criticality level of the equipment (see sections 5.3.2.2 and 5.3.2.3).

In addition, the effect of SEU in the configuration memory are highly application dependent. Moreover, implementing the same algorithm using different methods and IP core may result in different system integrities [78].

5.4.1 Estimation of “Critical” Bits

The most conservative value for an aggregated SEE rate would be to multiply the bit/device level SEE rate by the number of bits/devices. However, this computation may lead to over-specification and would not qualify for the required level of estimation method accuracy because not all bits/devices are created equally on an implementation.

Methods to determine critical bits are classified in three groups:

1. Estimation based on used resources
2. Estimation via fault-injection methods
3. Estimation via radiation testing

In some instances, a unique consideration of bits in usage is a conservative value for critical bits.

5.4.1.1 Estimation Based on Used Resources

The assumption is that only bits belonging to used resources can be critical. The fraction of on-chip resources used within the LRU during the various avionics modes of operation should therefore be specified.

A more precise estimation may be done via design tools. For example, critical bits for an FPGA can be estimated by multiplying the FPGA resource utilization reported by the Computer Assisted Design (CAD) tool by the number of configuration bits per resource [79]. Another method referred to as static criticality evaluation is based on the analysis of the design’s NETLISTs. However, this method typically returns very pessimistic estimations (see section 2.4.7.8).

To provide the reader with an order of magnitude, consider the FIT rate for a configuration memory typically computed by multiplying the FIT/Mb rate by the configuration memory size (minus overhead bits and block random access memory [BRAM] content). This method leads to overly conservative values because a maximum of only 10% of configuration bit upsets actually result in a functional failure in the design. It is recommended to integrate an analysis of critical bits based on the generation of functional failure.

5.4.1.2 Estimation Based on Generation of Functional Failure

Not all bits are created equal and previous research work has evaluated the vulnerability to configuration bit upset (in FPGA) and to control bit upset (in ASIC). The analysis attempted to qualify critical bits and quantify an architecture-dependent vulnerability factor. The determination of critical bits based on the generation of functional failure is cumbersome, time-consuming, and costly.

Applied methods for this estimation are based on fault injection and include two subcategories: external error injection and internal error injection (for more details, see section 2.4.7.7). Some manufacturers provide tools to identify the critical bits (less than 20% of the configuration bits) and claim the results are still conservative while reducing the FIT rate by approximately 33% [80].

5.4.1.3 Derating Factor

Another way to identify the probability that a bit flip will cause a failure is through the SEU probability impact, also known as the derating factor. The importance of appropriately derating the device can be understood from the following observation: on average, it takes between 10 and 100 upsets to actually generate a functional failure. In the absence of derating data, a conservative factor of 10 is recommended.

Figure 29 depicts the variation of the derating factor from Xilinx’s Rosetta experiment. The baseline value of 1.0 is being set in compliance with reference [72] (i.e., New York City and 34,000 ft altitude). The manufacturer’s recommendation, based on these results, is to consider a worst case derating factor of 561.7 when no precise context is provided.

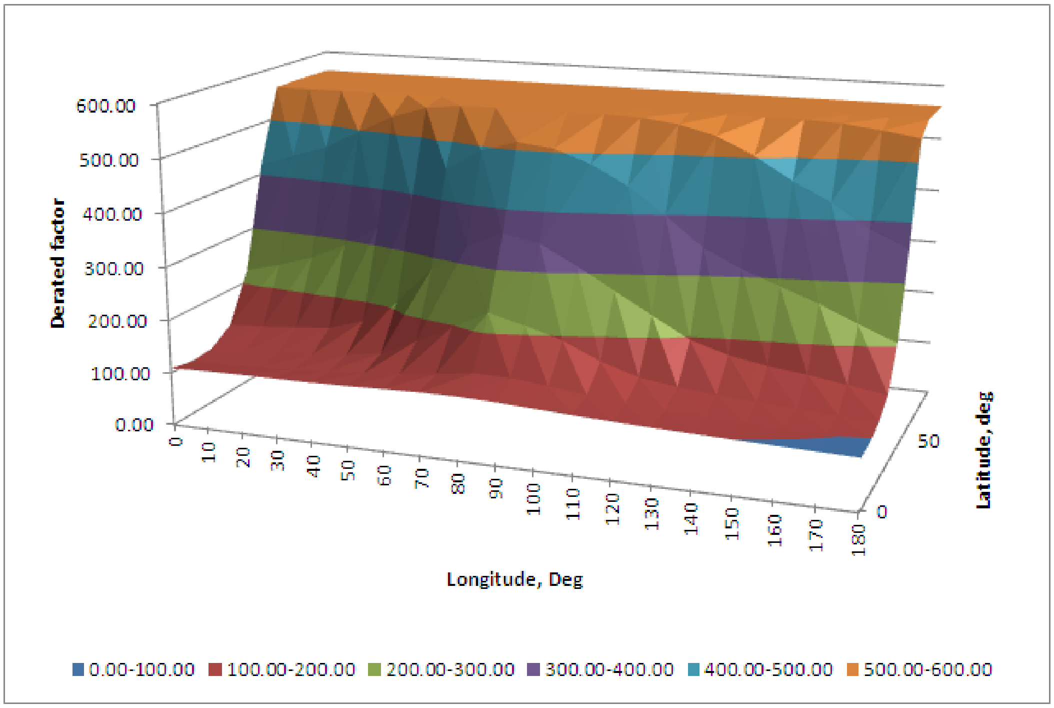


Figure 29. Derating factor from Xilinx's Rosetta experiment

5.4.2 Effectiveness of Mitigation

Fault tolerance is a capability of a system to recover from a fault or error without exhibiting a failure. Mitigation techniques can be used to increase the fault tolerance of a system and can be implemented on-chip (e.g., ECC), at circuit level (e.g., TMR), at LRU level (e.g., watchdog timer), and at system level (e.g., duplex architecture with dissymmetry). Not-built-in techniques are typically at circuit level and above. The selection of the technique(s), when not imposed by the aircraft manufacturer in its specification documents, depends on several factors. Before making a selection on the final ASIC or FPGA, designers should consider:

- The prescribed or derived by allocation FIT rate or MTBF (safety and reliability)
- The detection time of events (may impact the device time performance)
- The means of detecting the event (may impact the device performance through penalties)
- The recovery time after event detection (considering sensitivity to disruption)
- The performance penalty, area penalty, and monetary cost of the mitigation solution(s)
- The overall system performance
- The implications at system design level

The following subsections emphasize some of these aspects, whereas section 5.6 provides several examples.

5.4.2.1 Taking the Operation Into Account

Moreover, the selection of an appropriate mitigation technique is based on the operation of the device, not only in terms of reliability, but also in terms of availability, such as knowing whether the device operations can be interrupted.

5.4.2.2 Modular Redundancy, Software Fault-Tolerance, and Tradeoff

TMR with majority voting is typically implemented in safety-critical applications to protect against both SEU and SET. The major drawbacks are the penalties (overhead and area) and implementation challenges (e.g., application of optimization tools).

The effectiveness of TMR is determined by the size of the voted logic blocks and frequency of voting; smaller-size blocks and more frequent voting are more efficient, but the overhead might not be acceptable. To set a benchmark, redundancy/voting is set at FF level, which is the smallest level that is still transparent to the logic design (see figure 30).

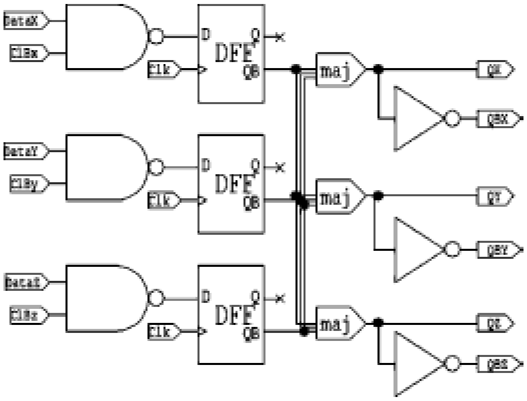


Figure 30. The TMR FF

More economical alternatives to TMR found in avionics include dual-rail (DMR) with self-voting (see the example in section 5.6.4). To compare with TMR at a similar level of implementation, consider SERT dual-rail FF (shown in figure 31).

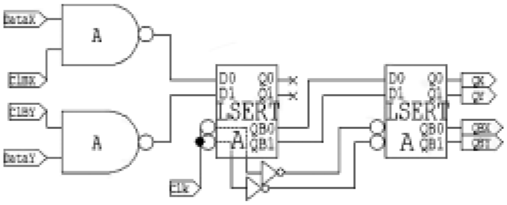


Figure 31. The SERT dual-rail FF

To reduce the performance and area penalties associated with hardware redundancy, software implemented fault-tolerance can be considered in combination with TMR/DMR. Most research has been performed on a group of software fault-tolerance techniques under SWIFT techniques for both ASICs and FPGAs. However, some work is still required to transfer these techniques into a viable market, most likely for high-reliability applications and, currently, primarily space applications. Such research work shows that software-implemented techniques can achieve decent detection rates compared to TMR or DMR, capturing approximately 90% of the errors [81]. The tradeoff comes from the fact that SWIFT techniques carry a performance penalty of 2X, whereas TMR and DMR carry an area penalty of 3.7X and 2.5X, respectively (while capturing more errors without impacting performance).

5.4.2.3 System Considerations

Should a built-in technique, such as ECC, be implemented to correct bit upset, it is still possible that while a critical configuration bit upset is corrected, an error can still propagate in the logic path. In particular, it is important to protect feedback or decision paths so that the device cannot be driven into an unintended mode prior to the correction of the upset configuration bit. To guarantee uninterrupted operation, hardware redundancy solutions, such as TMR/DMR, are required. Moreover, the designer can add a device reset if the upset is detected in a critical configuration bit.

5.5 PROPOSED METHODS FOR DETERMINING SEE RATES

Several methods are proposed ranging from radiation-based to analytical. The choice of the method(s) should be commensurate with the factors defined in section 2.4.6.1 and reasonableness of testing. In general, the process for determining the impact of neutron particle flux on avionics is a combination of analysis, simulation, and testing. The ratio of each is dependent on the criticality of the system.

5.5.1 In-the-Loop Testing

This method is recognized as the highest level of testing and is expected to provide the most accurate data for all SEE types. In this setup, the DUT is the LRU. It is subjected to a high-energy neutron or proton beam. The DUT is connected to a simulator platform that supports its operation during the exposure to the radiation and monitors/records the LRU output.

Section 5.6.4 presents a use-case of closed-loop testing on a recoverable FCC, and illustrates some of the lessons learned from using this setup to test for SEE-induced errors in avionics.

5.5.2 LRU Irradiation

In this setup, the LRU is not operating in an active loop. The LRU is subjected to a high-energy neutron or proton beam similar to tests performed for space applications. Because the LRU is of larger size than the irradiating beam, the test objectives must include several target areas on the LRU and different widths for the beam (see table 34).

This approach is relevant for identifying the propagation of SEE in the LRU to functional interrupts, latch-up, or reboot.

5.5.3 Using Components Datasheet or Test Compendiums

This approach is to use existing data (from datasheets or radiation testing) for key devices in the LRU. Because data are limited to snapshot results for each of the devices, the potential for propagation of SEE-induced errors within the LRU cannot be inferred from these data. This approach requires the setup and updating of a database, which to date remains limited. The content and status of existing databases are usually reported at the yearly IEEE RADECS.

Irradiation data come from two types of experiments: 1) neutron/proton testing and 2) heavy ion testing. Note that the data from heavy ion testing cannot be used as is for neutron cross-section and require a model-based transformation [3]. Finally, most data from heavy ion testing pertains to space application components and only a few of these components are also considered as targets for aircraft avionics.

5.5.4 Using Generic SEE Data

This approach has the least technical basis because it does not use data for the specific SEE-sensitive components in an LRU but rather generic SEE data. Like the previous approach, it relies on static responses to single events and ignores the dynamic response at the LRU level (e.g., error propagation). Because there are no specific data available, reference [3] suggests applying conservative margins. However, the rationale for the determination of these margins is not stated.

5.5.5 Stimulating Component With Focused Laser Beam

This approach uses focused picosecond-pulsed laser beams to measure SEU cross-sections as a function of LET. Transfer functions exist to then convert the LET-based cross-section into SEU rates [7].

The approach can be used as a less expensive alternative to neutron testing during both the initial estimation and the monitoring phases. There are several issues with the method: it is relatively new compared to neutron testing, it uses aggregated data to indirectly obtain the SEU rate, and the data substantiating the correlation between the LET cross-sections and SEU rates are limited.

5.5.6 Using In-Service Data

This approach is limited to components with ECC (e.g., EDAC), where the erroneous bits are identified and recorded as part of in-service monitoring. The output is an SEU bit error rate that can be compared with the rates obtained from testing.

To provide actionable results, the processing of the in-service data must consider (at least) the following:

- The error may not be the sole result of atmospheric neutrons; other factors, such as vibration transients and software issues, must be analyzed for exclusion
- The number of SEU-susceptible bits should be known beforehand or should have been reliably estimated

- Circumstantial data supporting the characterization of the SEU must accompany the recording (e.g., altitude, latitude/longitude)
- The data storage recovery and cleanup/reset must be part of the airline's regular maintenance program (including the fact that the process must be auditable)

5.5.7 Fault Injection Methods

Whereas the above methods present a direct way of testing, they might be expensive. Fault injection methods artificially flip bit(s) and can therefore be used to estimate soft error rates in a more economical manner. However, the efficiency of the method is directly related to the ability to reach all the critical nodes (issue of accuracy of injection) and inject a fault. It is, as with the previous methods, time-consuming (issue of injection speed).

5.5.8 Analytical Approaches

An analytical method to estimate the soft error rate is based on the generation of the individual and aggregate error rates from the NETLIST [82]. Therefore, an existing implementation is not required. The main challenge of the analytical approaches is to remain efficient in the presence of mitigation (e.g., a feedback loop on the TMR voter) and most of the time layers of mitigation (e.g., TMR with scrubbing).

Radiation effects are typically modeled with a Poisson distribution. SEU events are represented by a Poisson distribution with upset rate λ. As discussed in section 2.4.6, the upset rate is dependent on the radiation environment and device characteristics. The relationship between MTBF and the upset rate in the absence of mitigation is given by:

$$MTBF = \int_{0}^{\infty} e^{-\lambda t} dt \tag{5}$$

For TMR mitigation, each of the three modules is seen as independent and the result is correct as long as two modules out of three work correctly. Therefore, the MTBF can be expressed as

$$MTBF = \int_{0}^{\infty} \left(3e^{-2\lambda t} - 2e^{-3\lambda t}\right) dt \tag{6}$$

Note that periodic scrubbing is typically associated with TMR to avoid the accumulation of upsets. Although reference [83] has conducted its assessment in a space radiation environment (1,000 km circular orbit at 60 degree inclination), the numerical values provided in table 29 illustrate the efficiency of TMR mitigation. The FPGA is an Xilinx space-grade Virtex XVC300.

Table 29. Analytical reliability values for virtex FPGA with various mitigations

Mitigation Strategy	Reliability mission time = 1h	Reliability mission time = 10h
Without mitigation	0.959	0.659
TMR only	0.995	0.731
TMR with scrubbing (rate = 1 min)	0.99991	0.9991
TMR with EDAC	0.9999994	0.999994

Periodic scrubbing has a direct impact on the availability. Table 30 provides indicative numerical values for the same application as above.

Table 30. Analytical availability values for virtex FPGA with various mitigations

Mitigation Strategy	Availability Scrub period = 1min	Availability Scrub period = 10 min
Periodic scrubbing	0.9963	0.9962
Detect repair	0.999998	0.999998
TMR with scrubbing	0.9967	0.9996
TMR with EDAC	2e-11	2e-11

The greatest availability and most robust solution are offered by the implementation of TMR with EDAC and periodic scrubbing.

5.5.9 Considerations About Testing

5.5.9.1 Where to Perform Testing

When using an SEE rate obtained from testing, one should be mindful of the exact testing that was performed. There are significant adaptation factors to be applied to obtain a meaningful value. In addition, when semiconductor manufacturer Xilinx tested its devices at several facilities, it was discovered that, although the results were self-consistent from one visit to the next at the same facility, they yielded different cross-sections across facilities for the same part number and under the same testing conditions. To provide the reader with an order of magnitude, table 31 summarizes the cross-sections obtained for the configuration bits of the device referenced as XC2V6000 (5000 actual upsets each to obtain 95% confidence values) at various testing facilities.

Table 31. Configuration bit SEU cross-sections for different testing factilities

Technology	Part Number	Test Facility	Cross-section
150 nm	XC2V6000	LANSCE (Los Alamos)	2.56 10^{-14} (±10%)
150 nm	XC2V6000	TSL (Stockholm)	3.38 to 4.35 10^{-14}
150 nm	XC2V6000	ISIS (UK)	4.35 10^{-14} (±5%)
150 nm	XC2V6000	Anita	5.25 10^{-14} (±7.5%)

The lesson learned from this observation is that manufacturers may have to use more than one facility to obtain their cross-section information—or find a way to use one of their technologies as a benchmark to which others can be compared. For Xilinx, the results of the 150 nm technology are used as a gold standard for use in calibrating the results of other technologies subjected to the same beam.

5.5.9.2 How Much Testing?

As the hardness of semiconductor devices improves, whether through technology improvement or implementing mitigation techniques, the number of upsets occurring when subjected to the beam radiation is also reduced. As a consequence, the accuracy of the results is statistically less for the same number of test hours. Therefore, to maintain the level of statistical accuracy in the results, longer beam exposures are required.

This effect can be combined with power restrictions on the beam. For example, the Los Alamos facility (LANSCE) currently operates at one-third reduced beam power whereas the test time slots remain unchanged.

Therefore, there is a risk that the data collected based on this reduced number of upsets might not be enough (when considering the statistical relevance). Other testing solutions, such as proton beam testing, are now more palatable. They are inexpensive and show a satisfactory correlation with atmospheric neutrons.

5.5.9.3 Rationale for Testing vs. Simulating or Modeling

On commercial off-the-shelf complex integrated circuits such as FPGAs and ASICs, the radiation hardness is difficult to estimate because of the challenge in identifying the source of the fault and in assessing the production means (i.e., separating faults from defects). The analysis of commercial FPGA components using computer models and simulations is not directly transferable to the circuit level because of the intrinsic layers of protection and circuit management logic.

5.5.9.4 Timing of Testing: Pre- or Post-Implementation?

For some specific devices within the LRU or for the LRU itself, a cost/benefit analysis will clarify the advantages of early or late testing in the design process. Whether using radiation-based methods or fault-injection methods, they cannot give a rough estimate of the soft error rate prior to the implementation of the mitigation. Analytical methods are able to provide the designers with pre-design estimates.

5.5.9.5 Level of Testing: Chip or LRU?

There are so many uncontrollable variables in the SEE that testing at chip level and aggregating for the number of chips might not capture the full range of effect or the SEE rate. There is a lack of research in characterizing the correlation, or at least the trend, between an aggregated SEE rate obtained from chip-level testing and an SEE rate obtained from system or LRU level testing.

5.6 CASE EXAMPLES

In this section, examples are provided of investigations of the design and effectiveness of SEE mitigation techniques not built-in. The avionics domain is not spearheading the semiconductor technology evolutions and remains rather conservative. Today, for safety-critical applications, the initial design may be done using FPGAs, but, once finalized, it is converted into ASIC to ensure the required level of rigidity for the maximum number of devices. What is left as “dynamic” is the user-design logic and the configuration memories, which will be covered by built-in techniques.

5.6.1 General Considerations for an FCC

The following sections use semiconductor technologies employed in the design of FCC. Section 5.6.3 discusses results at the device level and section 5.6.4 at the LRU/system level. As a higher level of mitigation, the FCC LRU are implemented as duplex architecture with dissymmetry, which is flown down to the semiconductor technologies and the double sourcing on the devices. The current number of manufacturers that can produce for the avionics market supports this requirement. Inside the Thales FCC developed for Bombardier, one of the FCC is using Altera semiconductors (Stratix II®) on its Freescale ASIC microprocessor, while the other is using Actel (ProASIC3®). See table 33 for more details on ASIC-FPGA conversions. Although each manufacturer claims that its solution for SEE mitigation implementation is proprietary, both use a redundancy (TMR with voters) mitigation technique for the logic paths in combination with some variation of ECC built-in memory cells (e.g., EDAC, Hamming codes, cyclic redundancy check).

In terms of specifications, the requirements are typically provided, in our experience, by the aircraft manufacturer in different forms: Boeing specifies FIT rates, and it is up to the avionics manufacturer to demonstrate the compliance, whereas Bombardier and Airbus specify the semiconductor technology and the mitigation techniques in the design documents provided to the avionics manufacturers.

5.6.2 Example of Macro-Sizing a Device and Reliability Analysis

The following example is excerpted from a Xilinx information paper [79] and covers the controller macro in the Virtex-5 FPGA. It broadly shows a methodology to estimate the FIT and MTBF of macros occupying only a portion of a given device.

In this example, the controller macro takes up 174 logic slices and one RAM block memory of 18kb, and implements the detection, correction, and error injection tasks. Because the controller macro is on the FPGA, it is itself subject to SEU.

Starting with the manufacturer data (see appendix C), the reported FIT/Mb for the configuration bits is 131 FIT/Mb. The second step is to convert the logic slices, their interconnection to the configuration, and the interconnection of the RAM block memory into configuration bits. The manufacturer provides a conversion table (see table 32).

Table 32. Number of configuration bits in selected virtex-5 features

Device Feature	Approximate Number of Configuration Bits
1 logic slice	1,181
1 RAM block of 18 kb	585
1 I/O block	2,657
1 DSP48E slice	4,592

For the controller macro, the equation is, therefore, (174 x 1,181) + (1 x 585) = 206,078 bits, or 0.206 Mb. This results in a FIT of 27 for the macro—or an MTBF of 4,228 years.

The more pessimistic estimation method of the macro FIT uses the percentage of device slices and RAM blocks that the macro occupies on the device as a prorata applied to the total number of configuration bits. For this example, the controller macro occupies 2.42% of the slices and 1.84% of the RAM blocks in the device. The device itself holds 11.37 Mb configuration bits. Using approximately 2.4% of the 11.37 Mb yields 0.27Mb, leading to a device FIT of 35 and MTBF of 3262 years. This estimate is 30% more pessimistic than the previous one. It can, however, be more readily computed and be used as a first estimation to select a device from its additional features.

Additionally, it is reasonable to apply a derating factor of 10. So, the first and more accurate estimate would in the end turn out to have a configuration FIT of 2.7—or an MTBF of 42,280 years.

Finally, the susceptibility from the RAM block needs to be considered. The nominal RAM block FIT data (see appendix C) is 692. The FIT for the one RAM block in the device is, therefore, 11.85—or an MTBF of 9633 years. Considering that only half of the block data content can be tagged as critical, the FIT can be reduced to 5.9—or an MTBF of 19,348 years.

The final result is obtained from combining the configuration FIT of 2.7 with the data FIT of 5.9, representing a FIT = 8.6 or an MTBF = 13,274 years.

5.6.3 FPGA Device Testing

The most common device recently introduced in avionics components is FPGA. Whereas its sensitivity to SEU makes its use more frequent in space applications, it is penetrating the avionics market. Note that critical avionics still support specific developments of ASICs, such as the recent collaboration of Airbus and ON Semiconductor® to specifically develop a digital ASIC based on 110 nm technology for the FCC of the Airbus A350 XWB [84]. These ASIC semiconductor technologies now have FPGA conversion targets, as illustrated through various application examples in table 33.

Table 33. ASIC and FPGA conversions for examples of applications

ASIC Family	FPGA Conversion Targets	Application types
SC5 – 0.5µm	Legacy FPGA and PLD	Industrial
SC3 – 0.35µm	Virtex-1®, Spartan-2®, APEX 20K®, Acex®, ProASIC Plus/500K®	Industrial, communications
ONC18 – 0.18µm	Virtex-E®, Virtex II®, Spartan-IIE®, APEX 20KE®, Stratix®, APEX II®, Cyclone®, Axcelerator®, ProASIC3®	Low-cost mid-range ASIC, FPGA/ASIC conversions, industrial (automotive), communications
SP110 – 0.11µm	Virtex-4®, Spartan-3/6®, APEX II®, Stratix II®, Cyclone II/III/IV®, Arria®, IGLOO®	FPGA/ASIC conversions, industrial (automotive), communications, avionics, defense, space
SP65 – 65nm	Virtex-6®, Virtex-7®, Artix-7®, Kintex-7®, Stratix III/IV®, Arria II®	Avionics, defense, space
SP40 – 40nm	Virtex-7®, Artix-7®, Kintex-7®, Stratix V®	Avionics, defense, space

Whereas custom designs on ASICs for critical avionics applications are typically confidential and proprietary, testing and analysis on FPGA are more accessible. In the following subsections, we analyze the efficiency of several mitigation techniques on the Xilinx Virtex II FPGA. The device is a reconfigurable SRAM-based FPGA whose variations are currently implemented in avionics applications but which could also be acceptable for space applications. Another interesting feature of the device is that it can conduct partial reconfigurations or write to the configuration memory post-configuration without disturbing the operation; this feature justifies both static testing and dynamic testing.

5.6.3.1 Virtex II FPGA Testing Setups

Static testing seeks to quantify SEU in the configuration memory elements without the device executing routine execution tasks. The execution of these tasks would affect the device clock and activate inputs and outputs post configuration. Dynamic testing covers these aspects and investigates the response of the combinatorial logic paths as well as the signal propagation. In reference [85], the static tests serve as a baseline against which the dynamic test results can be compared. In addition, dynamic tests without the not-built-in redundancy mitigation are a baseline for the assessment of the mitigation efficiency. The FPGA elements elected for monitoring SEUs include configuration memory, the user-designed logic, and the combinatorial logic. The performance of the device is quantified based on errors in the shift registers output and read operations in the configuration memory.

The DUT is integrated on a development board that includes a “service” FPGA acting as a configuration monitor and performing detection, counting, and correction of errors in the configuration memory. The errors are detected via a bit-for-bit comparison between the configuration memory and a mask file stored in a separate programmable read-only memory (PROM). When a mismatch is detected, a pulse is sent by the configuration monitor to a host computer for diagnosis. The configuration monitor corrects upset-induced errors through partial reconfiguration, also known as non-intrusive scrubbing because it does not interfere with the operation of the loaded design. Finally, the development board includes a functional monitor using a Spartan FPGA to generate test vectors and perform the comparison of the DUT output vs. the expected values. Differences are sent to an external computer for logging/recording. This setup allows the assessment of the efficiency of the configuration monitor in detecting and correcting errors.

5.6.3.2 Implementation of the DUT

The baseline DUT design consists of eight simple shift registers clocking through a user-selectable pattern (e.g., checkerboard). Each register is made of 500 FFs. The usage for each register is 40% of the FFs. A mitigated design has four of the eight shift registers implement TMR. Because of the inherent penalty associated with TMR, this design uses 80% of the FFs. In total, there are 2.8 million configuration bits and 737,280 BRAM bits.

To harden the Virtex II for safety-critical avionics application and space applications, the device design uses both TMR and partial reconfiguration. The TMR is implemented on the user-defined logic and the combinatorial logic paths to address both the SEU and SET sensitiveness. In addition, the partial reconfiguration (non-intrusive scrubbing) repairs errors in the configuration bit-stream without disrupting the operation of the device. It is up to the user-designer to apply read-back prior to the scrubbing to determine if an error occurred. Scrubbing is typically required for safety critical applications as the accumulation of bit flips may in the end defeat the TMR voters; their combination covers both static errors in memory and errors in the user or path logic.

5.6.3.3 FPGA Device Testing Results

5.6.3.3.1 Dependence of Cross-Section on Design

When comparing cross-sections obtained from static and dynamic (with continuous monitoring) testing on a simple non-mitigated design, the results are very close. However, dynamic testing (with continuous monitoring) on the partial TMR design yields significantly higher cross-sections. This is illustrated in figure 32 with filled diamonds (◆) representing cross-sections of a static, non-mitigated single-shift register; squares (□); the cross-sections of a dynamic non-mitigated single-shift register with continuous monitoring; and crosses (x) from the cross-sections of a dynamic 50%-TMR-mitigated eight-shift register design. It can be deduced that the design has a greater impact on the cross-section than the testing technique.

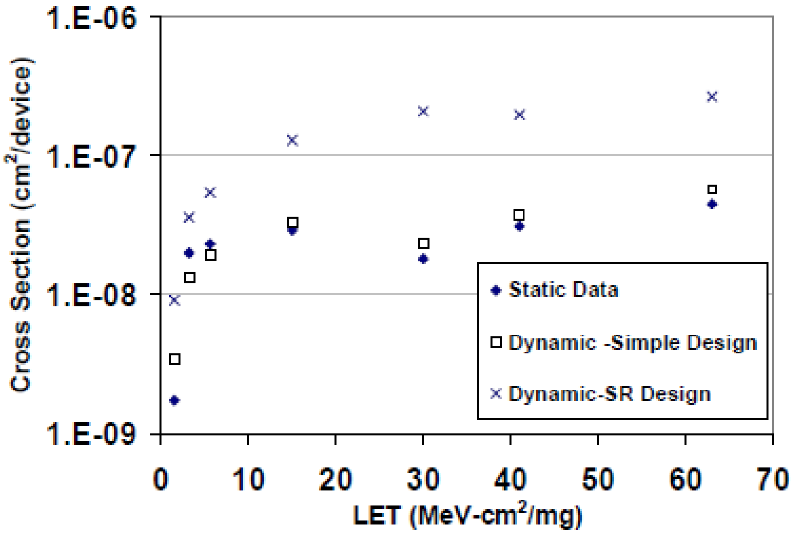


Figure 32. Cross-sections of total bits for static and dynamic tests without mitigation

5.6.3.3.2 Impact of Scrubbing

The efficiency of the scrubbing technique is assessed by comparing the rate of functional failures with and without mitigation as a function of the radiation fluence. A functional failure occurs when the shift registers can no longer shift the data out correctly and is characterized by a constant stream of errors. To be relevant, the test setup must be performed such that the upset rate remains below the by design scrub rate. In the DUT, the scrub frequency is set to 20 MHz (i.e., the maximum frequency for the communication hardware and software); however, it needs to be reduced by half because, for testing purposes, scrub cycles were alternated with read-back cycles. As a consequence, the maximum upset rate for meaningful results is three upsets/second.

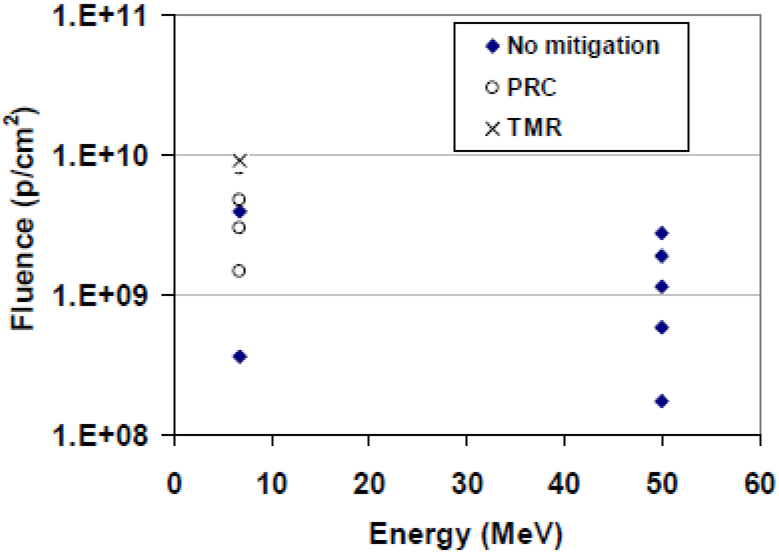


Figure 33. Fluence to first functional failure for non-mitigated and mitigated designs

The testing of maximum fluence to first functional failure (figure 33) shows, in order of efficiency: partial reconfiguration and TMR, with a maximum factor of 2. When TMR is combined with partial reconfiguration, no first functional failure could be obtained.

5.6.3.3.3 Comparative Efficiency of Mitigations

Partial reconfiguration, TMR, and a combination of partial reconfiguration and TMR were evaluated for functional failures against a non-mitigated design under a low upset rate heavy ion beam (see figure 34). The non-mitigated design showed a rate of functional failure of 45%; TMR reduces the frequency of functional failures by approximately 25% and partial reconfiguration provides a reduction of approximately 40%. When both were implemented, no functional failure was observed.

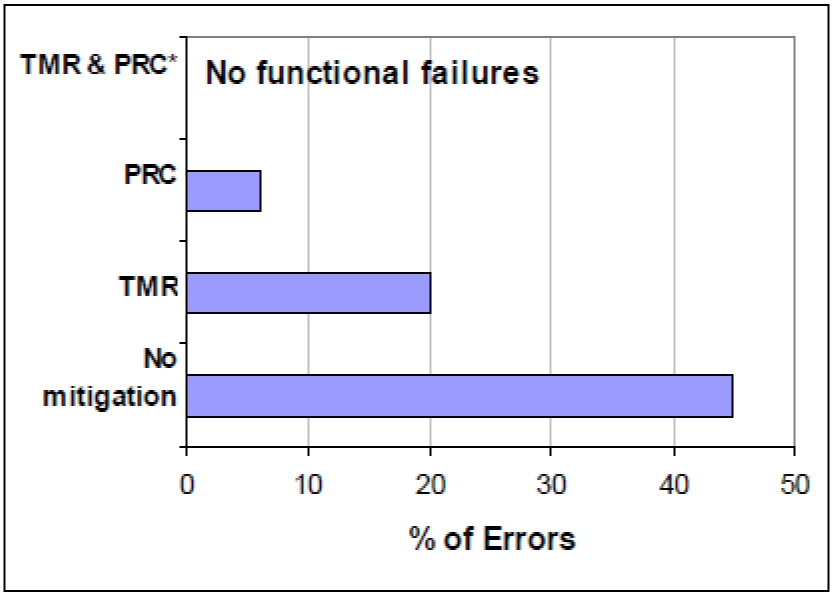


Figure 34. Comparison of error frequency per mitigated and non-mitigated designs

5.6.3.4 Lessons Learned

The testing that was performed involved simple operations. The sensitivity of a non-mitigated design (serving as baseline) is dependent on the amount and type of resources being used during the dynamic testing. Example of more complex resources could include lookup tables (LUTs), multiplier blocks, and digital clock managers (introducing their own SEU sensitivity).

5.6.4 Closed-Loop Testing of Recoverable FCC

This section is based on SEU experiments conducted at the Los Alamos National Laboratory on a closed-loop system consisting of a B737 simulator and a Honeywell Recoverable Control System (RCS) within an FCC [86].

5.6.4.1 Avionics Architecture

The RCS architecture is inherited from the Aircraft Information Management System (AIMS) offered on the B777 with a dual-lock-step computing platform (i.e., all computing resources are lock-step instead of cycle-by-cycle) and active hardware monitoring (independent from CPU) on every CPU cycle. This architecture ensures the detection of all hard and soft errors. When a fault is detected, the processing platform is trapped to service handlers.

This architecture is dual redundant with self-checking: the FCC has two copies of the processor's critical state data. When the self-check fails, the hardware and software fault detection and identification can isolate the error to either processor address, control bits, or data bits. The dual-lock-step technology then enables a roll-back to the state data from a previous processing cycle.
On the component level, the ASICs in a computing unit are implemented with robust software partitioning. Most of these ASICs have already been neutron tested at chip level so that background data on the qualitative sensitivity of the FCC are available.

5.6.4.2 Data Interpretation

For the experimental data from the testing to be relevant for aircraft operations, detailed considerations should be given to the determination of the scaling factor relating the time under the test neutron flux and the equivalent in operating conditions. The first step is to determine from the energy spectrum of the neutron source its correspondence to a normalized energy spectrum of atmospheric neutrons. The latter is based on models (see section 5.3.1.1). The ratio of the test facility integrated flux to the atmospheric model flux is the scaling factor to be used when interpreting the information. In the example under consideration, the reference of 34,000 ft/45º latitude corresponds to a normalized atmospheric neutron flux value of 0.56n/cm^{2}s. The scaling factor is 2.62x10^5, so that a 25-minute test run under the high-energy neutron beam corresponds to 1.09x10^5 equivalent flight hours at the reference altitude/latitude.

5.6.4.3 Closed-Loop Testing Results

The tests consisted of baseline runs (prior to exposure and in-between exposure) and test runs where the FCC was actuating control surfaces in the presence of a light gust. The test runs covered six test objectives, varying the targeted electronics components (e.g., RAM cells, CPU, flash memory) and beam width. The activation of the dual-lock-step recovery mechanism was also an input to the tests.

The article in reference for this section focuses on two runs, one with rollback recovery on and one with it off. The first run showed several SEU-generated recoveries (no recoveries were registered in the absence of neutron exposure). The induced SEU is noticeable as an error in the control command calculation, but it is captured by the self-checking algorithm after a miss-compare result between the two processors. The rollback recovery induces no noticeable perturbation in the flight dynamics. When the recovery mechanism is turned off, after a miss-compare, the control commands are reset rather than rolled back to a previous state (per legacy handling techniques in the B777 AIMS technology). Because the test runs involved small changes in control commands, the reset also showed no noticeable perturbations in the flight dynamics.

Finally, in some cases, the RCS stopped after several recoveries and the aircraft went out-of-control. Normal operations were resumed after power cycling. This effect is also attributed to the neutron exposure. The results are summarized in table 34. Each run has a duration of 60 minutes.

Table 34. Summary results from FCC closed-loop testing

Observation	Number of		Number of runs and target position
	Faults	Reboots	
No effects	0 0 0 0	0 0 0 0	7 – RAMs on scratched pad memory IC 8 – Flash on instruction memory 1 – Processor 6 – LSI chip next to processor
Normal rollbacks	2 5 34 14 7 9 11	0 0 0 0 0 0 0	2 – RAMs on scratched pad memory IC 1 – One CPU on processor 4 – Another CPU on alternate processor 3 – One CPU, as many RAMs & flash as possible 2 – As above but with wider beam (3”) 4 – As above but including the rollback area 2 – Narrower beam centered on first processor
Reboot but no rollback	0 0	1 1	1 – One CPU, as many RAMs & flash as possible 1 – LSI chip next to processor
Rollbacks and reboot	2 1	1 1	1 – One CPU, as many RAMs & flash as possible, including rollback area 1 – Processor
Rollbacks with reboot and stop	6 6 26	2 3 7	2 – One CPU on processor 3 – Another CPU on alternate processor 7 – As above but with wider beam (3”)
Rollbacks and stop	19 20 4 5 114	0 0 0 0 0	4 – One CPU on processor 3 – Another CPU on alternate processor 2 – One CPU, as many RAMs & flash as possible 2 – As above, wider beam to include the rollback area 11 – One CPU on processor with wider beam (3”)
Stop only	0 0 0 0 0 0	0 0 0 0 0 0	1 – One CPU on processor 1 – Another CPU on alternate processor 1 – One CPU, as many RAMs & flash as possible 1 – As above with wider beam (3”) 2 – One CPU on processor with wider beam (3”) 1 – LSI chip next to processor

5.6.4.4 Lessons Learned

To properly characterize and interpret the observations, it is necessary to go into detail:

- Consider not only the software in execution during the test (e.g., flight control laws, A429 interface software, and RCS software), but also the legacy AIMS resident software (e.g., Built-In Test Equipment, Init/Boot, operating system, dataload support). The resident software in this case included "retry" monitors that probably account for some of the observations by disabling the recovery software.
- Consider the beam width and neutron intensity distribution because it affects which components of the integrated circuit get exposed and with how many neutrons.

5.7 CONCLUSION ON SEE MITIGATION TECHNIQUES FOR NOT-BUILT-IN SYSTEMS OR COMPONENTS

The objective of this research was to further investigate the mitigation techniques for not-built-in avionics systems or components in terms of criteria for selection and effectiveness.

The first finding is more general and pertains to the selection of the appropriate mitigation technique(s) to be predicated on the development of SEE failure rates. The determination of these rates is a complex process that contains implicit clauses regarding the usability of the reliability data. Furthermore, the availability of reliability data varies widely according to the device manufacturer. Because these rates drive the selection of the device and its mitigation technique(s), substantiation of the approach should be commensurate with the safety objectives for the system.

Second, the challenges associated with the implementation of the mitigation technique(s) include the adequate assessment of the required safety and reliability values. To address potential tradeoffs, the designer must understand the intended use of the system to judge the acceptable time for detection of an SEE, the acceptable time to recover from an error, the acceptable level of penalty (performance, area, power, and monetary cost), the overall required level of performance at system level, and how the selection of mitigation technique(s) may impact the system design.

Third, the effectiveness of the mitigation technique is dependent on several factors. First, it is dependent on the SEE type (some SEE show after propagation inside the circuit whereas others affect the elementary cell level), which may translate as a level of implementation (cell, circuit, system) and a combination of solutions (TMR with scrubbing and/or partial reconfiguration). For redundancy, the mitigation is more efficient when covering smaller sized blocks with higher frequency voting, but the associated penalty might be unreasonable. In addition, TMR might be rendered useless in the absence of periodic scrubbing to prevent accumulation of bit flips.

Finally, the measurement of the effectiveness is dependent on the testing method used. The methods exhibit various levels of fidelity that may forbid their use according to DAL. In addition, the number of hours in the testing facility and the number of testing facilities used to build the SEE rate play a role in the quality of the data. Testing cannot encompass the full operational environment in which the device or LRU will be irradiated; adequate consideration should be given to the determination and substantiation of transfer functions between the testing conditions and the operational environment.

6. DETAILED RESEARCH: EXPLORATION OF BUILT-IN SEE MITIGATION TECHNIQUES

6.1 INTRODUCTION

Based on the compendium of mitigation techniques for SEE applicable to avionics systems, this research focuses on the next step of the SEE analysis methodology currently being drafted (i.e., the qualitative and quantitative SEE assessment and applying it to built-in mitigation techniques).

Memory elements have been chosen as the example for this investigation. These elements are part of FPGAs and ASICs used in avionics components that are SEE-sensitive. While demonstrating how to derive the reliability information for these elements using manufacturer data, the report places—in the context of an FPGA and ASIC—how the built-in technique is complemented with the non-built in technique investigated in the previous report. The tradeoff space for the designer is spanned across built-in and not-built-in techniques as they both apply to a single application.

Memory elements are sensitive to SEE, primarily to SEU, and, when unprotected, are the major contributors to a shift chain aggregated SEU cross-section. Protection against SEE can be part of the memory cell design itself (i.e., RHBD cell), built-in in the form of ECC, or not built-in in the form of redundancy. When penalties and benefits of each strategy are balanced for a given target application, the end result is typically a combination of all of the above.

The technology scaling trend has generated a noticeable increase in the occurrence of MBUs or MCUs against which the classic single error correction and double error detection (SEC-DED) ECCs are powerless and against which redundancy solutions are limited. Complementary mitigation is required and can take several forms, such as bit-interleaving, use of scrubbing with golden configuration, or more powerful ECCs. Moreover, the increased switching speed required for some applications has led to the more frequent occurrence of non-recoverable errors or SHEs due to damage to the substrate. These errors need to be mitigated at the circuit design level—for example by implementing multiple copies of the data chains using resources (e.g., memory cells, logic) implanted on diversified areas of the circuit.

The measurement of the effectiveness of the mitigation strategies is done via radiation testing using a combination of static and dynamic tests. To extrapolate the results from testing, analytical expressions exist for certain classes of ECCs. The designer can select key performance indicators with analytical expressions, such as mean time between errors (MTBE) or mean time to repair (MTTR), to substantiate his mitigation strategy.

This section is organized mainly around the major phases of the SEE safety analysis preparation of the SSA.

6.2 BUILT-IN MITIGATION TECHNIQUE

For this research, the focus is on built-in mitigation techniques for hardening the integrated circuit and, in particular, the memory cells against SEUs. Aerospace applications use ASIC boards to limit the natural flexibility of the FPGA, so the investigation will focus on FPGA technology for which an ASIC target exists.

Boeing conducted a detailed investigation of hardening techniques for a commercial-grade 90 nm ASIC cell to conclude on some of the complex considerations at play in deciding how to implement these techniques as a function of the target device (e.g., FFs, logic paths, clocks) [87]. This analysis is complemented by the assessment at the device level of the FIT for different types of memory elements.

6.2.1 Context

Recall the analysis steps preceding the risk assessment of the device:

- The system in which the device is installed has been tagged as SEE-sensitive for effects, including SEU.
- A target for reliability at the system level has been determined (e.g., provided by the airframer.
- Sensitive areas on the device have been identified. Typically, these areas include FFs, combinatorial logic, and clocks.
- Reliability information has been collected from semiconductor manufacturer datasheets, radiation testing, etc.

The selected built-in technique for this investigation is ECC. The technique is applied to memory elements either unhardened or on top of RHBD. The most commonly used ECC for embedded memory elements is SEC-DED Hamming [88] and/or Hsiao [89] codes. These codes are able to detect and correct one single bit error in a word or detect, but not correct, two single bit errors in a word. Their advantages include a relatively simple implementation with minimum area and latency penalties.

The Jet Propulsion Laboratory pointed out that MBUs need to be considered for DSM process technologies, such as the ones found in FPGA manufacturing. As an example, the likelihood of occurrence of MBU in the Xilinx Virtex-4 90 nm technology is approximately three times more likely than for the Virtex-II 130 nm technology and 69 times more likely than for the Virtex 220 nm technology [90].

Finally, scaling and increased switching speed contribute to faster aging of the substrate, which can translate into an increase of the proportion of SHE within the occurrences of SEUs. If the aging component is not taken into account, the FIT value may be underevaluated.

As a conclusion, SEU considerations for memory elements shall include single-bit and multiple-bit upsets as well as single hardware events.

6.2.2 General Assumptions

The most basic assumption is that the storage elements in the device being assessed are partitioned into groups. These groups are called words or frames. The bits within these words/frames are susceptible to SEUs, resulting in a flip of the bit stored value or bit-flip.

An EDAC scheme will define time periods (or cycles) for the entire time the device is operating. Once per cycle, the EDAC scheme will read the content of each bit and determine whether a flip has occurred. Moreover, if the scheme belongs to the most common SEC-DED class and it is determined that there has been not more than one bit-flip per word/frame, the EDAC will correct the bit-flip. If the scheme determines there has been more than one bit-flip per word, the function of the EDAC scheme is unpredictable, but the assumption is made that these flips are never corrected.

6.2.3 Assessment of Mitigation Effectiveness of 65 nm Technology FPGA

The SRAM FPGAs are composed of configurable logic blocks (CLBs) surrounded by programmable I/O blocks interconnected by programmable routing resources. The CLB contain LUTs, multiplexors, and FFs. Once programmed, the functionality of the FPGA building blocks is contained in the CLB.

6.2.3.1 Identification of Risk Areas

For sensitivity to SEU, the focus must be on all areas that contain memory storage elements and on the identification of the use of the storage (e.g., static, read-only, read/write, user-programmable). Such an assessment of the Virtex-5 FPGA family leads to the identification of four components:

1. FF (in the CLB): these memory cells contained in the configurable CLB are used for the user logic
2. LUT RAM (in the CLB): these memory elements are distributed register files or RAM built out of the CLB LUT and are used for user logic
3. BRAM: this refers to the embedded memory blocks for the user logic
4. Configuration memory: these cells store the configuration for the FPGA (e.g., routing information, logic path structure)

6.2.3.2 The EDAC Scheme Architecture

The EDAC scheme protects each of the BRAMs configurable as 512 x 64-bit RAM, with an 8-bit ECC for every 64-bit word. The 8-bit ECC is a parity checksum [ECCPARITY] generated and stored during each write operation and used during every read operation to either:

- Detect and correct single-bit errors.
- Detect but not correct double-bit errors.

For every word read, the 72 bits are fed into an ECC [decode and correct] ,which generates two status outputs [DBITERR and SBITERR] indicating either:

- No error.
- Single-bit error detected and corrected.
- Double-bit error detected.

Finally, the corrected data are presented on the data output [DO]. Figure 35 depicts the implementation of the ECC on Virtex-5 BRAMs.

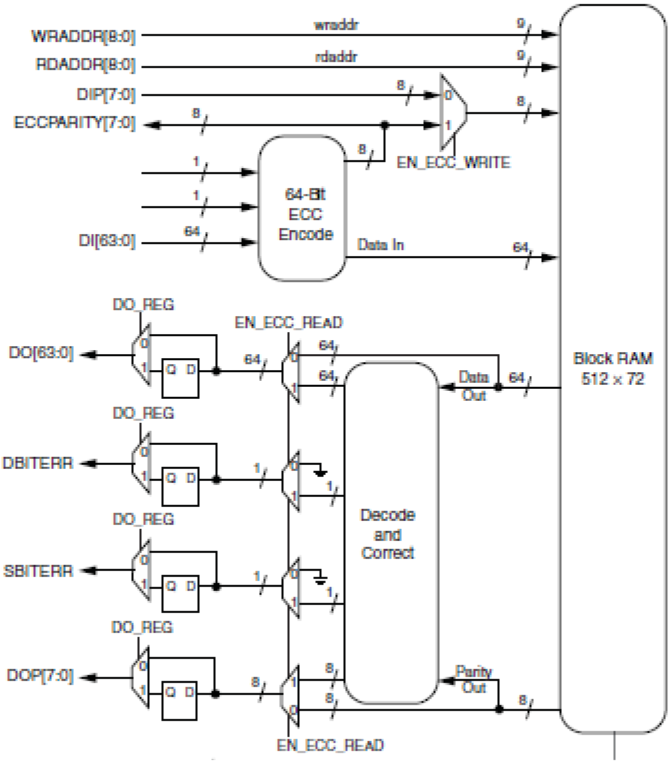


Figure 35. High-level view of ECC implementation on Virtex-5® BRAM

6.2.3.3 Xilinx Virtex-5 Example Assessment Using FIT

For this example, consider a Xilinx® Virtex-5® FPGA with part number XC5VLX50 (see appendix A for complete description of static memory content for Virtex-5 implementations). The following sections assess each of the relevant elements: FFs, LUT RAM, BRAM, and configuration memory.

6.2.3.3.1 FFs in the CLB

The manufacturer datasheet for these elements refers to a FIT rate between 1 FIT/Mb and 2 FIT/Mb, with a 95% confidence interval. The information was derived from accelerated testing under a neutron beam at sea level. Table 35 summarizes the elements supporting the analysis to obtain reliability numbers for the CLB FFs.

Table 35. Reliability analysis for CLB FFs in Virtex-5 device

Characteristics	Numeric Value or Interval
FIT	1 failure per 10^9 hours or per 114,155 years
FF in CLB FIT rate (95%)	*FITR* = 1 FIT/Mb to 2 FIT/Mb (sea level)
Number of implemented FFs in FPGA	*N* = 28,800 bits or 0.03Mb
FPGA level FIT	*N* x *FITR* = 0.03 to 0.06 FIT (sea level)
FPGA MTBF at sea level	$MTBF = \frac{10^9}{N \times FITR}$ =16.7x10^9 to 33.3x10^9 hours
	$MTBF = \frac{114{,}155}{N \times FITR}$ =1.9 to 3.8 million years

Between the small number of FFs implemented in the CLB and the MTBF values, these FF contributions to the risk assessment are negligible. There is no need to factor in derating for altitude/latitude and critical bits in the refinement of the analysis.

6.2.3.3.2 Distributed or LUT RAM

The CLB in the Virtex-5 device implements both SLICEL and SLICEM slices. The LUTs in the SLICEM slices can implement a synchronous distributed RAM or 32-bit shift register without using the FFs available in the slice. In this design, the write controls for the LUTs are passed from the FPGA configuration interface to the user design. During normal operation, the contents of the LUT RAM are changed from their initial values contained in the configuration memory.

The traditional scheme to mitigate SEU in configuration memory implies that any correction for an SEU causes the user content of the LUT RAM to be overwritten with the initial content from the configuration memory. In the Virtex-5 device, there is an option to prevent the user content in the LUTs to be overwritten in the form of a configuration option to be set. When the option is selected, an SEU in the bits of the user content in the distributed RAM is mitigated in the user-design.

When performing the mitigation effectiveness assessment, the user should be aware of how the built-in data error and correction schemes are implemented and decide how to implement the mitigation in the user-design or to avoid the use of these schemes.

6.2.3.3.3 Embedded BRAM

The Virtex-5 device employs large amounts of bulk RAM as 36 Kb dual-port RAM (a.k.a., BRAM) arranged in columns. Each block can further be split into two independently controlled 18Kb RAMs. BRAMs are more susceptible to SEU than CLB FFs and configuration memory because of the required speed performance of these cells (Xilinx's Rosetta experiment reports up to five times the susceptibility compared to configuration memory).

The traditional mitigation scheme for BRAMs is the implementation of an ECC. This technique is built in and operates in full transparence for the user. However, the configuration of the ECC is accessible to the user [91].

In addition to the ECC, the BRAM words are implemented with an interleaved bit separation scheme so that every bit in the word is in a separate BRAM.

6.2.3.3.4 Configuration Memory

The configuration memory in the Virtex-5 device is formatted using application-specific data through the configuration interface. These data typically include bits to set the configuration for each LUT and FF, the routing connections, etc. Compared to the BRAMs, these cells are expected to be less sensitive because they should remain static. The risk is not from the use of the memory cells but from the large amount on the device. Indeed, configuration memory is the single largest group of static RAM (e.g., four to six times the number of BRAM bits).

Despite the large volume of memory cells, the SEU impact is limited by two factors: the number of critical bits and the number of unused cells. Critical bits are defined as bits that affect the design. In one acceptation of critical bits, they can be equated to the bits being used. On any of the Virtex-5 designs, the number of critical bits is defined based on usage and is limited (typically less than 10%, but it can rise up to 20%).

The risk analysis would proceed according to the steps in table 36 for a conservative analysis.

Table 36. Reliability analysis for configuration memory in Virtex-5 device (conservative)

Characteristics	Numeric Value or Interval
FIT	1 failure per 10^9 hours or per 114,155 years
Configuration memory FIT rate (95%)	*FITR* = 101 to 215 FIT/Mb (sea level)
Number of configuration bits	*N* = 10,541,440 bits or 10.54 Mb
FPGA level FIT	*N* x *FITR* = 1,064 to 2,266 FIT (sea level)
FPGA MTBF at sea level	$MTBF = \frac{10^9}{N \times FITR}$ = 0.44 x 10^9 to 0.94x10^9 hours
	$MTBF = \frac{114{,}155}{N \times FITR}$ = 50.4 to 107.3 years
Derating factor for latitude and altitude (from Xilinx's Rosetta experiment)	*DF*= 561.7 (worst case for commercial aviation)
FPGA derated MTBF	$MTBF_D = \frac{MTBF \times 12}{DF}$ = 1.08 to 2.29 months

This analysis can be considered overly conservative because it does not take into account the limited number of configuration cells in use or the percentage of critical bits. If we consider the number of configuration bits actually used in the design to be between 10% and 20%, the rates above can be improved by a factor of at least 5 (see table 37).

Table 37. Reliability analysis for configuration memory in Virtex-5 device (critical bits)

Characteristics	Numeric Value or Interval
FIT	1 failure per 10^9 hours or per 114,155 years
Configuration memory FIT rate (95%)	$FITR$ = 101 to 215 FIT/Mb (sea level)
Number of configuration bits	N = 10,541,440 bits or 10.54 Mb
Number of critical configuration bits (usage-based)	$N_c = 0.1N$ (10% use) to $N_c = 0.2N$ (20% use)
FPGA level FIT	N x $FITR$ = 1,064 to 2,266 FIT (sea level) N_c x $FITR$ = 106–227 FIT (10%) or 213–453 FIT (20%)
FPGA MTBF at sea level	$MTBF = \frac{10^9}{N_c \times FITR}$ = 4.4 x 10^6 to 9.4 x 10^6 hours (10%) $MTBF = \frac{10^9}{N_c \times FITR}$ = 2.2 x 10^6 to 4.7 x 10^6 hours (20%)
	$MTBF = \frac{114{,}155}{N_c \times FITR}$ = 503 to 1,077 years (10%) $MTBF = \frac{114{,}155}{N_c \times FITR}$ = 252 to 536 years (20%)
Derating for latitude and altitude (from Xilinx's Rosetta experiment)	DF = 561.7 (worst case for commercial aviation)
FPGA derated MTBF	$MTBF_D = \frac{MTBF \times 12}{DF}$ = 10.8 to 22.9 months (10%) $MTBF_D = \frac{MTBF \times 12}{DF}$ = 5.4 to 11.45 months (20%)

However, even with the conservative approach, the MTBF exceeds the longest duration of a commercial flight (it takes 24 hours as an upper bound) by order of magnitude. In addition, the system power cycling eliminates most uncorrected SEUs. Therefore, the issue of SEU is to be considered not for a single flight but for all devices in flight on a given day.

6.2.3.4 Xilinx Virtex-5 QV Example Assessment of EDAC

The Virtex-5 QV is a 65 nm technology space-grade variation of the Virtex-5. It is also known as the single event immune reconfigurable FPGA (SIRF). In the XQR5VFX130 reference, the logic cells, CLB-FF, and distributed RAM are RHBD; the BRAMs are unhardened but protected with an EDAC scheme. Table 38 summarizes the relevant features of the SIRF.

Table 38. Feature set for Xilinx Virtex-5 QV (XQR5VFX130)

Feature Element	Number of Elements	SEU mitigation scheme
Logic cells	131,072	RHDB
LUTs and CLB-FF	81,920	RHDB
Distributed RAM	1,580 kBits	RHDB
RAM blocks (36 kBits)	296	EDAC
Total RAM blocks	10,368 kBits	EDAC
Clock tiles	6	none
DSP48E slices	320	none
MGT-GTX channels	18	none
PCI express blocks	3	none
Ethernet MACs	6	none
User I/O	836	none

The EDAC assessment was performed subjecting the Virtex-5 QV device to heavy ions and protons to acquire statistics during both static and dynamic tests (see section 6.3.2). The objective was twofold:

- Collect enough statistical data to validate an analytical expression for the EDAC error at word level (see section 6.3.1.1).
- Observe the impact of the EDAC circuitry on the cross-section (see section 6.3.4.3).

6.2.4 Assessment of Mitigation Effectiveness on 90 nm Technology ASIC

The proposed example is an ASIC developed by the Boeing Satellite Development Center in IBM’s 90 nm CMOS technology [87] composed of 140 1024 bit-long shift chains. The shift chains are implemented using different strategies to support a comparative assessment of the effectiveness of built-in and not-built-in mitigations:

- Eight types of FFs: unhardened, hardened with TMR voters (using AND-OR, NAND, and 3-input voters), and DICE with varied well/node spacing characteristics
- Three types of combinatorial logic between FFs to characterize SET sensitivity: BUFFER (back-to-back inverters), NOR2, and NAND2 gates

6.2.4.1 Identification of Risk Areas

Within a standard ASIC design flow, three circuitry types are sensitive to SEE:

- The clock

- The FFs
- The combinatorial logic

Each of these elements is sensitive in its own way, such that their contribution to the ASIC overall cross-section is varied. Consider for example the sensitivity to SET: the clock can be affected anytime, the combinatorial logic is sensitive only during the setup and hold-time of the FFs, and the FFs are vulnerable at any point with an error appearing at the next clock cycle.

6.2.4.2 SEU Cross-Section Assessment

The contributions of the three sensitive elements to the overall chain SEU cross-section σ are assumed to be independent. This assumption is deemed reasonable based on the fact that the FF storage nodes are isolated by a built-in inverter and the gate capacitance of the transistors in the combinatorial logic is not affecting the capacitance on the FF storage nodes. Therefore:

$$\sigma_{chain} = \sigma_{FF} + \sigma_{CLK} + \sigma_{Logic} \tag{7}$$

The test plan is defined so that each of the contributions can be isolated based on the varied implementations in the chains. A simple average of the measured cross-sections over several test runs is used to determine the final contribution of each element.

6.2.4.2.1 FF Sensitivity

The sensitivity is determined by testing chains with no combinatorial logic between FFs ($\sigma_{Logic} = 0$) using the constant value of input (SEU in the clock has no effect). Figure 36 shows the test results for the comparison of cross-sections contributed by unhardened FFs (LMX), DICE-hardened FFs, and TMR-hardened FFs [87].

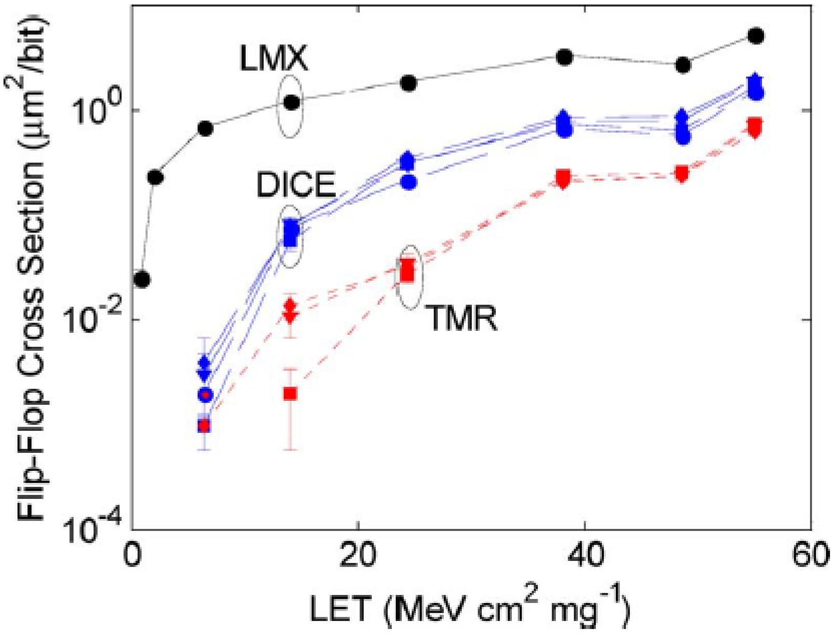


Figure 36. Comparison of SEU cross-sections for unhardened and hardened FFs

The unhardened FF (LMX) is the most sensitive with the highest cross-section, regardless of the energy level, followed by the DICE cells, regardless of well/contact spacing options. Finally, the TMR-voted design presents the least sensitivity to SEU. There is approximately a one order of magnitude gain with the DICE design and two with the TMR-voted compared to the unhardened baseline.

6.2.4.2.2 Clock Sensitivity

The sensitivity is determined by testing chains with no combinatorial logic between FFs ($\sigma_{Logic} = 0$) using a dynamic pattern of '0' and '1' input. This captures both σ_{FF} and σ_{CLK}, the latter of which is obtained after subtraction of the FF sensitivity previously obtained. Figure 37 shows the cross-sections for the entire chain and its elements: clock, unhardened FFs (LMX), and BUFFER-type combinatorial logic implemented between FFs [87].

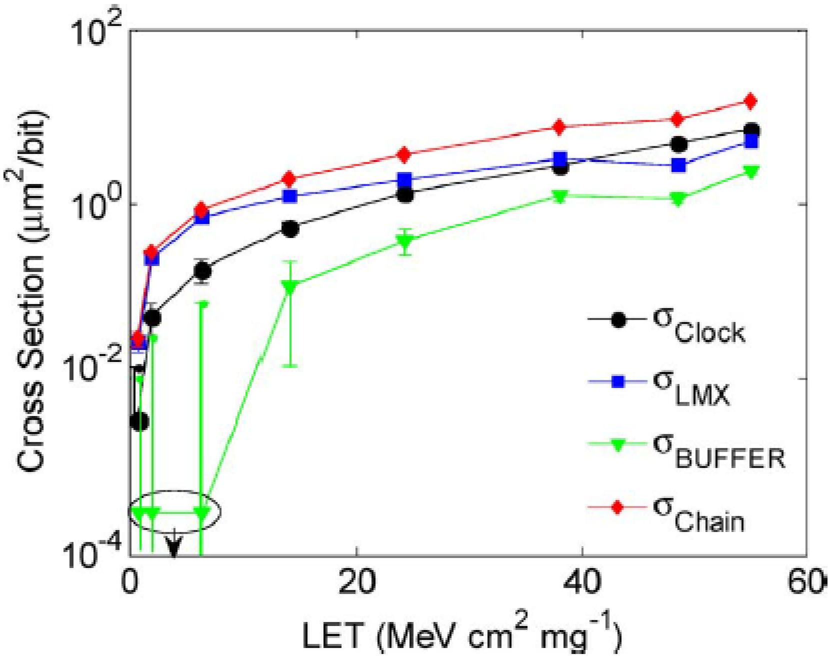


Figure 37. Contribution of clock to the chain SEU sensitivity

As a relative comparison, the clock contribution is close to that of unhardened FFs and becomes dominant for higher LETs (LET > 40MeV.cm^2.mg^{-1}).

6.2.4.2.3 Combinatorial Logic Sensitivity

The sensitivity is determined by testing chains with combinatorial logic between FFs using a constant value of input. This captures both σ_{FF} and σ_{Logic}, the latter of which is obtained after subtraction of the FF sensitivity previously obtained. This value can be considered a worst-case because, in a real design, not all SET would propagate—some would be blocked by logic constructs. Figure 38 shows the comparison of SEU cross-sections for the three types of combinatorial logic implemented on the ASIC: BUFFER, NAND gates, and NOR gates [87]. The BUFFER implementation is the most sensitive and the NAND implementation is the least.

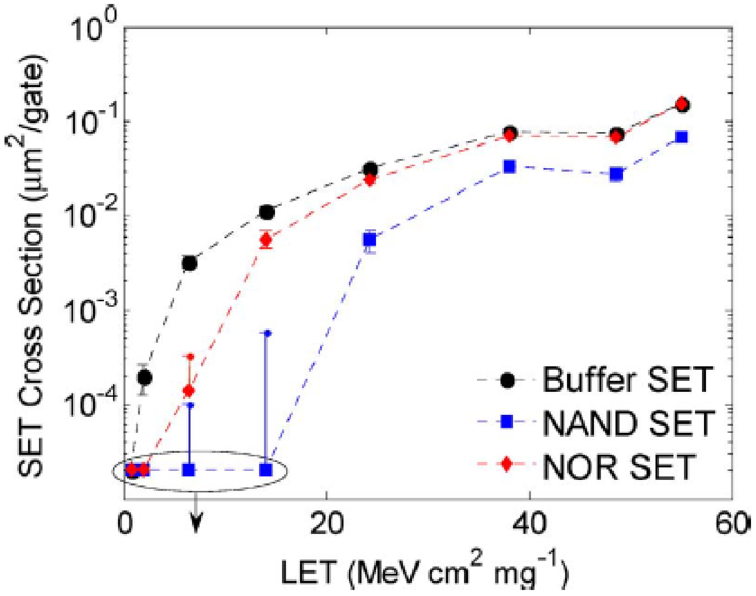


Figure 38. Comparison of SEU cross-sections for BUFFER, NAND, and NOR logic

The relatively smaller cross-section of the NAND implementation is explained by the use of wider transistors, whose drive strength overcomes the resistance from the serial connection and allows the energy from a neutron strike to be dissipated faster.

6.2.4.2.4 Aggregated Cross-Section at the Chain Level

To understand how the elemental sensitivities play at the shift chain level, consider the composite graphs in figure 39 [87]. On the left side, the chain contains unhardened FF, whereas on the right, the chain is implemented using TMR-voted FFs.

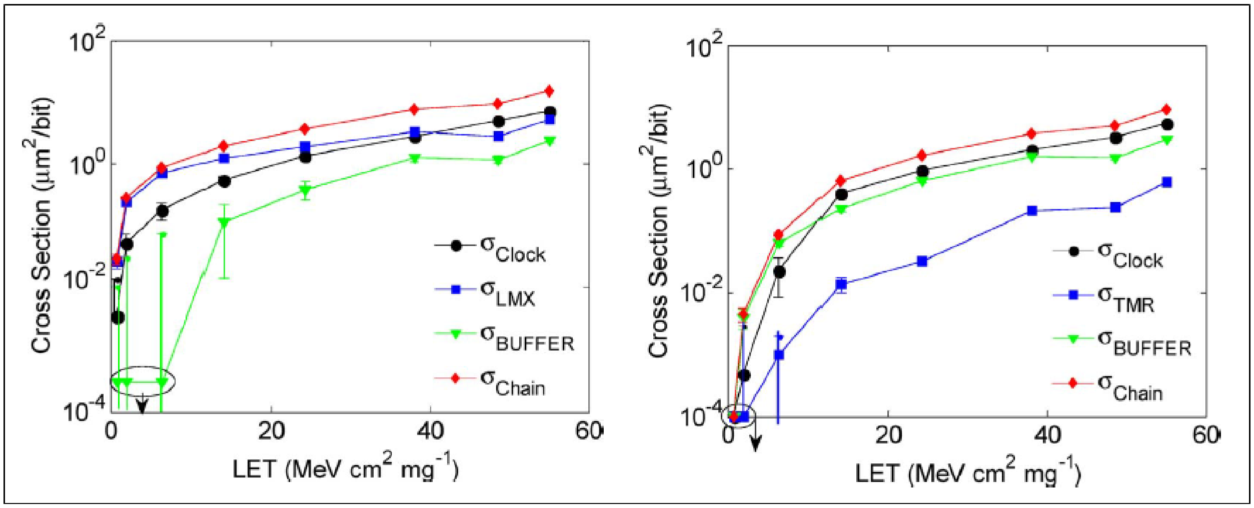


Figure 39. Aggregated SEU cross-sections with unhardened and TMR-hardened FFs

The implementation of TMR mitigation on the FFs changes the relative influence of each element to the chain cross-section. By design, the FF component no longer dominates, the logic element is the main driver at lower LET (LET < $10\text{MeV.cm}^2.\text{mg}^{-1}$), and the clock drives the cross-section at higher LET. Second, the clock component cross-section is lower with the TMR design than with the unhardened implementation. This can be attributed to the larger clock buffer structure necessary to drive the triplicated FFs in the TMR architecture.

Finally, the aggregated cross-section for the chain remains unchanged, which supports the hypothesis that the total cross-section can be built from its identified sensitive components.

6.2.5 Issues

6.2.5.1 Limitations in Upset Rate Calculation Tools

Current hardening strategies and upset rate calculation tools do not account for all effects, including:

- Angular asymmetries in the sensitive volume cross-section.
- Nuclear reactions between heavy ions and the metallization layers of the chip.

6.2.5.2 Increase in Multi-Bit Upsets for Mitigated SRAM

DSM technologies are more likely to experience MBUs. Because these upsets may affect multiple redundant modules and because multiple bit-flips cannot be corrected by SEC-DED ECCs, neither redundancy (e.g., TMR) nor read-back with correction techniques address the MBU issue. The following sections briefly present strategies to address the issue of MBUs.

6.2.5.2.1 Layout-Based Technique: Bit Interleaving

Triple-well is a commonly used hardening technique used to reduce the single bit failure rate in thin SRAM cells (e.g. 65 nm, 90 nm). A collateral effect, known as “battery effect,” has been shown to increase the multi-bit failure rate by a factor of 10 [92]. This effect depends on the p-well architecture of the cell when the memory pattern is ‘1’. Mitigation for this effect includes the relaxation of the ECC design guidelines down to the simplest bit interleaving with the smallest available column multiplexer.

6.2.5.2.2 Scrubbing Technique: Gold Configuration

The NASA Glenn radiation effects and analysis group developed a scrubber capable of mitigating MBU by using so-called gold configuration stored outside of the FPGA and used to periodically refresh the configuration, regardless of whether or not upsets have occurred [93]. This technique is intrusive and has an impact on the FPGA CLBs, where the user-design is stored. In a worst-case scenario, the correct value specified by the user could be overwritten.

A similar architecture is proposed in reference [94], in which the golden backup memory is stored on a device less sensitive to SEU, such as ROM on or off the chip. In addition, the EDAC circuit is inserted between the configuration memory and the reconfigurable logic device. When one or two errors are produced in the configuration memory block, the EDAC exports corrected values to the reconfiguration device. The other advantage of this structure is its ability to increase the dependability performance compared to a classic TMR structure and the ability to instantly correct errors.

6.2.5.2.3 Development of More Powerful ECCs for MBUs

Powerful ECCs developed to address the issue of MBUs include Bose-Chaudhuri-Hocquenghem (BCH) code [95] and Euclidian geometry code [96]. However, they bring a significantly higher latency and area penalty compared to SEC-DED codes because of the required large number of check-bits.

6.2.5.2.4 Improvement of SEC-DED Codes to Address MBUs

Improvement to SEC-DED codes includes selective cycle avoidance [97] and bit placement [98] codes. These improvements to classic SEC-DED extend the capability to double adjacent error correction (DAEC) or triple adjacent error detection without changing the bit overhead. The main issue with these is the introduction of the potential for misinterpreting non-adjacent errors as adjacent ones (i.e., a probability of miscorrection).

The next logical step is to reduce the probability of miscorrection. In reference [99], a new scheme is proposed that extends the basic SEC-DED coverage to DAEC with scalable adjacent error detection (*x*AED) while reducing the probability of miscorrection for adjacent/non-adjacent double-bit errors. The approach is to investigate the check-bit design space because it is the culprit of the more powerful BCH codes and is directly related to the *x*AED capability and miscorrection probability. As an example, a code is developed that uses the same number of check-bits as the classic SEC-DED codes but provides DAEC-TAEC. That is orthogonal to and independent of interleaving.

6.2.5.3 Handling of MCU

The semiconductor technology scaling results in an increased bit-cell density; a direct consequence is the increase of the likelihood that a single particle strike upsets multiple adjacent cells. MCUs are typically addressed by using bit interleaving (see also section 6.2.5.2.1), whereby the bits of multiple memory words are physically distributed (e.g., interleaved throughout a memory row). Interleaving breaks an upset that is beyond the capability of an ECC into multiple smaller upsets that can be handled individually. For example, a physical MCU can be converted into multiple logical single-cell upsets.

The caveat is that there are limits to the implementation of interleaving, mainly dictated by the memory area, performance, and aspect ratio. Interleaving increases the routing complexity, which translates into increased area and latency. For small memories for which there is a tight coupling of the cells and comparison circuit hardware structures, such as CAM, interleaving is not practicable and other methods need to be applied to mitigate the upsets. These methods are ECC schemes that take advantage of substrate and design engineering to limit the number of parity-bits [100].

6.2.5.4 Handling of Single Hardware Error (SHE)

Contrary to SEUs and MBUs, SHEs are not recoverable. The simplest way to address detected SHEs is to avoid using the damaged resources [101]. More advanced techniques are designed to take full advantage of the reconfigurability of the FPGA by adapting the system around the damaged substrate at runtime. However, these techniques have not (to date) been successfully demonstrated for complex systems and present a major latency or unavailability impact because of the time required to run the system reconfiguration [102].

6.3 TESTING CONSIDERATIONS

6.3.1 Modeling and Experimental Methods to Assess EDAC Mitigation

Methodologies used to quantify the failure of EDAC mitigation schemes have been developed primarily for the space environment. They measure EDAC effectiveness by counting failures as a function of the raw bit-flip rate and the scrubbing time (or word refresh time).

6.3.1.1 Modeling of EDAC Failure Rates

Modeling is required to extrapolate the EDAC failure rates. As an example, reference [103] proposes the following theoretical model

$$EWER = \frac{1}{2} T_C N_W N_{BW} \left(N_{BW} - 1 \right) R_{BF}^2 , \tag{8}$$

Where EWER stands for the EDAC word error (EWE) rate, T_C the cycle time for refresh/scrubbing, N_W the total number of words, N_{BW} the number of bits in the word, and R_{BF} the per-bit flip rate. The per-bit flip rate is the product of two measurements: the per-bit cross-section σ_B and the ion flux. For a given environment, σ_B is measured as a function of the effective LET selected by the test engineer and static cross-section. Typically, a Weibull fit can be used to interpolate between the discrete measurements.

The derivation of the model can be found in the appendix of reference [103].

6.3.1.2 Supporting Measurements

The ion flux has a direct impact on the EDAC failure rate through the per-bit flip rate. It is therefore important to measure the instantaneous flux available at the test facility. An instantaneous flux increase may generate the majority of the EWEs, while having less impact on the averaged value over the run. It is up to the test plan to address flux variations either through the provision of error bars with the results or the discarding of any event that occurred during the flux variation.

Finally, the effective LET for the per-bit cross-section estimation should be chosen from the saturated region of the static cross-section; the corresponding flip-bit rate will be less sensitive to LET variations; moreover, higher LET ions increase the probability of occurrence of MBUs, thus corresponding to a worst-case value for the EWER.

6.3.1.3 Model Assumptions and Limitations

The bit-flips are assumed to be independent in the statistical sense. As a consequence, multiple bit-flips are assumed to have been created by multiple particle hits. The possibility that a single particle hit generates several bit-flips is not directly addressed by the proposed model.

The second major assumption concerns the environment. As indicated in section 6.3.1.1, the environment is considered given; therefore, its variation or uncertainty are not reflected in the output probabilities. The objective is to use measurement data from the given environment and the device SEU cross-section to compute two probabilities:

1. That one or more EWE occurs during a user-specified time in which the device is operating.

2. The EWER as a statistical average over at least a cycle during which the environment is constant. The definition of the averaging period is application-dependent (e.g., an orbit for a satellite) and will provide different results for different values based on the environment variations within the averaging period (e.g., overfly of south Atlantic anomaly).

6.3.2 Types of Tests

The literature agrees on two types of tests, both needed to characterize the effectiveness of the mitigation technique in a statistical manner: static tests and dynamic tests. However, the definition of these tests varies.

6.3.2.1 Static Tests

The static tests are usually described as one of the following two setups:

1. Data are recorded on the device, the device is irradiated, data are read out. For example, memory elements are programmed with all ones, or all zeroes, or a checkerboard pattern. Then the elements are submitted to the irradiation until a statistically significant number of events is generated. During the entire test run, the memory elements are un-clocked. When the test run is completed, the memory elements are read and the errors counted.

2. A constant value of input data is continuously read by the device during irradiation. The contents of the memory elements are continuously read back and the errors logged.

6.3.2.2 Dynamic Tests

Dynamic tests are in general defined as:

A varying sequence of input data is continuously read by the device during irradiation. The dynamic sequence can follow various patterns of zeroes and ones.

Note: static test setup number 2 with a patterned input sequence (e.g., checkerboard) is equivalent to the definition of the dynamic test above.

6.3.3 Definition of Errors and Failures

In the literature, the definition of error and failure varies according to the specific area analyzed. The following paragraphs provide the background for the use of these terms within this report.

An error is defined as the deviation from the correct state. When an error is produced, the fault at its source (e.g., SEU, MBU, SHE) is active; otherwise, it is called dormant.

When two or more bit-flips are detected, the EDAC behavior is unpredictable but it is assumed that the bit-flips are never corrected. The occurrence of uncorrected bit-flips in a cycle is called a EWE.

Whereas the bit-level error is easy to define as a bit-flip, a system level error might be defined differently. In reference [103], the system-level error is defined as the detection of two SEUs in a single word or an anomalous failure in the EDAC system. In reference [102], the system-level error is defined as an error that propagated to the system output and caused a deviation at the service level.

6.3.4 Limitations of Experimental Methods

6.3.4.1 Impact of TID on SEU Results

During extended testing periods, the TID needs to be monitored and compared to a-priori estimation of the TID limit (e.g., from tests on similar technologies with the addition of a margin to take into account charge recombination). The leakage of the circuit needs to be monitored to ensure that the TID degradation is not confounding the SEU results. If there is a doubt, test runs should be redone.

6.3.4.2 Considerations on Beam Penetration

The testing needs to ensure that all ions have sufficient range to range the identified sensitive areas. If testing includes variation in the incidence angle of the beam, then the ions should have enough range to reach the sensitive areas under all angles. This consideration may require modification to the packaging for testing (e.g., removing lid) or substrate (e.g., thinning) which modify the DUT compared to the device in real operational conditions.

6.3.4.3 Impact of the EDAC Circuitry

The ECC decode, correct element, and ECC control logic are unhardened. When test results are compared to the modeled system error rate (from equation 2), these unmitigated elements show as a deviation for low bit-flip rates as a function of the scrubbing rate. If the scrub period is on the order of a minute or less, the EDAC error rate can remain linear at a low flip-bit rate. A scrub period on the order of a minute and above will contribute to the total error rate. Figure 40 shows such an effect for the Xilinx Virtex-5 QV after heavy ion irradiation tests at the Texas A&M

cyclotron. The deviation from the linear model is clear for bit flip rates of 10^{-4} bit-errors/bit-second and below.

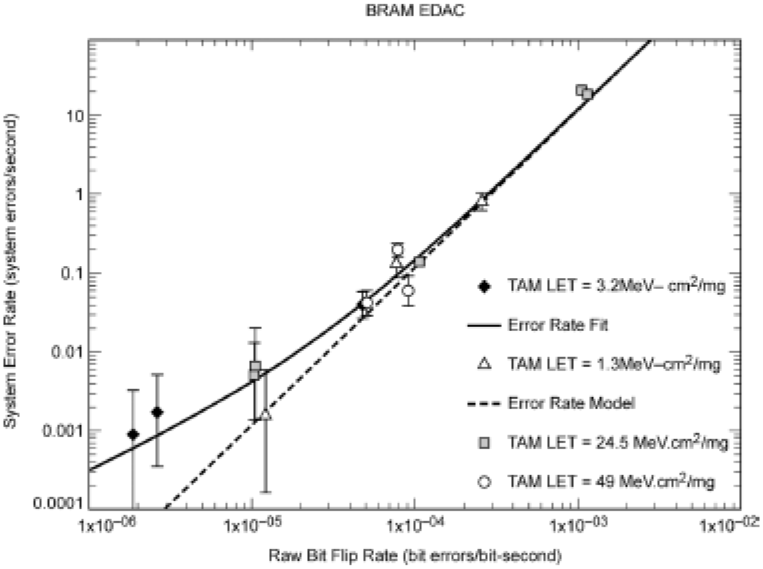


Figure 40. BRAM ECC system error rate per underlying upset rate [103]

To correct for the EDAC unmitigated circuitry impact, an equivalent number of unmitigated bits is found by adjusting the fitting parameters of the model (e.g., T_c, N_w, N_{WB}) to the test results. To give an order of magnitude, for the Xilinx Virtex-5 QV, this represents approximately 300 bits for 10,368 kbits of BRAM.

6.4 EXAMPLE FAULT HANDLING METHODOLOGY

The following is an example of fault handling strategy to address the issues of SEU, MBU, and SHE on SEE-sensitive memory elements applied to a Xilinx Virtex-4 FPGA [102]. The Virtex-4 FPGA family is based on 90 nm technology with 263 FIT/Mb (±11%) for the configuration memory and 484 FIT/Mb (±11%) for the BRAMs. The bitstream is composed of fixed-length configuration frames of 41 words, each spanning the height of a row. The configuration frames are of different types and in different quantity according to the type of logic resources:

- “00” for the I/O block, the CLBs, the vertical clocks, and the DSP48s
- “01” for the BRAM performing interconnection
- “10” for the BRAM holding content

Each frame is identifiable by its logic resource type, location on the top of bottom half of the device, row number, major column address, and minor intra-column address. This allows the addressing of every frame during the read-back process but also the physical identification of the location of a fault. Furthermore, each configuration frame is protected by a 12-bit SEC-DED Hamming code allocated in the 21st word (640–651 bit positions). Bits in the power of two positions are reserved for the ECC parity bits.

The key performance quantities addressed by the fault handling strategy are MTBE and MTTR.

6.4.1 System Failure Prevention

The system failure prevention mechanism aims at increasing the MTBE and is based on TMR. When a single error is detected, TMR masks the error while the correction action takes place. The majority voter allows for the identification of the element that is not in agreement and launches the scrubbing procedure before more errors can occur and cause the failure of the TMR architecture. Therefore, the key element is the voter, and it needs to be more robust to SEE than the basic SRAM-based configuration memory elements. One solution is to implement the voter asynchronously and use DSP48 blocks. The DSP48 blocks offer a greater robustness to SEE because they are built in to the device substratum.

Moreover, to reduce the likelihood that one faulted TMR module corrupts other modules, the spatial arrangement of the TMR structure has been planned separately. This specific placement allows mapping the TMR module with the bit position within the bitstream, so when a faulty bit is detected the impacted module is identified. Another advantage stems from the continuous reading of the configuration memory (i.e., preventive read-back) so that even when a detected single bit flip has not yet generated a fault (these faults are called dormant), the correction mechanism reverts the flip and rewrites the correct value in the memory.

Finally, MBUs are addressed via scrubbing of the affected frame and replacement of its content by the correct values stored in flash memory (gold configuration, see section 6.2.5.2.2).

If the system failure prevention actions above fail, there are two alternatives:

- The fault affects one TMR module and therefore should have been corrected by the above actions. It is likely that an SHE has occurred and an SHE recovery process should be initiated.
- This is a system malfunction and the content of the configuration memory should be protected from self-corruption. The interface to the gold configuration should be disabled (e.g., ICAP port, JTAG).

6.4.2 Module Error Correction

The module error correction aims at reducing the MTTR. When a fault becomes active, it generates an error that is instantaneously captured by the asynchronous voter that launches the recovery process. To maximize the time of correction, the first step is to address the most likely faults—SEU and MBU—and start reconfiguring the affected module with the correct configuration content in what is called “blind scrubbing.”

If the error is not corrected after this step, the next most likely diagnosis is an SHE. This requires the analysis of the module bitstream, also called “module-focused read-back,” to pinpoint the issue within a frame and identify, if possible, the position of the faulty bit.

Once the non-recoverable damage to the device has been located, a different module implementation is loaded in the TMR slot. Implementation diversity has been included in the design, whereby up to three different versions of each module exist and use logic resources in three out of the four quadrants in the device. It is therefore possible to select an implementation that does not use resources in the damaged area. If this is not possible, the TMR is degraded as only two modules are functioning.

6.4.3 Analytical Expressions, Decision Tree, and Fault Propagation

This section wraps up the fault handling strategy detailed in sections 6.4.1 and 6.4.2 . First, the analytical expressions are shown for the key performance quantities selected as MTBE and MTTR. Second, the strategy can be expressed in terms of a decision tree that progresses through the diagnosis and repair of SEU, MBU, and SHE (figure 41). Lastly, a fault propagation view is provided where the fault, when not mitigated, propagates from the bit/memory cell level to the system level (figure 42).

6.4.3.1 Analytical Expressions for MTBE and MTTR

To better understand how the strategies explained in the previous sections impact the MTTR and MTBE, consider the analytical expressions for MTTR

$$MTTR = N_f T_{WBf} \frac{FIT_{SEU+MBU}}{FIT_{SEU+MBU} + FIT_{SHE}} + \left(\frac{N_f}{2} T_{RBf} + N_f T_{WBf} \right) \frac{FIT_{SHE}}{FIT_{SEU+MBU} + FIT_{SHE}} \qquad (9)$$

and for MTBE

$$MTBE(h) = \frac{N_{fT}}{N_f} \left(\frac{10^9}{FIT_{SEU+MBU}} + \frac{4}{3} \frac{10^9}{FIT_{SHE}} \right) \frac{N_f T_{RBf}}{N_f T_{RBf} - 2MTTM}, \qquad (10)$$

Where:

$\frac{N_{fT}}{N_f}$	is the ratio of the total number of frame, N_f, and the number of frame that configure each TMR module, N_{fT}, and represent the spatial diversity element of the design
T_{RBf}	is the necessary time to read back a frame
T_{WBf}	is the necessary time to write a frame in the configuration memory when performing module partial reconfiguration (also includes time to access the flash memory when the golden configuration is stored)
$\frac{4}{3}$	represents the implementation diversity factor coming into play to mitigate SHE
$MTTM$	is the mean time to manifest (MTTM) errors and defined as the mean period of time a fault is dormant (this varies according to the functionality assigned to the faulty configuration bit)
$\frac{N_f T_{RBf}}{N_f T_{RBf} - 2MTTM}$	represents the probability that the fault turns active

For the Virtex-4 FPGA XC4VFX12 part in reference [102], numerical evaluation yields:

T_{RBf}	2,545	measured
T_{WBf}	5,077	measured
MTTM	5 clock ticks	measured
N_{fT}	3,848	manufacturer data
$FIT_{SEU+MBU}$	1,142	manufacturer data
FIT_{SHE}	30	manufacturer data
Mean time to detect an error	97.93 ms	measured

6.4.3.2 Decision Tree for SEU, MBU, and SHE Fault Handling

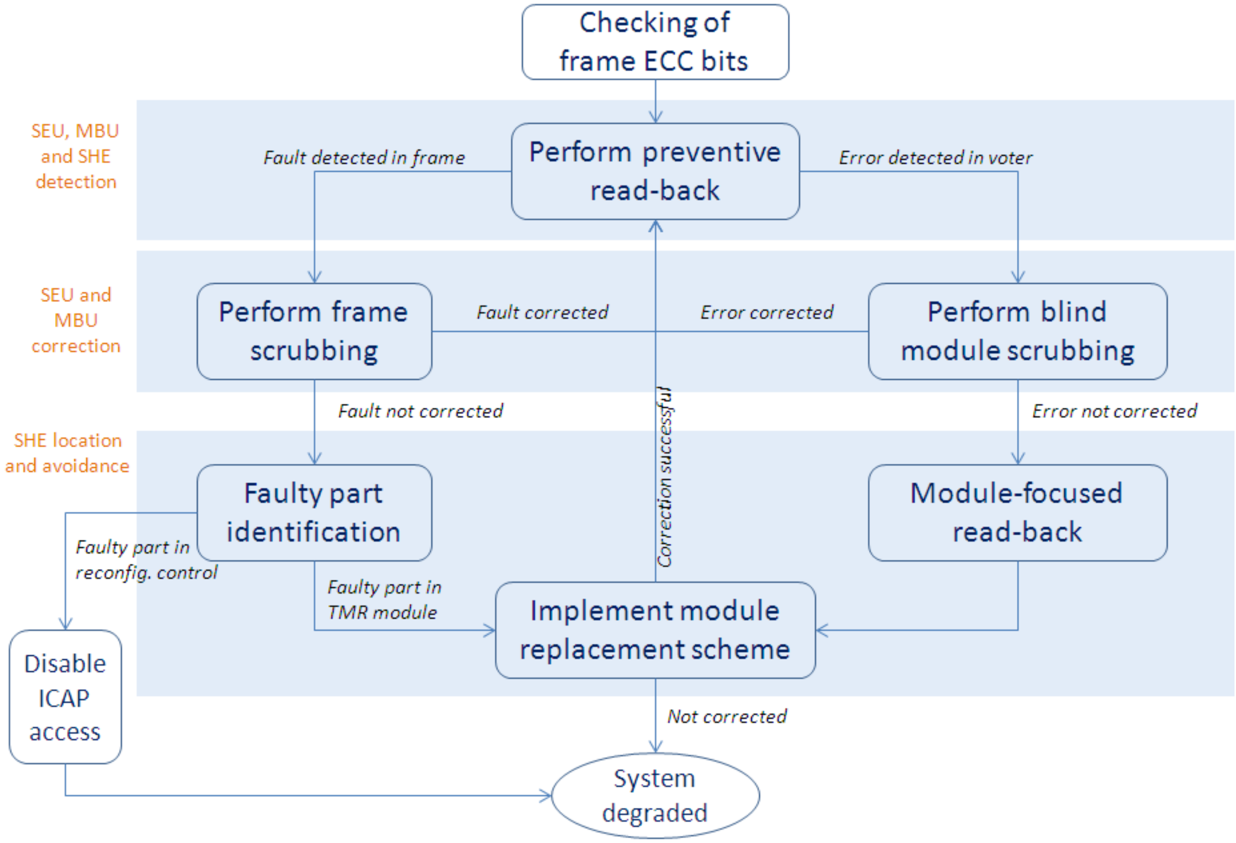

Checking of frame ECC bits
SEU, MBU and SHE detection
Fault detected in frame
Perform preventive read-back
Error detected in voter
SEU and MBU correction
Perform frame scrubbing
Fault corrected
Error corrected
Perform blind module scrubbing
Fault not corrected
Correction successful
Error not corrected
SHE location and avoidance
Faulty part identification
Module-focused read-back
Faulty part in reconfig. control
Faulty part in TMR module
Implement module replacement scheme
Disable ICAP access
Not corrected
System degraded

Figure 41. Flow diagram of the fault handling strategy for SEU, MBU, and SHE

The process starts with the reading of the ECC bits (e.g., parity bits) to detect errors. An error can be detected at two different levels: within a configuration frame (e.g., bit-flip) or within a TMR chain (the error is then detected at the voter level). If the error is detected in the frame, that frame is scrubbed before more errors can occur and defeat the mitigation techniques (both built-in and the TMR). If the error is in the TMR chain, blind scrubbing is performed on the TMR module to gain time in recovering. The underlying assumption is that there is a greater chance the error is of SEU or MBU type. After scrubbing, if the fault is not corrected, the diagnosis points to the occurrence of an SHE. This requires the identification of the impacted area, whether at the bitstream level or within the TMR module. If an SHE-impacted area is in the reconfiguration control of the device, the interface with the golden configuration must be disabled before the configuration self-corrupts and the system runs in a degraded mode. If the SHE-impacted area is in the TMR module, then a replacement scheme (e.g., based on the implementation diversity of multiple TMR modules) is engaged. If the replacement of the unrecoverable TMR chain is not possible with the replacement scheme, the TMR runs with only two modules (mitigation degraded) and the system is now in a degraded mode.

6.4.3.3 Fault Propagation Diagram

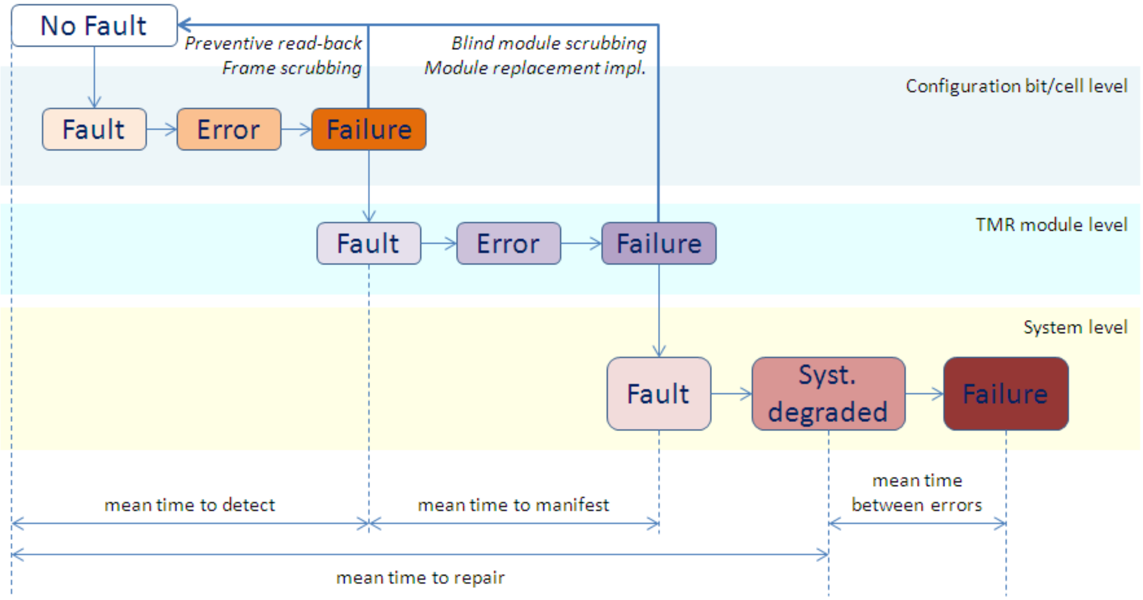


Figure 42. Identification of key elements in SEU, MBU, and SHE fault handling strategy

Figure 42 shows a fault propagation view of the process described in the previous section and introduces the visual representation of supplementary key performance indicators, such as mean time to detect and mean time to manifest. In this flow, a bit-level dormant fault eventually becomes active and, if not corrected by the frame scrubbing, generates a failure at the bit/memory cell level, which is now propagated to the TMR chain level as a fault. The voter detects the associated error and, if not corrected by the blind module scrubbing (e.g., SEU, MBU) or by the module replacement scheme (e.g., SHE), propagates to the system level as a fault. The system-level fault results in a degraded system that may, in time, fail.

6.5 CONCLUSION ON SEE MITIGATION TECHNIQUES FOR BUILT-IN SYSTEMS OR COMPONENTS

For this investigation, memory elements within avionics components have been selected. These elements are SEE-sensitive and their sensitivity is a function of their use (e.g., static memory, read-only, read/write, user-programmable) and the speed at which operations are performed on their content (the less operated on, the more robust to SEE).

FPGAs are an example of such SEE-sensitive components directly used in avionics or via an ASIC transformation. FPGAs are composed of CLBs surrounded by programmable I/O blocks interconnected by programmable routing resources. The areas to be mitigated for SEE include all components for the user logic (FFs, LUT RAM, and BRAM) and the configuration memory. From a device area perspective, the protection must include FFs, combinatorial logic, and clock.

These components are sensitive to SEU, which is typically mitigated by ECCs. With the scaling in technology, MCU and MBU have become noticeable and require more powerful ECCs and interleaving. In addition, because ECCs do not protect combinatorial logic, TMR needs to be implemented with scrubbing. More recently, SHEs have been noticed (faster aging is a byproduct of scaling and increased switching speed). Because SHE is not recoverable, mitigations target the avoidance of the damaged area until a replacement can be performed.

The sensitivity at the chain level is the sum of the sensitivity of each element: the FFs, combinatorial logic, and clock. The reduction of the sensitivity in one of the elements modifies the dominance of the others. The mitigation strategy may, therefore, be expressed for a single element (e.g., deciding to focus the mitigation on the FFs using TMR and leave the clock) or as a combination of measures on each (e.g., TMR on the FF and implementation of NOR gates on the logic).

Focusing on the memory element, which—if unmitigated—is the highest contributor to the SEU cross-section, the first trade space is on the ECC scheme. The most commonly used schemes are SEC-DED codes, which are limited to the detection of two bit-flip errors within a word (or frame) and can only correct a single bit-flip. Additional protection may take the form of:

- Selecting a hardened by design cell (this means changing manufacturer or part number).
- Scrubbing with a higher frequency that prevents the occurrence of bit-flips beyond the capability of the ECC (scrubbing frequency can be user-programmable).
- Opting for a more powerful ECC (typically, the ECC is attached to a device so it means changing manufacturer or part number).
- Implementing TMR.

TMR-protected FFs are more robust to SEE than RHDB cells by one order of magnitude and two compared to unhardened cells. The significant gain in robustness needs to be weighted against the x3 area penalty of the TMR and the manufacturing cost of a DICE cell. The major issues with more powerful ECCs are the bit overhead penalty (the increased number of check-bits not only translates into an area penalty but is also a source of increased latency) and the potential for miscorrecting non-adjacent errors.

Techniques to directly address MBUs include interleaving and scrubbing with a golden configuration. At a minimum, one bit interleaving is recommended. Interleaving introduces area penalty (to distribute the bits) and increases the routing complexity (generating latency). Moreover, when there is a strong coupling between the cells and comparison circuit hardware structures, such as in CAM, interleaving is not practical and mitigation techniques revert to ECCs. The scrubbing with golden configuration increases the dependability of the TMR because scrubbing is regularly performed whether or not errors have occurred (i.e., preventive action).

The drawback is that this technique is intrusive (the golden configuration is stored outside of the device) and requires protection against self-corruption in case of SHE.

SHE protection is part of the device design—for example, by implementing several copies of the chains using resources located in different areas of the circuit. The limitation is the area and power penalty. Not considering aging in the estimation of the cross-section may lead to overly optimistic values.

Finally, when deriving failure rates from manufacturer information, the computation needs to include at least the FPGA level FIT and MTBF, including the derating factor for altitude and latitude. To refine the analysis, consideration of the critical bits must be added.

7. DETAILED RESEARCH: SEE SSA FOR CDS

7.1 INTRODUCTION

7.1.1 Definitions

The following terminology is used within this report:

Critical	This term is used to designate a system function for which the most critical FC identified is CAT.
Essential	This term is used to designate a system function for which the most critical FC identified is HAZ or MAJ.
Non-essential	This term is used to designate a system function for which the most critical FC identified is MIN.
Not safety related	This term is used to designate a system function for which the most critical FC identified has NSE.
Side	This generic term is associated with the left or right cockpit/aircraft function or resource.

7.1.2 Purpose

This section discusses the SEE SSA applied to a CDS. The CDS has been selected for the performance of a sample SSA because it is a complex system with varied SEE-sensitive components (e.g., combinatorial logic chains, memory cells) mitigated both by built-in and not-built-in techniques. The highest level of FC for a CDS is CAT, therefore requiring an SEE safety analysis. This section will also address the lower-yet-relevant FC of MAJ/HAZ.

The objective is to verify the acceptability of the CDS implementation with regard to:

- safety objectives defined within the FHA and applicable regulation requirements.
- safety requirements allocated to or derived from design.

The demonstration of compliance is performed through several quantitative and qualitative analyses, mostly issued from ARP4761 guidelines [4]. This safety assessment includes system SEE assessment, according to reference [1], to demonstrate that the system is adequately mitigated against SEE. The results of the various analyses are synthesized within the following subsections, with additional details provided in appendix D.

This section is organized as follows: section 7.2 describes the system architecture of a CDS, including its physical components, intended functions, internal and external interfaces, and system FCs. Section 7.3 provides information on the safety mechanisms implemented in a CDS at system level, equipment level, and in relation to the FWS. Section 7.4 develops the methods of compliance to meet the safety objectives; in particular, an SEE safety assessment approach is proposed that builds from the investigations covered in the previous deliverables and integrates the latest discussions with the EASA. Section 7.5 describes the main elements of a safety analysis (e.g., fault-tree analysis, determination of DAL, and CMA), and shows the main findings of an SEE safety analysis following the proposed process. Section 7.5.4 summarizes the outcomes of the safety assessment as they impact the maintenance and operation of the CDS.

7.2 SYSTEM ARCHITECTURE

7.2.1 The CDS Description

The CDS under investigation consists of (see figure 43):

- Five DUs:
  - Two outer DUs referred to as outer right (OR) and outer left (OL)
  - Two inner DUs referred to as inner right (IR) and inner left (IL)
  - One center DU referred to as center display (CD)

- Two control panels that interfaced with the DUs and were used for reversions management, crew display, and alerting controls. They include:
  - DU format reversion switches included in a reconfiguration control panel (RCP)
  - Sources reversion switches for air data and attitudes & heading sensors included in an RCP
  - Controls for system pages selection display included in the EICAS control panel (ECP)
  - Controls for crew alerting system (CAS) messages and check-list windows management in the ECP

The CDS provides the following functions:

- The Primary Flight Display (PFD) format displays the basic critical information to fly the aircraft, such as altitude, speed, and the artificial horizon.
- The Navigation Display (ND) format displays data (flight plan, etc.) to navigate the aircraft.

- The Engine and Warning Display (EWD) format displays information to monitor the aircraft systems and engines, such as engine parameters (thrust and flight controls status) and crew-alerting messages and procedures (from the flight warning).
- The System Display (SD) format displays pages to monitor several aircraft systems.

The CDS configuration at aircraft power-up is the following (see figure 44):

- Both outer DUs (OR and OL) display the PFD format.
- The center DU displays the EWD format.
- In normal conditions, the inner DUs have the functionality of multi-format display (MFD):

  - IL DU displays the ND format.
  - IR DU displays the SD format.
  - Both ND and SD formats may be swapped and configured by the flight crew according to their operational needs (e.g., pilot flying side vs. pilot monitoring aircraft system side).

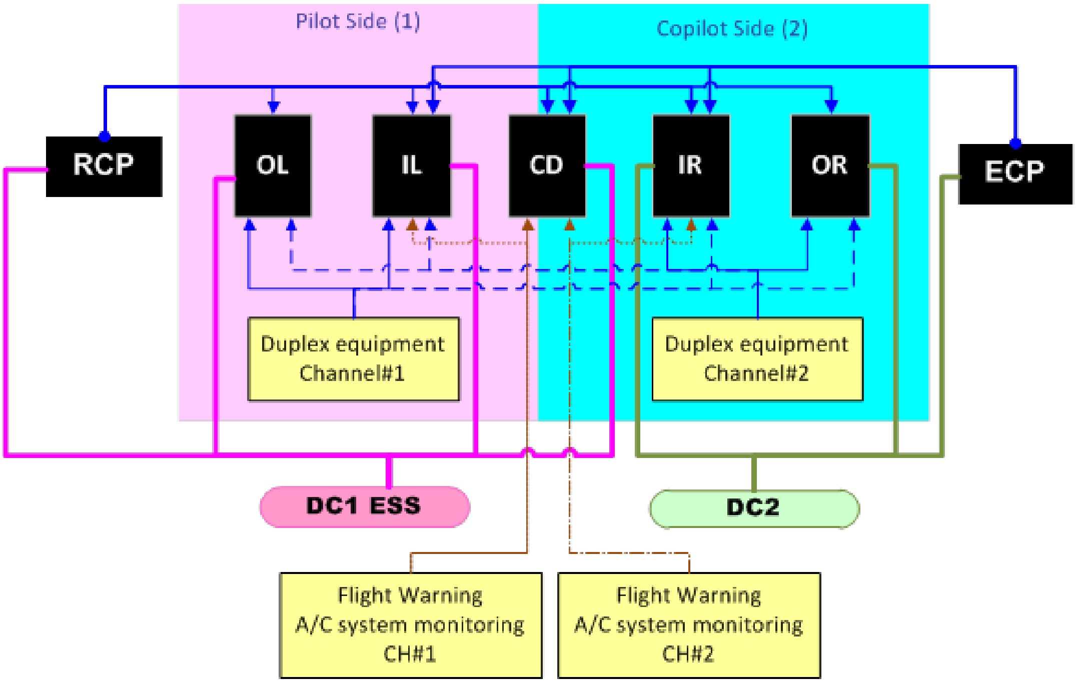

Pilot Side (1)
Copilot Side (2)
RCP
OL
IL
CD
IR
OR
ECP
Duplex equipment Channel#1
Duplex equipment Channel#2
DC1 ESS
DC2
Flight Warning A/C system monitoring CH#1
Flight Warning A/C system monitoring CH#2

Figure 43. The CDS architecture

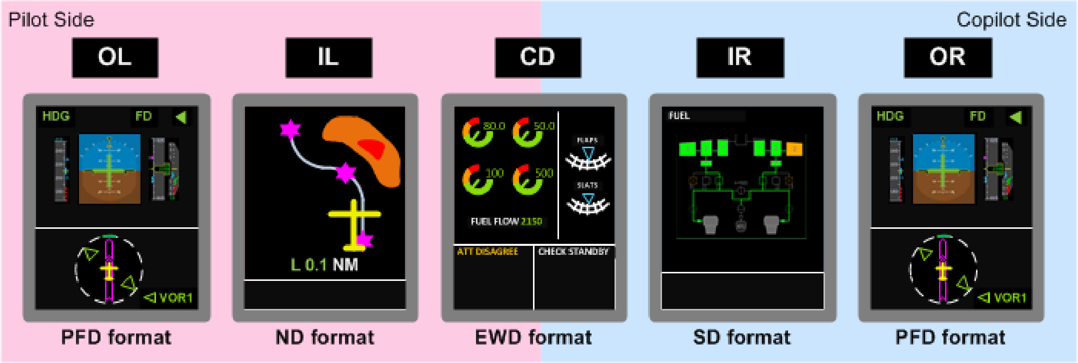


Figure 44. CDS configuration at power-up

7.2.2 Boundaries With Other Aircraft Systems

This section describes the interfaces of the CDS under investigation in terms of input flows (table 39), output flows (table 40), and electrical interfaces (figure 43).

7.2.2.1 Inputs From Other Aircraft Systems to the CDS

Table 39 describes the data flows from aircraft systems other than the CDS that provide input to the CDS.

Table 39. Description of input flows to the CDS

FROM Aircraft systems	TO Avionics system(s)	Functions/Flows
Landing Gear	Cockpit Primary Displays	Weight on wheels (for mode transition logics).
Flight Warning	Cockpit Primary Displays	Flight warning computer master/slave status; Master Warning/Master Caution; EWD CAS messages and associated check-lists.
Primary References	Cockpit Primary Displays	Air data (standard and corrected barometric altitude, airspeed); Attitude & heading parameters (attitudes, heading, inertial vertical speed)
Navigation and Flight Guidance	Cockpit Primary Displays	Radio navigation, flight management, flight guidance data (for PFD, ND, and SD formats)
Engine Controls	Cockpit Primary Displays	Engines’ parameters (EWD and SD formats)
Flight Controls	Cockpit Primary Displays	Flight controls status (EWD and SD formats)
Aircraft Systems	Cockpit Primary Displays	Aircraft systems’ monitoring parameters (SD pages)
External Protection Systems	Cockpit Primary Displays	Terrain and traffic collision alerts, radio-altitude data (PFD and ND formats)

7.2.2.2 Outputs to Other Systems

Table 40 describes the data flow from the CDS to the other aircraft systems.

Table 40. Description of output flows to the CDS

FROM Avionics systems	TO Aircraft system(s)	Functions / Flows
ECP	Flight Warning	CAS messages or procedure scrolling (ECP); Amber Caution clear (ECP); Amber Caution recall (ECP)

7.2.2.3 Aircraft Resources

The electrical buses distribution is illustrated in figure 43. The aircraft provides forced air cooling to the CDS. In case of cockpit cooling loss, the failure will be annunciated on all DUs (the message DU OVERHEAT is detected through the internal monitoring of the DUs). More information can be found in section 7.3.3.4.

7.2.3 CDS Internal Electrical Interfaces

Table 41 details the main interfaces within the CDS perimeter between different components of the system.

Table 41. Main interfaces internal to the CDS

Interfaces/data flow□Avionics system(s)		TO	
		Cockpit Primary Displays	Control Panels
FROM	Cockpit Primary Displays	DU(s) healthy status (discrete) Automatic reversions (Ethernet) Feedback monitoring (Ethernet)	N/A
	Control Panel (RCP)	Sources reversions (ARINC429) PFD/ND & EWD/MFD format swap (discrete) MFD format selection (ARINC429)	N/A
	Control Panel (ECP)	SD pages call (ARINC429)	N/A

7.2.4 System Mission Profile

7.2.4.1 CDS Life Cycle

Table 42 describes the mission profile for an aircraft X to be used in the fault-tree simulations of the CDS.

Table 42. Aircraft X life cycle parameters

Mission Profile Parameter	Value
Average flight time	4 flight hours
Average power on time per day	12 hours
Aircraft life	70,000 flight hours

7.2.4.2 Maintenance Intervals

Table 43 describes the intervals between maintenance checks for aircraft X that are used in the fault-tree simulations for the CDS.

Table 43. Aircraft X maintenance intervals

Maintenance Check Interval	Value
Not used	N/A

7.2.4.3 Aircraft Routes

This information is used in the computation of the SEE flux and is derived from the standard aircraft mission profile. For the purposes of this sample analysis, the hypothesis is an aircraft operating at a maximum altitude of 40,000 ft and maximum latitude of 45º.

7.2.5 System FCs From FHA

Table 44 lists the FCs from the FHA applicable to the CDS functions, standalone or in combination with stand-by display function.

Table 44. CDS FCs from FHA

Ref	Function	FC title	Severity	Quantitative objectives	Advisory/ guidance material
FC 01	Cockpit Primary Displays	Total loss of cockpit primary displays	HAZ	Extremely remote	Ref. [104]
FC 02		Total loss on primary display of any displayed parameter on both cockpit sides	MAJ	Remote	Ref. [104]
FC 03		Erroneous display on one primary display of any critical parameter (Airspeed, Barometric Altitude, Attitudes)	HAZ	Extremely remote	Ref. [104]
FC 04		Erroneous display on primary display of any critical parameter (Airspeed, Barometric Altitude, Attitudes) on both cockpit sides	CAT	Extremely improbable	Ref. [104]
FC 05		Erroneous display on primary display of any non-critical (including navigation and engine parameter) parameter	MAJ	Extremely remote	Ref. [104]
FC 06		Total loss of engine parameters display for all engines	HAZ	Extremely improbable	Ref. [104]
FC 10	Cockpit Primary and Standby Displays	Total loss of any critical parameter (Airspeed, Barometric Altitude, Attitudes) display on both cockpit sides combined with loss of standby display	CAT	Extremely improbable	Ref. [104]
FC 11		Erroneous display on one primary display of any critical parameter (Airspeed, Barometric Altitude, Attitudes) combined with a failure of standby display	CAT	Extremely improbable	Ref. [104]

Note: The FCs associated with the CAS are out of scope for this document.

7.3 SAFETY MECHANISMS

7.3.1 The SBs Against FCs

The architecture of primary cockpit displays is driven by the split cockpit philosophy implemented through the use of three segregated sets of displays: left displays, right displays, and the central display. This segregation between left (pilot) and right (copilot) sides mainly answers the fulfillment of most of the integrity safety objectives. It also supports the compliance with the primary display availability safety objectives, which have a lower criticality.

The standby display is fully independent from the primary cockpit displays, providing a redundant and segregated backup for displaying critical primary references. The primary/standby arrangement addresses the cockpit display's availability safety objectives.

Table 45 summarizes the safety mechanisms (at system or equipment level) identified in the safety process that are implemented in the design of the CDS at system or equipment level to comply with the safety objectives defined in the FHA. The first column lists the FC linked to the loss of availability and the second column to the loss of the integrity of the system. The right side of the table, "induced safety mechanisms," summarizes the SBs implemented in the design.

Table 45. CDS SBs

Function	Availability		Integrity	
	Max hazard severity	Induced safety mechanisms	Max hazard severity	Induced safety mechanisms
Primary Displays & Standby Display (STBY)	CAT (FC10)	The compliance to fail-safe criteria is provided by: SB_STBY1: Independence and segregation between cockpit primary displays and standby display	CAT (FC11)	The compliance to fail-safe criteria is provided by: SB_STBY1 : Independence and segregation between cockpit primary displays and standby display
Cockpit Primary Displays (left and right sides)	HAZ (FC01 & FC06) MAJ (FC02)	Redundancies between Pilot and Copilot sides at flight deck level: SB_CDS1: Segregation between left and right cockpit sides, including aircraft power supply (section 7.2.1) SB_CDS2: automatic and manual formats reconfiguration capabilities between own side Primary Displays (section 7.2.1) RCP allows reversions between Primary References Sources at one cockpit side level (section 7.3.2.2)	CAT (PFD format, FC04)	The compliance to fail-safe criteria is provided by: An independence and segregation between display and monitoring chains inside the DU (sections 7.3.2.3 & 7.3.3.4): SB_CDS3: feedback monitoring for critical parameters (CAT FCs) (section 7.3.2.3) SB_DU1: DU-specific CBITs monitoring to cover the DUs functional channel from graphic stage to screen stage (section 7.3.3.4). SB_DU2: Segregation/ partitioning at DU software level
Cockpit Primary Displays (one side)	MAJ (FC02)	Redundancies within one flight deck side : SB_CDS2: automatic and manual formats reconfiguration capabilities between own side Primary Displays (section 7.2.1 and 7.3.2.1)	HAZ (PFD format, FC03) MAJ (non-critical data, FC05)	The compliance to fail-safe criteria is provided by: Independence and segregation between display and monitoring chains inside the DU (sections 7.3.2.3 & 7.3.3.4): SB_CDS3 feedback monitoring for critical parameters (HAZ FCs) (section 7.3.2.3) SB_DU1: DU-specific CBITs monitoring to cover the DU's functional channel from graphic stage to screen SB_DU2: Segregation/ partitioning at DU software level

CBIT = continuous built-in test; STBY = stand-by (display)

7.3.2 Safety Design Features at System Level

7.3.2.1 Reconfigurations of Formats

7.3.2.1.1 Automatic Reversions Inside the System

Because the formats do not have the same criticality, automatic reconfigurations might maintain the availability of the most critical information (i.e., PFD and EWD formats) when one DU fails. Manual reconfigurations using the control panels are also feasible.

A reconfiguration happens when a display no longer receives information from the other displays and thinks that a format more critical than its own is no longer displayed. To prevent cascading failures, only one automatic reversion inside the CDS is allowed.

The principles of automatic reconfigurations of PFD or EWD format follow. Also, see figure 45:

- In case of failure of a DU displaying PFD format, the remaining own-side DU will automatically revert to PFD format:

    - If OL (respectively OR) displaying PFD format becomes failed or switched OFF, then IL (respectively IR) switches to PFD format.
    - If IL (respectively IR) displaying PFD format becomes failed or switched OFF, then OL (respectively OR) switches to PFD format.

- In case of a failure of CD displaying EWD format, the IL display will automatically revert to EWD format:

    - If CD displaying EWD becomes failed or switched OFF, then IL switches to EWD format.

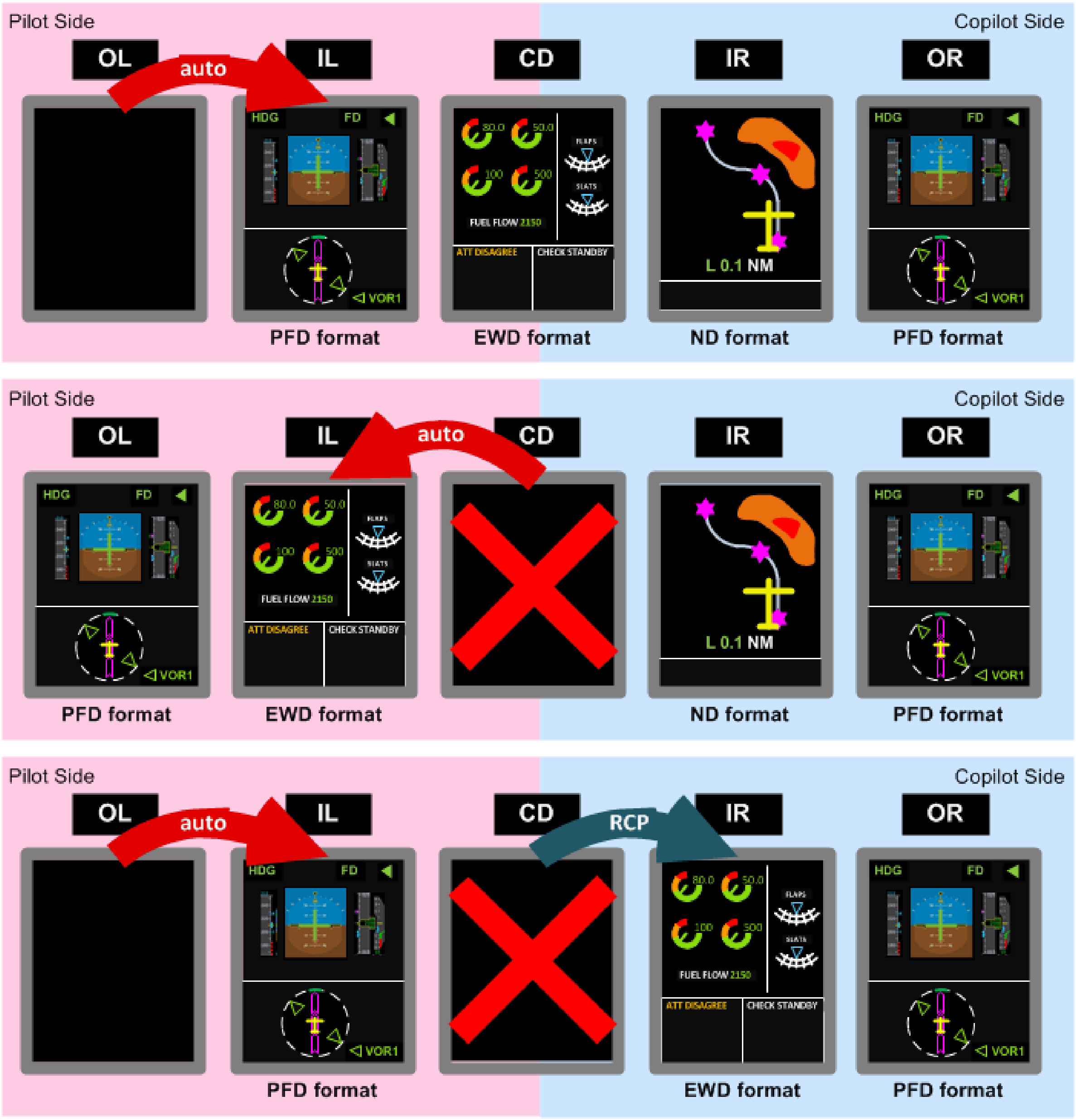


Figure 45. Automatic reversions (red arrows) in case a single DU is lost

<u>7.3.2.1.2 Manual Reconfigurations of Formats</u>

Means are provided independently to the pilot and copilot to select the format to be displayed. To that end, each DU is interfaced with a dedicated control—located in the control panels—to reconfigure in case of pilot or copilot request. The manual configuration possibilities follow. Also, see figures 46 and 47:

- OL (respectively OR): units can display ND format on manual crew selection through the left (respectively right) RCP PFD/ND XFR pushbuttons.

- IL (respectively IR): units can display EWD format on manual crew selection through the left (respectively right) RCP EWD/MFD XFR pushbuttons.
- When not displaying PFD or EWD formats, the inner units hold the ability of MFD:
  - ND formats may be displayed on the inner DUs on manual crew selection through the RCP ND key pushbutton.
  - SD formats may be displayed on the inner DUs on manual crew selection through the RCP ND key pushbutton and appropriate system pages may be called through ECP-specific pages or “all swap” pushbuttons.

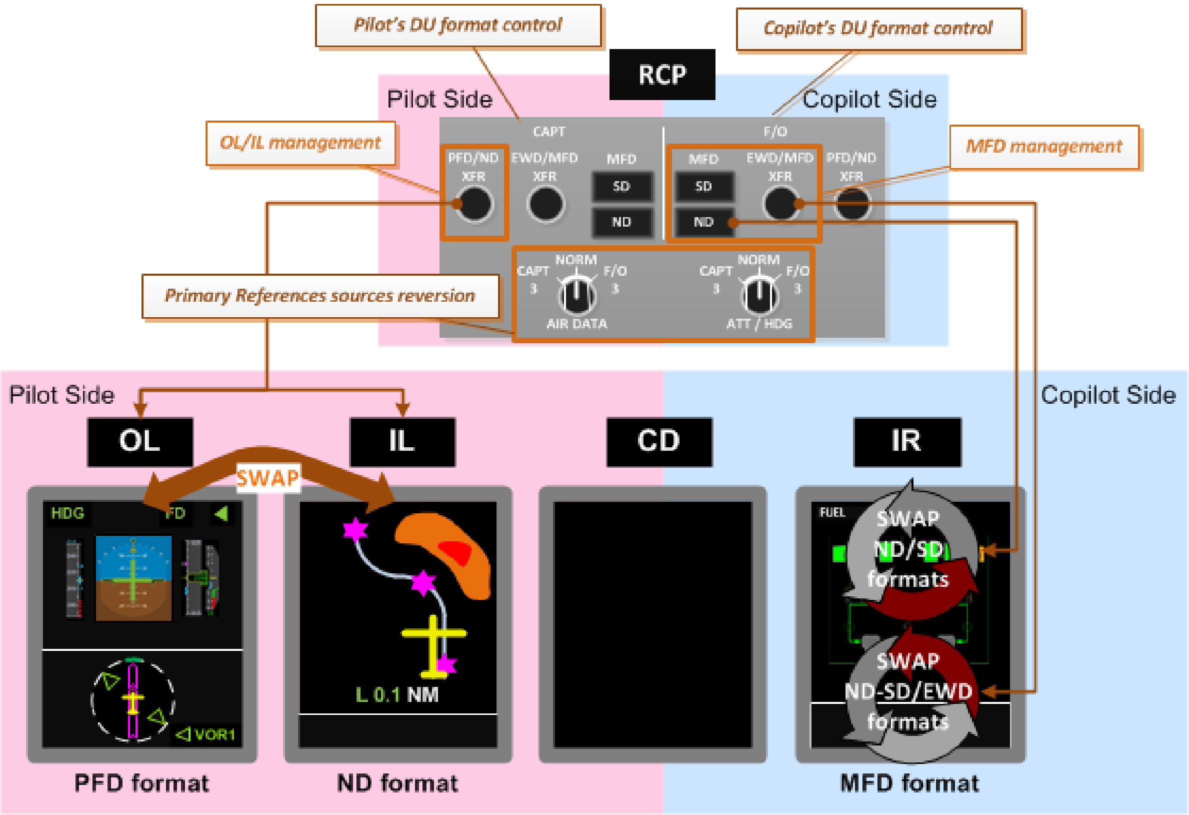


Figure 46. Format manual reconfiguration through RCP

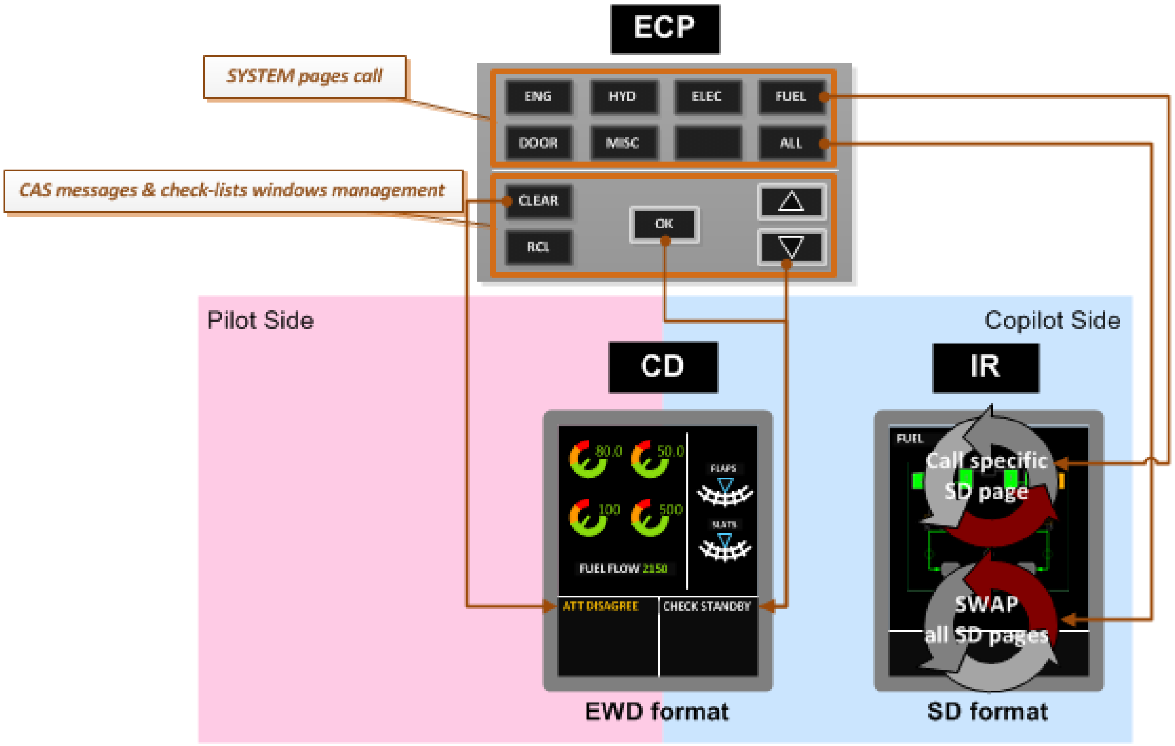


Figure 47. Format manual reconfigurations through ECP

7.3.2.2 Reconfiguration of Sources for Primary References

The architecture for displaying primary flight data are composed of dual primary altitude and air data channels based on the segregation between sources used by the cockpit pilot and copilot's sides. In nominal configuration:

- Data from source #1 are displayed on pilot's DUs (PFD format on DU1 or DU2).
- Data from source #2 are displayed on copilot's DUs (PFD format on DU4 or DU5).

Pilots may select a third independent source (source #3) through the RCP air data and attitudes/heading-dedicated rotary switches (see figure 48).

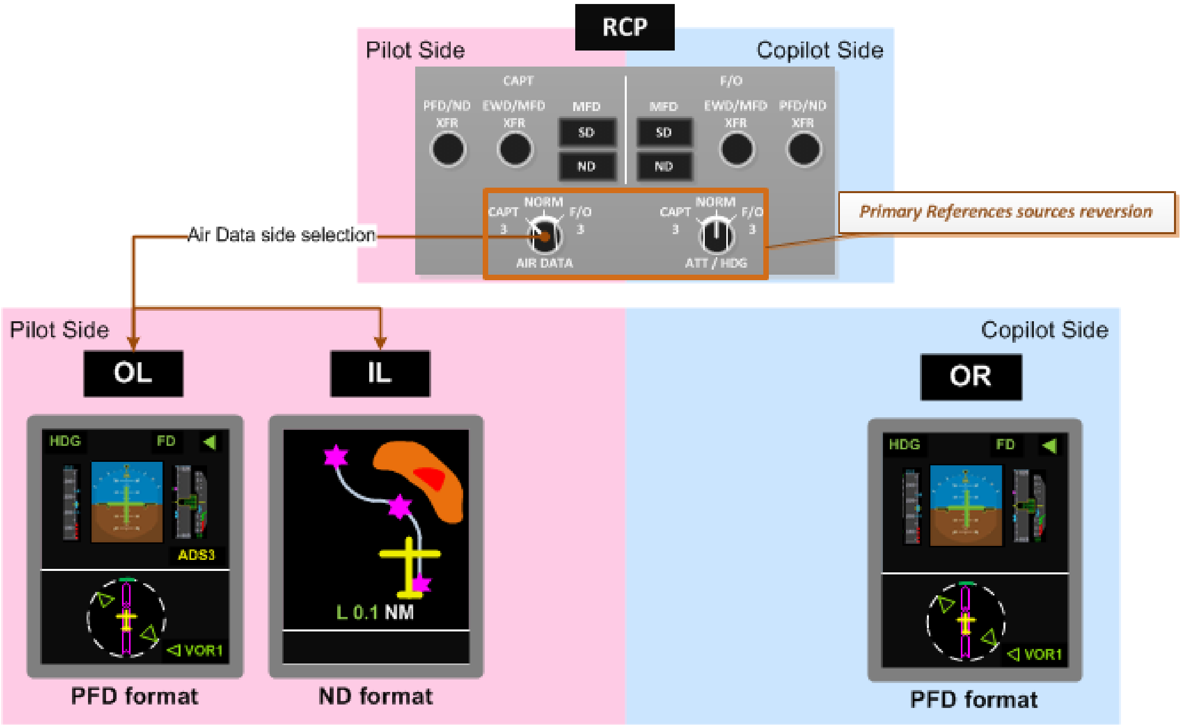


Figure 48. Manual reconfigurations of cockpit primary references (single-sensor loss)

Note: the sources for primary references are out-of-scope of the CDS and the present safety assessment.

7.3.2.3 Feedback Monitoring

Feedback monitoring is implemented to prevent common mode failures between all DUs due to a single cause (e.g., software fault inside the DU) leading to an undetected erroneous display of critical parameters on the whole cockpit. Data display and feedback functional paths are independent inside the DUs.

The feedback consists of verifying the correct drawing of these critical parameters on the DU and in alerting the crew if it detects hazardous misleading display information, as defined in AMC 25-11.

To perform feedback monitoring (or reverse computation denoted F^{-1} function), two different DUs are used: one unit is used for display and the other is used for the feedback and the computation of the F^{-1} function. The data between the monitored and the monitoring DUs are transmitted over Ethernet [*F(p)* data] and feedback messages are displayed by the monitored DU.

The parameters being monitored include:

- Airspeed and barometric altitude air data (displayed in PFD format).
- Attitude (pitch, roll) data (displayed in PFD format).
- Engine parameters (displayed in EWD format).

As shown in figure 49, the CDS is virtually divided into two half sub-systems: the left feedback loop consisting of OL and IL displays, and the right feedback loop consisting of CD, IR, and OR displays. Each DU feeds back the valid DU preceding it in the loop only if the monitored unit displays a critical format (i.e., PFD or EWD).

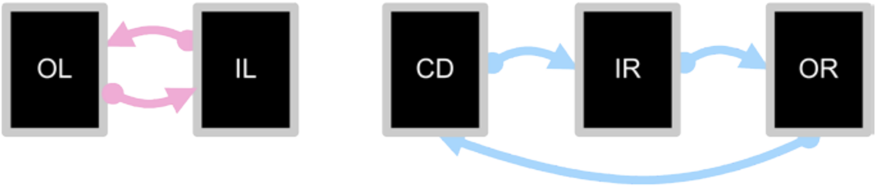


Figure 49. Left and right feedback loops

In one monitoring display fail, the feedback loop is dynamically reconfigured as described by the following rules:

- In normal configuration:
  - OL (respectively OR)—if it displays PFD format—is fed back by IL (respectively IR).
  - IL—if it displays PFD or EWD format—is fed back by OL.
  - IR—if it displays PFD or EWD format—is fed back by CD.
  - CD—if it displays EWD format—is fed back by OR.
- In degraded configuration:
  - if OR is failed, CD is fed back by IR.
  - if IR is failed, OR is fed back by CD.
  - if CD is failed, IR is fed back by OR.
  - if IL (respectively OL) is failed, OL (respectively IL) is no longer fed back.

The algorithm of feedback monitoring inside the monitoring DU implements the following steps (see figure 50):

1. The monitoring unit acquires the information $F(p)$ from the monitored unit over Ethernet and also acquires the parameter p from the same source sensor as the one displayed on monitored unit.
2. It computes the inverse function “F-1” of $F(p)$ and compares the result with p.
3. The result of this comparison, for each critical parameter, is then filtered to give a feedback result for $F(p)$ according to the rules in table 46.

Table 46. Feedback sanctions rules

P status/ F(P) status	Not valid	Valid
Not valid	Feedback Inhibited	Feedback cannot be performed: “DUxx NOT MON” message
Valid	Feedback cannot be performed: “DUxx NOT MON” message	- “CHECK” message when the discrepancy between *p* and $F^{-1}(F(p))$ is significant; - Otherwise, no message is displayed because the *p* parameter is well represented

Because the feedback detects errors on the outputs of the graphical chain, this monitoring covers both hardware failures and software errors. It also detects hardware faults on the processing and graphics generation. Additional internal monitoring is performed to cover the functional stages between the graphical function and screen display function (see section 7.3.3.4).

The monitoring DU performs the reverse computation (F^{-1} function) that uses the outputs of the graphic channel and compares them with the corresponding direct input parameter (acquired in A429). The reverse computation is done by DAL A software, according to RTCA-DO 178B [105].

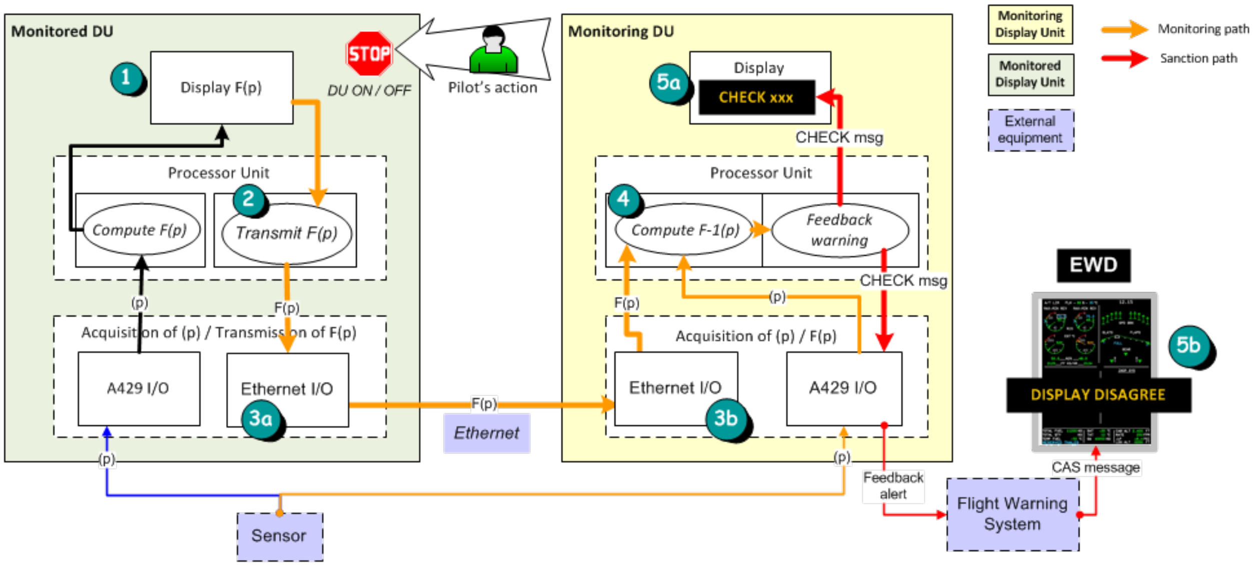


Figure 50. Feedback principles

1. Acquisition and display of any critical parameter "*p*" on the monitored DU: the "*p*" parameter is acquired by data acquisition unit on A429 I/O module;
   the parameter is then processed: graphic language commands are transmitted to the graphic processing module, which executes SGL commands and draws the symbols and then sends some characteristic information of the drawing, called *F*(*p*), back to the data acquisition unit

2/3a. Transmission of *F*(*p*) information to the monitoring DU: the monitored DU transmits *F*(*p*) information to the monitoring DU via Ethernet bus.

3b/4. Feedback monitoring: the data acquisition unit of the monitoring DU acquires the *F(p)* information. The processing unit also acquires the "*p*" parameter coming from the same sensor as the one displayed on monitored DU. It computes the inverse function "F^{-1}" of *F(p)* and compares the result with *p* (step 4). The result of this comparison for each critical parameter is then filtered to give a feedback result for *F(p)* according to rules detailed in table 46.

5a/5b. In case of feedback discrepancy detection (i.e. feedback result = "CHECK"), two types of messages are provided:

- Message for FWS performed by the feedback monitoring DU X/DU Y DISAGREE CAS caution message (step 5b) (see section 7.3.4). The procedure associated with this kind of message asks crew members to compare monitored DU with opposite-side DU if disagree; monitored DU shall be rebooted or switched off.
- Three different CHECK messages (called "CHECK PFD LEFT," "CHECK PFD RIGHT," or "CHECK EWD") of feedback warning are displayed on the monitoring DU (step 5a) and sent through the Ethernet bus to the other DUs, which may also display the message (feedback DU and offside DU displaying PFD format exclusively for CHECK PFD message). On each DU format (PFD, ND, EWD and each page of SD format), a zone is available for the display of one of the three CHECK

7.3.3 Safety Design Features at Equipment Level

7.3.3.1 DU Internal Architecture

The global principles of a working DU are:

- Units receive the data to display through ARINC429 or Ethernet.
- The data received are processed into graphic parameters, which are transformed in digital frames.
- These frames are then transmitted to the liquid crystal display (LCD) along with timing and synchronization signals.

The DU includes the following modules (see figure 51):

- The power supply module (PSM), which provides the main secondary low voltage for the equipment.

- The input/output module (IOM), which provides the protection and filtering for all in/out interfaces.
- The core processing module (CPM), which provides the processing resources for image computation.
- The graphic generation module (GGM), which supports the graphic generation and mixing with an external video input. The picture displayed is processed in a video output.
- The LCD assembly module (LAM) and the backlighting module (BLM), which provide dimming function and allow for the display of the processed picture on the LCD screen.
- The human-machine interface, which is available by means of a keyboard.

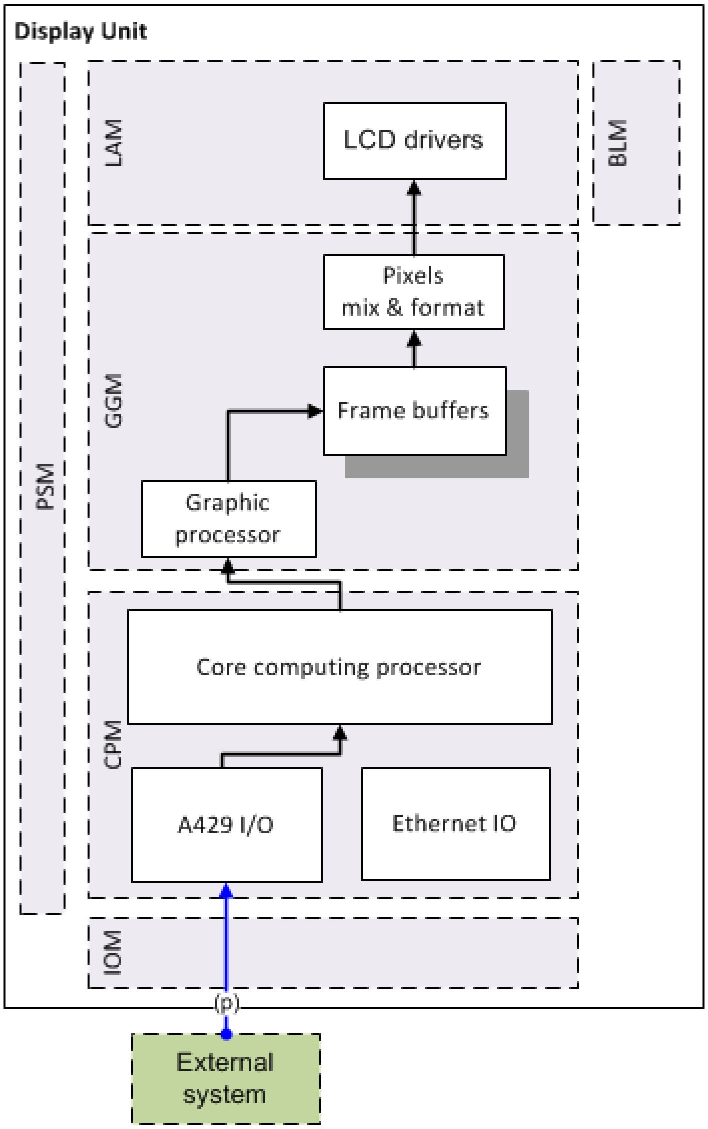


Figure 51. DU internal breakdown

7.3.3.2 DU Modes

Figure 52 details the DU's operational and maintenance modes and the transitions between different modes:

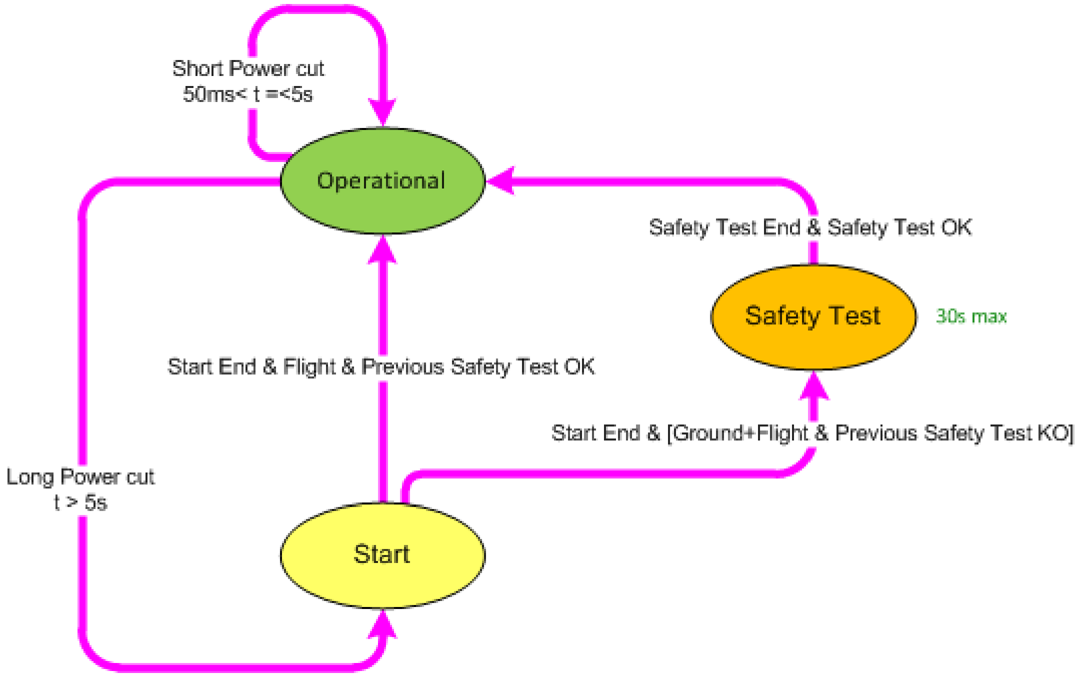

Short Power cut
50ms< t =<5s
Operational
Safety Test End & Safety Test OK
Safety Test
30s max
Start End & Flight & Previous Safety Test OK
Start End & [Ground+Flight & Previous Safety Test KO]
Long Power cut
t > 5s
Start

Figure 52. DU modes

7.3.3.3 Monitoring of Electrical Interfaces

The A429 inputs are monitored by the DU's embedded applications to detect the following failure modes:

- No refresh of a sampling message.
- Sign/status matrix (SSM) of an A429 label considered not valid by an application.
- Data inconsistency with normal functional range expected by the application.

A monitoring of RCP frame is performed by the outer and inner DUs to trigger the default image display mode when some RCP selections are not valid (e.g., parameter not valid in the A429 SSM) and send the RCP healthy status to the flight warning for alarm computation when its frame is not refreshed.

7.3.3.4 DU Safety Cyclic Mechanisms for Integrity

Continuous monitoring is for safety purposes only. It is performed to detect hardware failures related to integrity and significantly reduce the exposure time of the associated failure modes. This monitoring is summarized in figure 53:

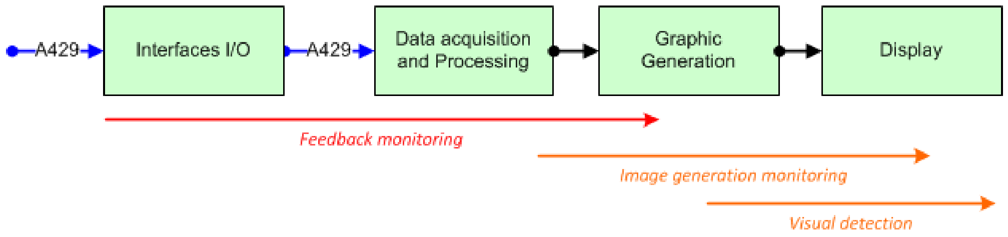


Figure 53. Overview of DU integrity monitoring

Feedback monitoring performed at system level is described in section 7.3.2.3. To monitor the graphic generation and display functions that are not tested by the feedback monitoring, three complementary mechanisms (called Image Generation Monitoring) are implemented:

- Monitoring of frame buffer permutation on each graphic channel (see section 7.3.3.4.1)
- Test of the graphic mixing on each graphic channel (see section 7.3.3.4.2)
- Frozen display monitoring (see section 7.3.3.4.3)

In addition:

- Image display failures can be detected by visual direct effects (see section 7.3.3.4.4).
- Overheat protection mechanisms are implemented within the DU to avoid DU front face or internal overheats:
  - A monitoring detects overheat (first threshold) through the BLM thermal sensor. If it trips, the DU is set in low power consumption (luminance is decreased) and annunciates a DU OVERHEAT message on all DUs.
  - A monitoring (second threshold) detects overheating via the power supply thermal sensor (the signal is tested with power on). If the overheating is tripped, the DU exhibits a fatal error.

DU Frame Buffer Permutation MonitoringThe aim of the frame buffer permutation monitoring in figure 54 is to check the switch mechanism of the frame buffer on each graphic channel by the processor unit. Each frame buffer memory is composed of two distinct memory modules (double-page frame buffer) cyclically performing writing or reading/erasing tasks. For symbology, each graphic processor writes generated pixels in the write page. At the end of the writing cycle, it sends an order of permutation to its own-channel mix and format of its erasable programmable logic device (EPLD), which reads, mixes, erases, and then permutes the two pages (after synchronization with the other mix and format EPLD from the second graphic channel), so that symbology data are cyclically refreshed and sent back a switch status. This test detects frozen display due to graphic raster generation (frame buffers permutation function). The sanction of the monitoring is a DU fatal failure.

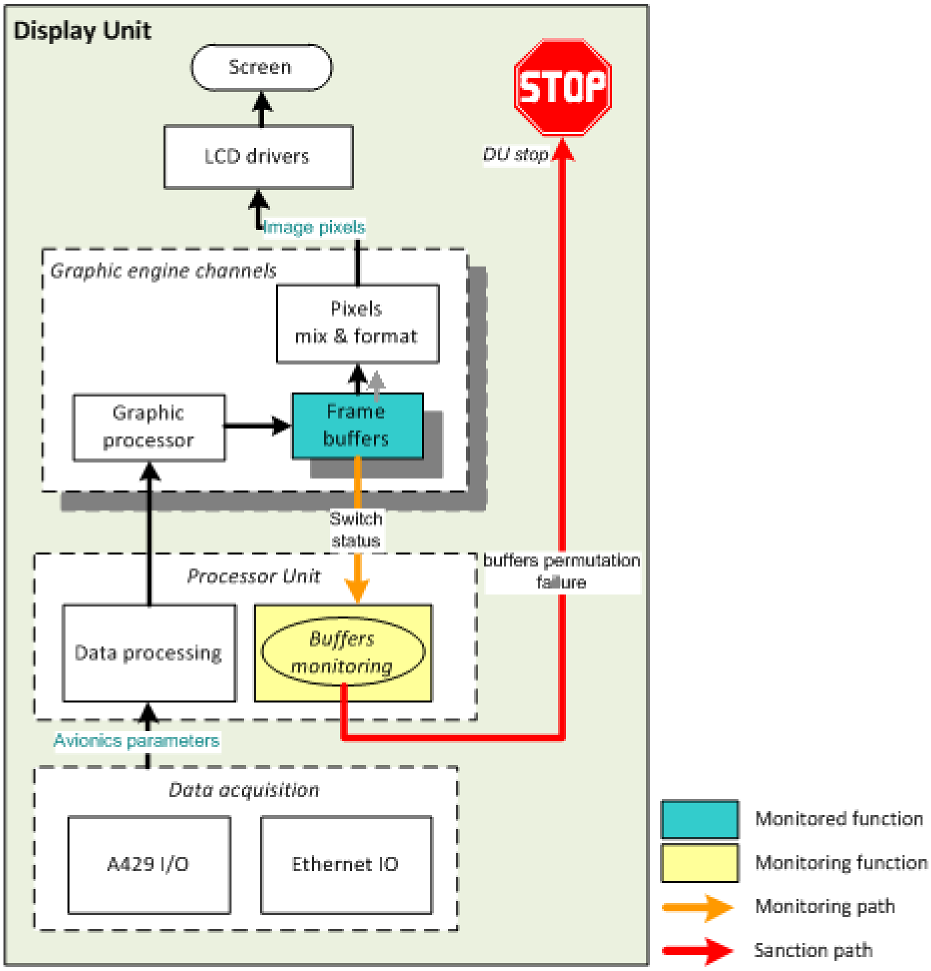


Figure 54. Frame buffer permutation monitoring

7.3.3.4.1 DU Graphic Mixing Monitoring

The aim of the monitoring in figure 55 is to check the mixing mechanism of each channel of the graphic engine. This monitoring uses several test patterns generated and monitored by the processor unit that are chosen outside the visible area of the screen and change cyclically.

This test detects degraded display due to graphic raster generation (writing/reading in graphic memories function). The sanction of the monitoring is a DU reset.

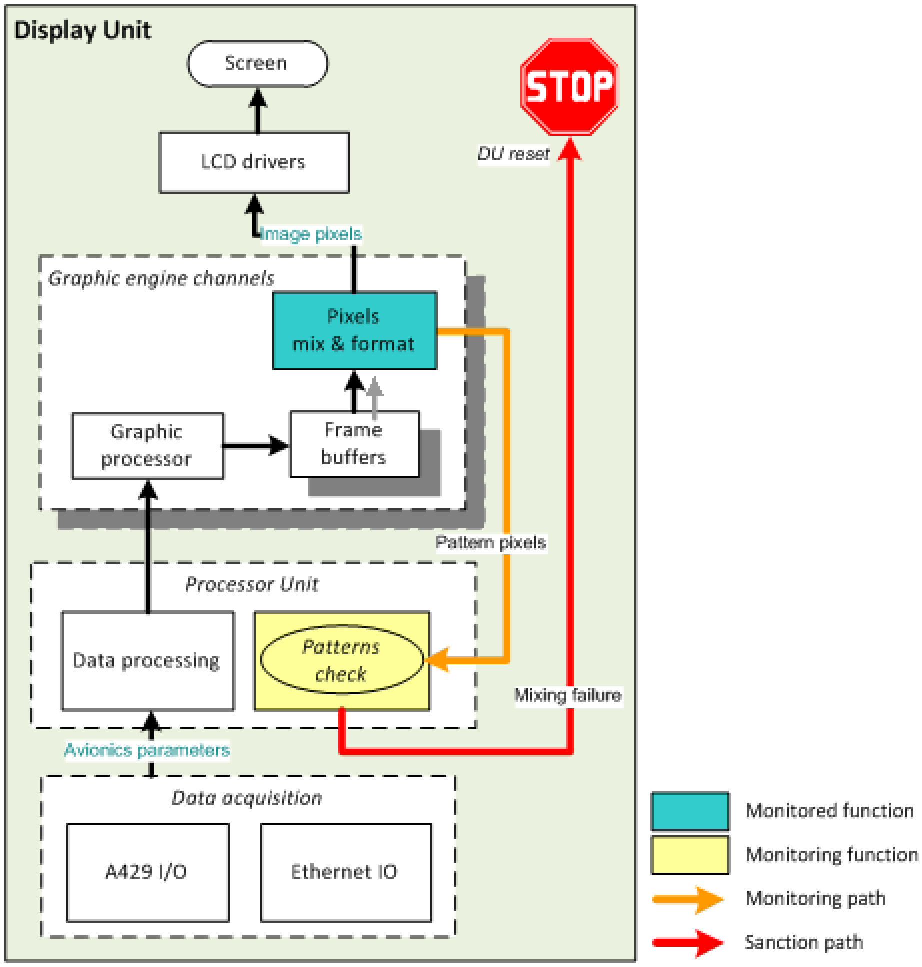


Figure 55. Graphic mixing test

7.3.3.4.2 DU Frozen Display Monitoring

The aim of the monitoring in figure 56 is to check image signals generated by the LCD drivers that can lead to a frozen display. This monitoring uses selected line (the intersection of one line and one column is the pixel composed of three dots: red, green, blue) driver return signals generated by the LCD drivers, whose validity, consistency, and periodicity are monitored by the processor unit.

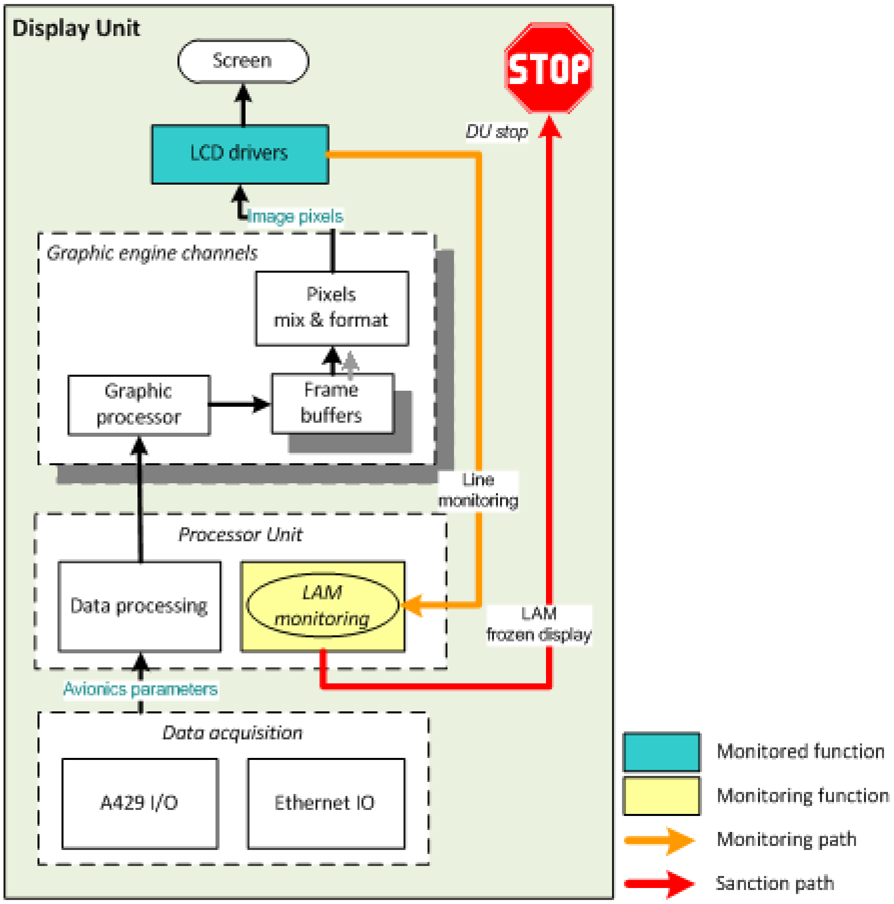


Figure 56. Frozen display monitoring

This monitoring detects the frozen display due to LCD drivers. The sanction of the monitoring is a DU fatal failure.

7.3.3.4.3 Visual Detection for Image Display Failures

In addition to continuous monitoring, some failure of the graphic generation and display chain downstream from the processing functions are detected visually by the flight crew (failures leading to loss of part of the screen, reduction of contrast, grey level degradation, flicker) as illustrated in figure 57.

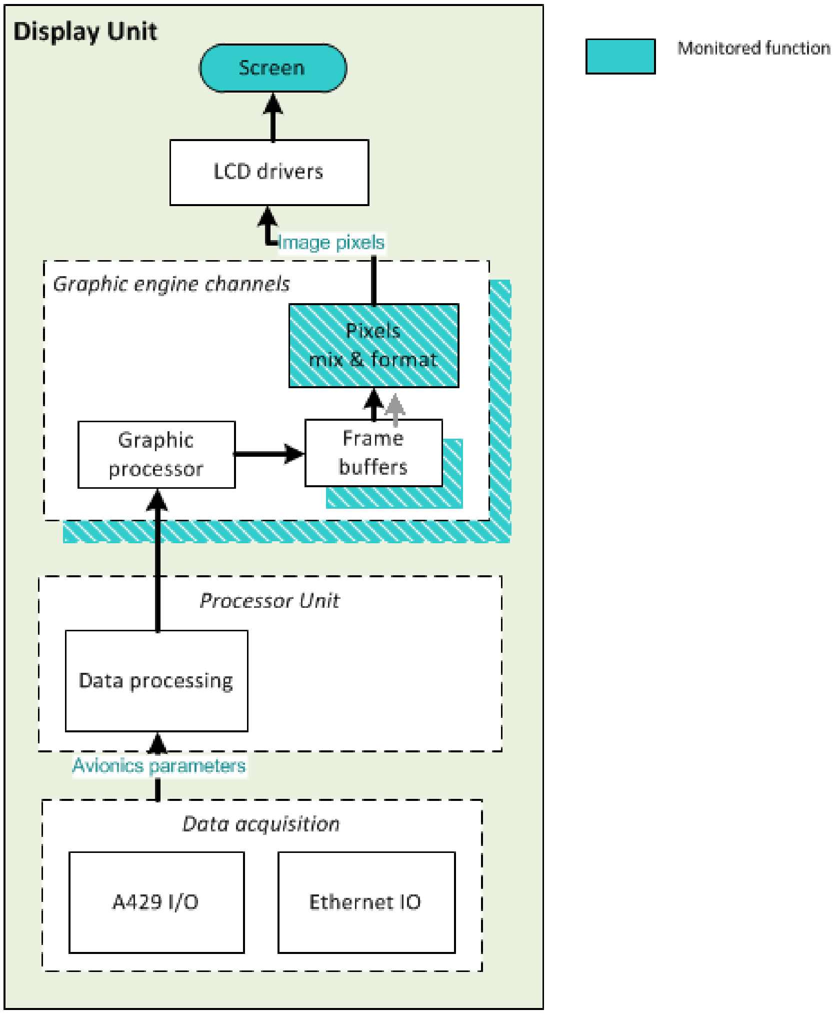


Figure 57. Visual monitoring detection

The pixel generation is performed by two independent graphic channels inside graphic generation (except for the permutation of graphic memories); each of them is dedicated to the pixel generation of one column over two in order to interlace the LCD screen columns. Failures of one graphic channel—graphic processor or pixels mix & format—excepting those leading to frozen display and detected by the previous monitoring, will then lead to degraded or lost display. Failures of line or column drivers or failures of pixels (LCD matrix) are visually detected (part of the screen is lost leading to degraded display of the image).

7.3.4 Crew Alerting and Flight Warning

The FWS gathers the aircraft system and avionics data status needed to compute the crew system alerts (aural alerts and visual CAS messages displayed on a specific window EWD format) and associated abnormal or emergency situation. When an unexpected situation occurs, it also drives the attention getter (master warning or master caution push button annunciators depending on the level of the associated alert) to draw crew attention.

The crew has the capability to manage the CAS message area display (e.g., clear or recall a message, open the associated electronic procedure, scroll up or down in a display area) using the ECP. A new caution and warning CAS message needs to be acknowledged by the crew through the master caution/warning attention-getter push-buttons.

The aim of table 47 is to detail flight warning annunciations specific to the CDS when faced with failure dormancy and requested flight crew corrective action.

Table 47. CDS failure modes monitored by the FWS

CAS message	Type	Abnormal situation Description	Master lights	Audio alert
DU X FAULT	Caution	One DU is faulty	Master Caution	Single Chime
DU X/DU Y DISAGREE	Caution	Discrepancy is detected between two (monitored and monitoring) DUs on PFD or EWD critical parameters (see table 46). This message is normally accompanied by a CHECK PFD or CHECK EWD message on monitoring DU.	Master Caution	Single Chime
DUx NOT MON	Advisory	Critical parameters displayed by the DU are no longer monitored	None	None
RCP X FAULT	Caution	One RCP is faulty (detected by the DUs)	Master Caution	Single Chime

7.4 METHODS OF COMPLIANCE

The compliance with the regulations is established by a combination of analyses and testing, as detailed in the acceptable means of compliance of the aviation regulations:

- Significant single failure analysis using FMEA at equipment level
- Significant multiple FCs analyses:

  - FTA techniques at system level
  - CMA
  - DAL allocation

- SEE safety analysis, according to reference [1].

The demonstration of compliance is performed through several quantitative and qualitative analyses, mostly issued from ARP4761 guidelines [4], which are detailed in the following sections.

7.4.1 Single Failures Analysis

7.4.1.1 LRU Failure Mode & Effect Analysis/Failure Mode & Effect Summary

The LRU FMEA is a bottom/up method used to:

- Identify random hazards associated with the incorrect operation of component functions.
- Quantify the failure rate of these hazards.
- Quantify test coverage rates and location rates for testability analysis.

An FMEA has been carried out at equipment level of the system. The FMES is a summary of the FMEA, in which all failures leading to the same consequence at LRU level are grouped. An LRU FMES will be provided on a case-by-case basis if the LRU FMEA size and complexity does not permit easy handling of the FMEA results.

7.4.2 Significant Multiple FCs Analysis

7.4.2.1 The FTA

7.4.2.2 Foundations of the Analysis

The applicable FCs are those detailed in the FHA of the CDS provided by the airframer. Each FC with a severity greater than MIN (according to AMC 25.1309) is modeled in a fault tree to identify the combinations of elementary failure events that caused the top-level hazards.

7.4.2.2.1 The FTA Method

The FTA provides a graphical description of the logical interconnections between various functions or component failure events leading to the feared event. The feared event, also named “undesired event,” is represented at the top of the tree. The initial branches in the fault tree are defined by identifying the immediate causes of that event. Further branches are derived by determining the next immediate causes. This process is repeated following the desired level of detail. Each event will then be a combination of lower level events using various “AND” and “OR” gate types. The leaves at the final level will represent the elementary failure modes of each involved component. In principle, a fault tree is built so that only independent failure events are combined through AND gates. In fact, with fault tree software, this condition is not obligatory because the basic events, worded in the same way, represent the same event and are then considered as common modes at the level of the “AND” gates. The combination of triple or more independent failures are generally not studied in fault-trees, assuming their probability is less than 10% of double set overall probability.

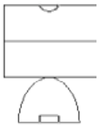
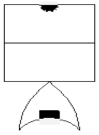
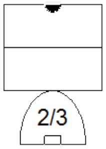
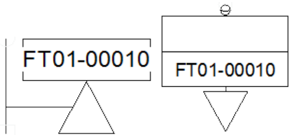
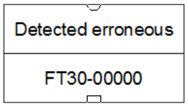
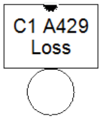
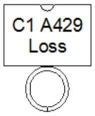
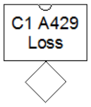
To check the compliance with quantitative objectives and some qualitative requirements, the fault tree is decomposed into minimal cut sets (see section 7.4.2.2.4 for the concept definition).
In fact, the probability of the top event is computed by summing the probabilities of all minimal cut sets. The probability of a minimal cut set is equal to the multiplication of the probabilities of the basic events in the set because these events are independent by definition of the set.

In accordance with ARP4761 [4] and AMC25.1309 [106], the probability of occurrence of an FC is calculated for the "Average Flight," defined in section 7.2.4, and divided by the "Average Flight" duration in flight hours to obtain the Average Probability per Flight Hour. This last quantitative value is then used in conjunction with the hazard category/effect established by the FHA to determine if it is compliant for the FC being analyzed.

7.4.2.2.2 Symbology

The symbology used in fault-tree analysis is described in table 48:

Table 48. Fault tree symbols

Symbol	Designation
	The AND gate describes the situation whereby the coexistence of all input events is required to produce the output event. P(AND) = P(E1) x P(E2)
	The OR gate describes the situation whereby the output event will exist if one or more of the input events exists. P(OR) = P(E1) + P(E2)
	The Combination gate used for *m* out of *n* allowed combinations
	Transfer gates: The triangles are used if necessary to indicate and reference the transfer from the main diagram to a sub-diagram
	Intermediary event: permits only to incorporate visibility within the fault tree by introducing comments
	Elementary event: the circle indicates a basic fault event that requires no further development
	Dormant event: the dual circle indicates that failure is not detectable during the flight—its probability of occurrence is computed considering the relevant exposure time (e.g., time intervals between maintenance and operational checks/inspections)
	Event considered as not elementary: The possible causes of the event are not developed for the purpose of the subject analysis or out of Thales scope package (external event)

7.4.2.2.3 Use of Generic Parameters in Basic Events

Basic events are characterized by two parameters: the failure rate (λ) and the exposure time. The FTA tool permits sharing of the same generic failure rate or exposure time among several basic events. This is particularly useful for the modeling of several instances of identical resources.

7.4.2.2.4 Minimal Cut Set

The minimal cut set provides the exhaustive list of minimal basic event combinations leading to the feared event. The minimal cut sets are provided for all CAT and hazardous FCs. To ease the understanding of the minimal cut set, they are sorted by order and then probability of occurrence. This view allows verifying that for the CAT FC, there is no minimal cut set of order 1 (no single failure) that leads to the feared event.

7.4.2.3 Allocation of DALs

This section presents the methodology to allocate DAL for software and complex hardware assurance levels to justify compliance with the applicable regulations according to SAE ARP4754A [5]. The certification and quality assurance procedures to apply for the development of an item depend on the DAL allocated to this item and are documented in the aeronautical standards of RTCA DO-178 B [105] for software and DO-254 [107] for hardware.

The method consists of the identification of each hardware and software component of the composition list, the most severe failure case identified within the FHA of the system. The classification of functions is made according to the most severe FC in which the function is involved; for items that support multiple aircraft functions, the DAL requirements are based on the most severe of the effects resulting from failure or malfunction of any supported aircraft function or any combination of supported aircraft functions.

The DAL assigned to an item depends therefore on the DAL required for the system and also on the system architecture—in particular, the number of independent failures and/or errors that, in combination with the considered item failures/errors, lead to an FC. ARP 4754A [5] defines rules to break down DAL and assign the refined DALs to each item involved in the functional FC as a function of the architecture and independency criteria.

In a partitioned software design, the applications of lower DAL level must not perturb the application of higher level (in term of integrity and availability). Spatial and temporal partitioning is then implemented to ensure segregation among software partitions of different levels.

7.4.2.4 CMA

The common cause analysis is composed of the CMA and the complementary zonal safety and particular risks analyses.

7.4.2.4.1 Foundations of the Analysis

The aim of the CMA is to demonstrate that the risk induced by a common fault impairing independence mechanisms implemented within the actual design is reduced to an acceptable level.

In the CMA, independence mechanisms used within the SSA are verified to be effective against common mode failures. The analysis investigates the effects of design implementation, manufacturing, and maintenance errors—and failures of system components which defeat those independence principles.

The CMA covers the following common mode aspects:

- Concept and design errors
- Manufacturing
- Installation/integration
- Operation
- Maintenance
- Test
- Calibration
- Environmental

All of these common mode aspects are issued from ARP4761 [4] and are detailed in table 49.

7.4.2.4.2 CMA Method

The method to perform the CMA is issued from ARP4761 [4] and is purely qualitative. This method consists of:

- Identifying the FHA FC and associated independences mechanisms:

    - Identify the CAT FCs issued from FHA.
    - For each FC, identify the independence mechanisms that permit reducing the occurrence to a common mode failure. Those independence mechanisms can be intrinsic to a system architecture, but some are required from external systems (typically power supply systems, cooling systems, etc.). For the latter, the independence assessment is not under airframer responsibility.

- Checking that these independence mechanisms are not impaired by a common fault identified in the hazard checklist (see table 49).

7.4.2.4.3 Hazard Checklist

The following hazard checklist is issued from ARP4761 [4]. The applicability of each common failure mode or error is established with regard to:

- System architecture (mainly the technology used).
- Work-sharing with airframer (aircraft implementation, Particular Risks Analysis, and Zonal Safety Analysis remain under airframer's responsibility, with the support of the system supplier).

Table 49. Hazard checklist

COMMON MODE TYPES	COMMON MODE SUB TYPES	EXAMPLES OF COMMON MODE SOURCES	EXAMPLES OF COMMON MODE FAILURES/ERRORS
CONCEPT AND DESIGN	DESIGN ARCHITECTURE	Common discharge header	Common discharge failure
		Common external sources (ventilation, electrical power)	Failure of common external sources
		Equipment protections	Designer failure to predict an event
		Operating characteristics (normal running, standby)	Inadequate operating mode
	TECHNOLOGY, MATERIALS, COMPONENT/EQUIPMENT	New, sensible	General design error
		Component type (size material)	Hardware error
		Software	Software error
		Component use	Usage out of prescribed domain
		Internal conditions (T° ranges)	Usage out of operating ranges (T, P)
		Initial conditions	Out of range
	SPECIFICATIONS	Origin	Origin error (human), lack of specific protection in equipment design
		Requirements	Requirement errors, Defective specification

Table 49. Hazard checklist (continued)

COMMON MODE TYPES	COMMON MODE SUB TYPES	EXAMPLES OF COMMON MODE SOURCES	EXAMPLES OF COMMON MODE FAILURES/ERRORS
MANUFACTURING	MAKER	Personnel	Common error due to manufacturer, error because of inadequately trained personnel
	PRODUCTION	Process/Procedure	Incorrect process, Inadequate manufacturing control, inadequate inspection, inadequate testing
INSTALLATION/ INTEGRATION AND TEST	FITTER	Fitter	Installation error
	PROCEDURES	Installation phase	Common error because of phase
	LOCATION	Same zone	Local failure or event
	ROUTING	Routing	
OPERATION	STAFF	Staff	Error due to inadequately trained personnel, overstressed or disabled operator
	PROCEDURES	Procedure	Faulty operating procedures, misdiagnosis (following wrong procedure), omission of action, incorrect or inadequate commission of action
MAINTENANCE	STAFF	Staff	Error due to inadequately trained personnel, incorrect human action
	PROCEDURES	Procedure	Failure to follow repair procedures, defective repair procedure, lack of repair procedures
TEST	STAFF	Staff	Error due to inadequately trained personnel, incorrect human action
	PROCEDURES	Procedure	Faulty test procedure

Table 49. Hazard checklist (continued)

COMMON MODE TYPES	COMMON MODE SUB TYPES	EXAMPLES OF COMMON MODE SOURCES	EXAMPLES OF COMMON MODE FAILURES/ERRORS
CALIBRATION	STAFF	Staff	Error due to inadequately trained personnel
		Calibration Tools	Inadequate tools adjustment
	PROCEDURES	Procedure	Failure to follow calibration procedures, defective calibration procedure, lack of calibration procedures
ENVIRONMENTAL	MECHANICAL AND THERMAL	Temperature	Fire, lightning, welding equipment, cooling system faults, electrical short circuits
		Grit	Airborne dust, metal fragments generated by moving parts with inadequate tolerances
		Impact	Pipe whip, water hammer, missiles, structural failure
		Vibration	Machinery in motion
		Pressure	Explosion, out of tolerance system changes (pump overspeed, flow, blockage)
		Humidity	Steam pipe breaks
		Moisture	Condensation, pipe rupture, rainwater
		Stress	Thermal stress at welds of dissimilar metals, thermal stresses

Table 49. Hazard checklist (continued)

COMMON MODE TYPES	COMMON MODE SUB TYPES	EXAMPLES OF COMMON MODE SOURCES	EXAMPLES OF COMMON MODE FAILURES/ERRORS
ENVIRONMENTAL	ELECTRICAL AND RADIATION	Electromagnetic	Welding equipment, rotating electrical machinery, lightning, interfaces power supplies
		Radiation	Gamma radiation, charged particle radiation
		Conducting medium	Medium moisture, conductive gases
		Out-of-tolerance	Power surge voltage, short circuit, power surge current
	CHEMICAL/BIOLOGICAL	Corrosion (acid)	Leak of acid used in maintenance for removing rust and cleaning
		Corrosion (oxidation)	Moisture around metals
		Other chemical reactions	Galvanic corrosion, complex interactions of fuel cladding, water, oxide fuel
		Biological	Poisonous gases, animate causes (mussels in heat exchanger)

Note: additional environmental hazards (e.g., tire burst, rotor burst, bird strike) covered by Particular Risks Analysis are not included in this analysis.

The hypothesis is made that the equipment environmental qualification is adequately specified according to the equipment severity and environment. Thus, environmental common modes are mainly covered by specific qualification tests.

7.4.3 SEE Analysis

The objective of this assessment is to demonstrate that the system is adequately mitigated against SEEs. Such mitigation can be achieved through architectural system considerations, equipment design, component selection, component testing, or a suitable combination thereof.

7.4.3.1 Terminology and Definitions

EASA [1] defines SEE as:

> Atmospheric radiation is a generic term that refers to all types of electromagnetic radiation that can penetrate the earth's atmosphere. The main contributors to atmospheric radiation are solar and galactic radiation. Solar radiation is emitted from the sun and galactic radiation originates from outside our solar system. Both types of radiation can be affected (distorted or bent) by the earth's magnetic field.
>
> SEE occur when atmospheric radiation, comprising high-energy particles, collide with specific locations on semiconductor devices contained in aircraft systems. Memory devices, microprocessors, and FPGAs are most sensitive to SEE.
>
> Some examples of these types of effects are SEU, MBU, SEGR, and SEB. However, SEU and MBU are the two single effects that present the largest potential threat to aircraft systems.
>
> The rates of SEE are likely to be greater on aircraft flying at high altitudes and high geographic latitudes. This is due to the effects of atmospheric absorption and magnetic deflection of solar and galactic radiation. Although the intensity of atmospheric radiation varies with altitude and geographic latitude, the high-energy particles are randomly distributed at any given location. As a result, the predicted SEE rates can be derived based on the characteristics of the aircraft equipment (number of vulnerable elements) and operating conditions (altitude, latitude).

The effect of atmospheric radiation is one factor that could contribute to equipment loss or malfunction. From a system safety perspective, the existing methodology covering random failures (FMEA/FMES and FTA, see sections 7.4.1 and 7.4.2.1) is used in the assessment of atmospheric radiation effect rates and consequences [1].

This assessment considers the normal atmospheric radiation levels, which could be experienced during a typical flight, and not those which could be experienced during a solar flare.

As stated in EASA SEE CM [1] and information bulletins [108 and 109], solar flares that result in large bursts of solar particles arriving in the atmosphere—creating a significant increase in atmospheric radiation, with higher levels than that normally expected and of a short duration (order of hours)—should result in operational limitations relating to the routing of the flight (i.e., avoiding high latitudes).

Reference [3] provides the descriptions of SEE types and consequences listed in table 50 and table 51.

Table 50. SEE types

SEE Type	Description
Single Event Upset	Occurs in a semiconductor device when the radiation absorbed by the device is sufficient to change a cell’s logic state.
MBU	Occurs when the energy deposited in the silicon of an electronic component by a single ionizing particle causes upset to more than one bit in the same logical word.
MCU	Occurs when the energy deposited in the silicon of an electronic component by a single ionizing particle induces several bits in an IC to fail at one time.
SEL	Occurs in a four layer semiconductor device 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. Regardless of the applied input power, the fixed state is latched up until the device is powered down. Such latch up may be destructive or non-destructive.
SEGR	Occurs in the gate of a powered insulated gate component when the radiation charge absorbed by the device is sufficient to cause gate rupture, which is destructive.
SEB	Occurs when a powered electronic component or part thereof is burnt out as a result of the energy absorption triggered by an individual radiation event.

Table 51. SEE consequences

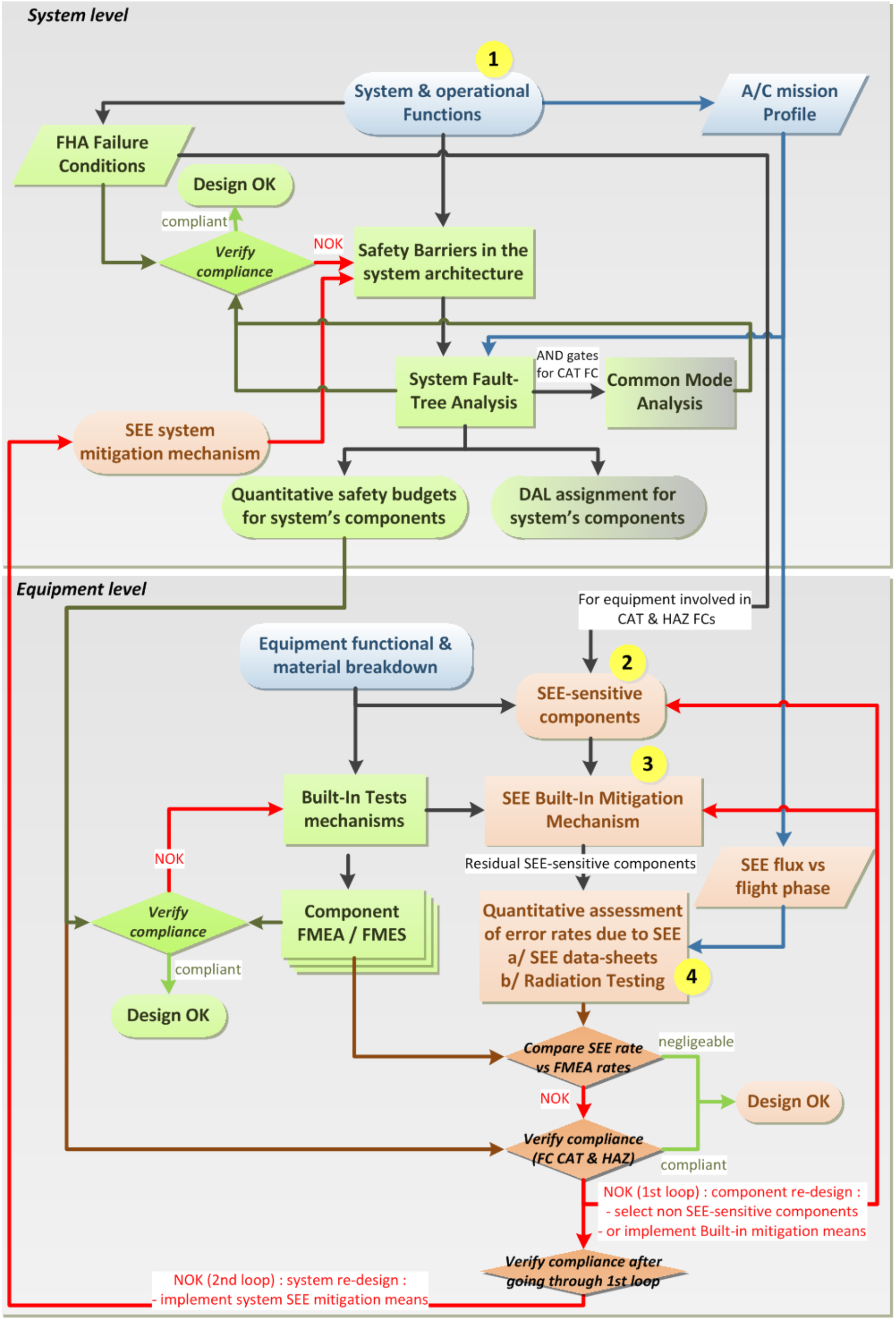
SEE Occurrence	Consequence
SET	A spurious signal or voltage induced by the deposition of charge by a single particle that can propagate through the circuit path during one clock cycle.
Single Event Functional Interrupt	Upset usually in a complex device, for example, a microprocessor, such that a control path is corrupted, leading the part to cease to function properly.

7.4.3.2 SEE Analysis Method

Figure 58 recalls the proposed SEE analysis method. Figure 59 references steps that have been covered in the project’s previous deliverables. Figure 60 focuses on the steps associated with the system-level analysis and figure 61 with the equipment level.

At system level, the preparation phase includes the description of the system and its operational functions. The environment in which the system is intended to be operated is defined within the aircraft mission profile. In accordance with ARP4761 [4], FHA-derived FCs at system level are then retrieved based on the system and its functions. A first inner loop consists of verifying compliance with the safety objectives associated with the FCs of the SBs implemented in the system architecture. The verification uses a system fault-tree analysis and includes SEE mitigation techniques.

The system fault-tree analysis is the input for the CMA to be performed for AND gates, CAT FC, and the determination of quantitative safety budgets and associated DAL for each system component. The analysis then shifts from the system to the equipment level.



System level
1
System & operational Functions
A/C mission Profile
FHA Failure Conditions
Design OK
compliant
Verify compliance
NOK
Safety Barriers in the system architecture
System Fault-Tree Analysis
AND gates for CAT FC
Common Mode Analysis
SEE system mitigation mechanism
Quantitative safety budgets for system's components
DAL assignment for system's components
Equipment level
For equipment involved in CAT & HAZ FCs
Equipment functional & material breakdown
2
SEE-sensitive components
3
Built-In Tests mechanisms
SEE Built-In Mitigation Mechanism
NOK
Residual SEE-sensitive components
SEE flux vs flight phase
Verify compliance
Component FMEA / FMES
Quantitative assessment of error rates due to SEE a/ SEE data-sheets b/ Radiation Testing
4
compliant
Design OK
Compare SEE rate vs FMEA rates
negligeable
NOK
Design OK
Verify compliance (FC CAT & HAZ)
compliant
NOK (1st loop) : component re-design :
- select non SEE-sensitive components
- or implement Built-in mitigation means
Verify compliance after going through 1st loop
NOK (2nd loop) : system re-design :
- implement system SEE mitigation means

Figure 58. Proposed SEE safety analysis process

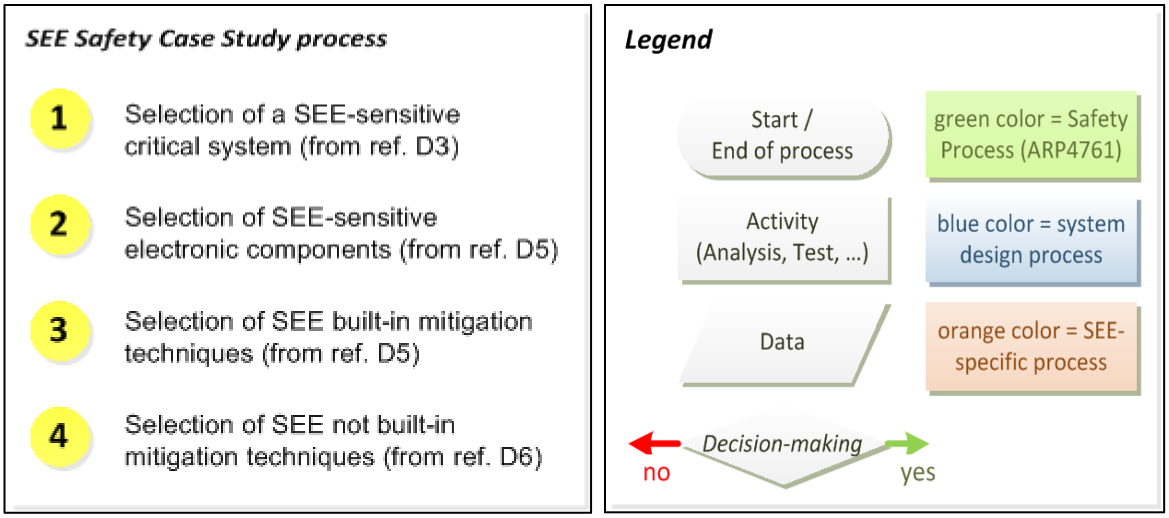

SEE Safety Case Study process
1
Selection of a SEE-sensitive critical system (from ref. D3)
2
Selection of SEE-sensitive electronic components (from ref. D5)
3
Selection of SEE built-in mitigation techniques (from ref. D5)
4
Selection of SEE not built-in mitigation techniques (from ref. D6)
Legend
Start / End of process
green color = Safety Process (ARP4761)
Activity (Analysis, Test, ...)
blue color = system design process
Data
orange color = SEE-specific process
Decision-making
no
yes

Figure 59. SEE safety process tags for the sample SSA and legend from figure 2

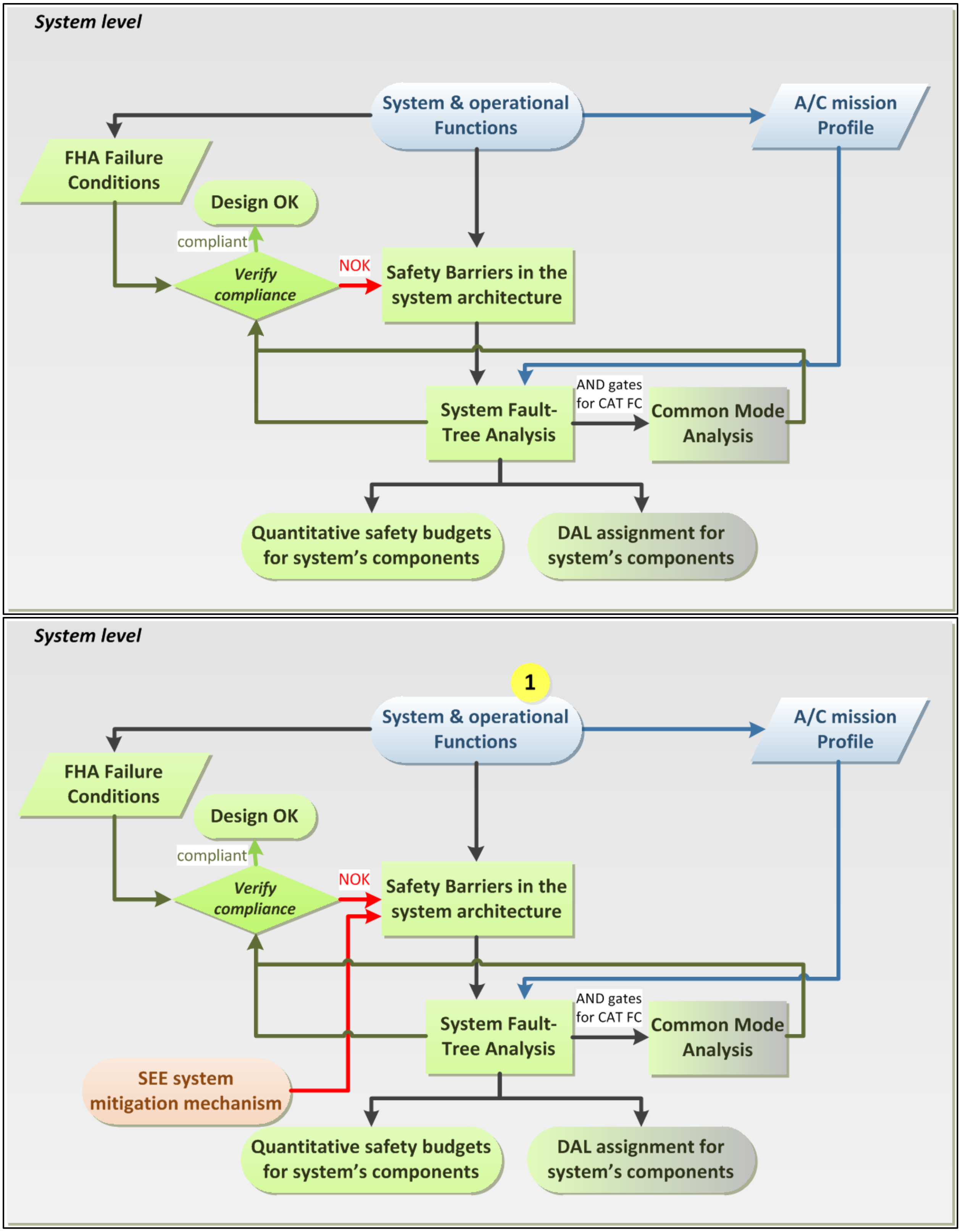

System level
System & operational Functions
A/C mission Profile
FHA Failure Conditions
Design OK
compliant
Verify compliance
NOK
Safety Barriers in the system architecture
AND gates for CAT FC
System Fault-Tree Analysis
Common Mode Analysis
Quantitative safety budgets for system's components
DAL assignment for system's components
System level
1
System & operational Functions
A/C mission Profile
FHA Failure Conditions
Design OK
compliant
Verify compliance
NOK
Safety Barriers in the system architecture
AND gates for CAT FC
System Fault-Tree Analysis
Common Mode Analysis
SEE system mitigation mechanism
Quantitative safety budgets for system's components
DAL assignment for system's components

Figure 60. Safety analysis process at system level (with/without SEE analysis)

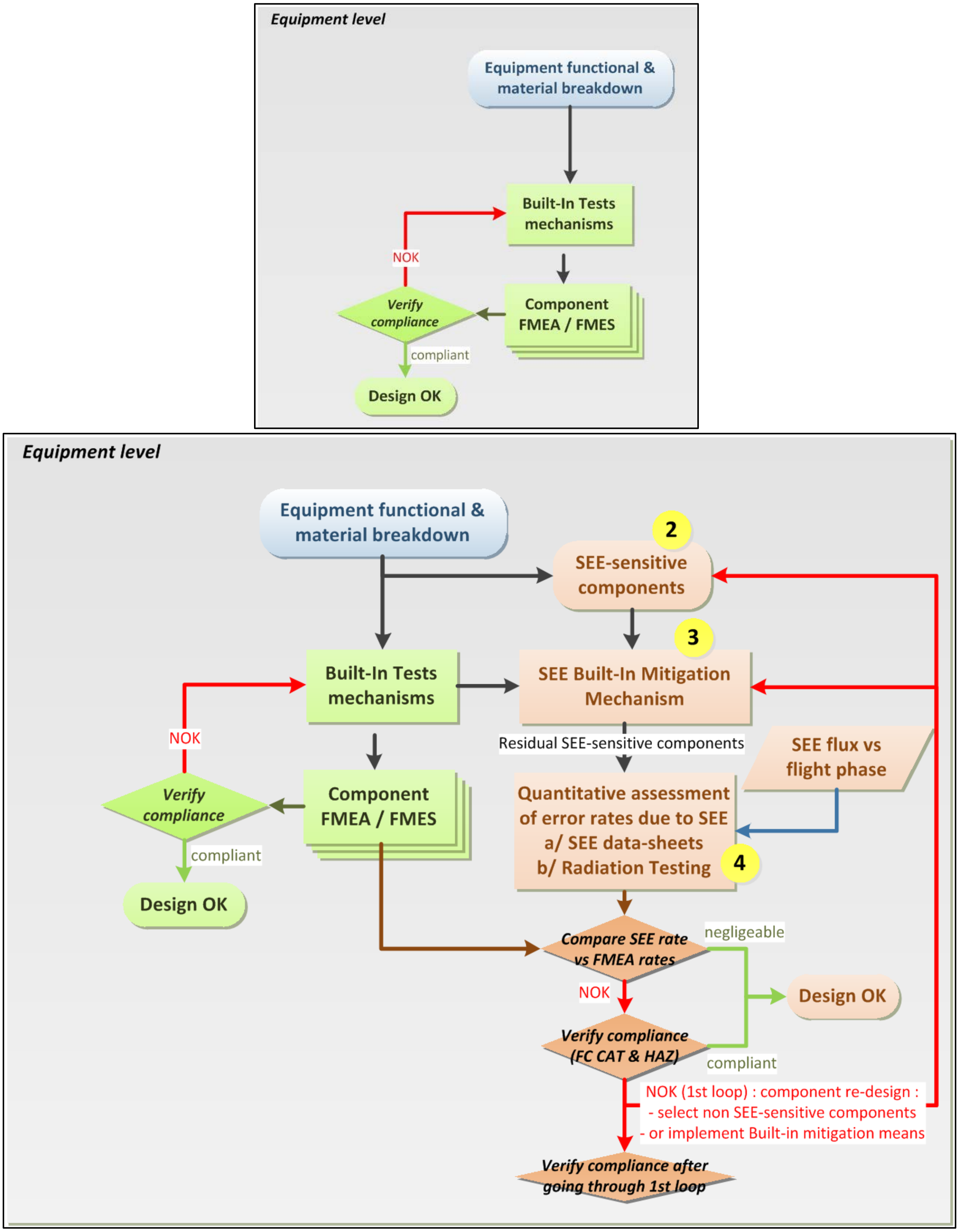

Equipment level
Equipment functional & material breakdown
Built-In Tests mechanisms
NOK
Verify compliance
Component FMEA / FMES
compliant
Design OK
Equipment level
Equipment functional & material breakdown
2
SEE-sensitive components
3
Built-In Tests mechanisms
SEE Built-In Mitigation Mechanism
NOK
Residual SEE-sensitive components
SEE flux vs flight phase
Verify compliance
Component FMEA / FMES
Quantitative assessment of error rates due to SEE
a/ SEE data-sheets
b/ Radiation Testing
4
compliant
Design OK
Compare SEE rate vs FMEA rates
negligeable
NOK
Design OK
Verify compliance (FC CAT & HAZ)
compliant
NOK (1st loop) : component re-design :
- select non SEE-sensitive components
- or implement Built-in mitigation means
Verify compliance after going through 1st loop

Figure 61. Safety analysis process at equipment level (without/with SEE analysis)

- At system level, a top-down analysis based on the safety assessment process described in section 7.4.2 in accordance with ARP4761, leading to identify safety objectives to components:
    - Assessment of FHA requirements
    - Determination of aircraft mission profiles and specific routes
    - Assessment of SBs necessary to meet the FHA safety requirements
    - Assessment of DAL objectives and safety quantitative budgets for system components, based on system fault-tree analysis
    - Assessment of system equipment involved in CAT and HAZ FCs
- At equipment level, the aim of a bottom-up analysis:is determination of SEE-sensitive components (memory cells, registers, etc.) for all equipment involved in CAT and HAZ FCs.
    - For these components, a qualitative analysis aims to:
        - Assess the safety mechanisms (hardware/software) implemented to mitigate their effects.
        - Identify residual SEE-sensitive components.
    - For these residual SEE-sensitive components, a quantitative analysis aims to:
        - Assess the SEU/MBU probability of occurrence face to the potential functional effects on the equipment, either through SEE data-sheet or radiation testing, depending on available analyses.
        - Summarize the impact of SEU/MBU analysis on the equipment FMEA/FMES analyses: if the SEE quantitative impact on equipment FMEA/FMES analyses is not negligible, SEE quantitative figures have to be integrated in the fault-trees to demonstrate compliance with system fault-tree budgets.

- The development of an iterative assessment, at system and equipment level, which aims to:
  - Integrate quantitative results of SEE impacts in the budgets of the system fault-tree analysis.
  - Define and implement specific design protections either at equipment or system level if the SEE error rate is shown to be too high to demonstrate compliance with system safety objectives.

7.4.3.2.1 Focus on the System Level

At system level, the preparation phase includes the description of the system and its operational functions. The environment in which the system is intended to be operated is defined within the aircraft mission profile. In accordance with ARP4761, FHA-derived FCs at system level are then retrieved based on the system and its functions. A first inner loop consists of verifying compliance with the safety objectives associated with the FCs of the SBs implemented in the system architecture.

The verification that the implemented system is compliant with safety objectives is performed through the PSSA and SSA. The verification of quantitative safety objectives is based on the system FTA. The objective of the PSSA is to establish the safety requirements of the system and determine whether the proposed architecture can reasonably be expected to meet the safety objectives identified by the FHA; the PSSA FTA generally uses quantitative budgets for the products, which are refined as safety objectives at equipment level (see figure 5). The SSA is based on PSSA FTA and uses the quantitative values obtained from the FMES on the products to demonstrate previous quantitative budgets for FTA.

SEE-related demonstration activities are mainly performed at equipment level (see overall process described in figure 2). In some cases, the SEE analysis will highlight the need for specific SEE mitigation techniques (which may also provide additional passivation means for intrinsic random failures of the components) to be implemented at system level. These mitigation means must be reintegrated in the SBs, in the system architecture, and the verification of safety objectives must be reassessed through a new FTA, taking into account these new SBs.
The system FTA is the input for the CMA to be performed for AND gates of CAT FC, the determination of quantitative safety budgets, and the determination of Functional Failure Sets and associated DAL for each system component (in accordance with ARP4754A). The analysis then shifts from the system to the equipment level.

As the effect of atmospheric radiation is one factor that could contribute to equipment loss or malfunction, SEE safety assessment concerns only quantitative assessments (FMEA/FMES and FTA) aiming to cover random failure effects [1].

This leads to three concerns:

1. EASA SEE CM [1] states the susceptibility to SEE should be assessed for systems or equipment capable of causing or contributing to CAT or HAZ FCs at aircraft level. However, IEC TS 62396-1 [3] states SEE assessments should be performed based on the DAL of the systems and with more rigor on the quantitative assessment for DAL A and DAL B systems.

   The recommended criteria to select systems or equipment for which SEE safety analysis will be performed is their involvement in CAT or HAZ FCs rather than their DAL. This is based on the following:

   a. DAL levels aim to cover software and hardware systematic errors, whereas SEEs result in stochastic events, addressed by the system FTA. The list of items involved in CAT or HAZ FCs is a direct outcome of the FTA.
   b. According to ARP4754A [7], DAL A to DAL C items may be involved in the functional failure sets of a CAT FC. A DAL C system contributing to a CAT FC will then be selected for SEE assessment with the recommended criteria (involvement in CAT FC), whereas it may be excluded with the DAL-based criteria.

Therefore, the criteria pointing to items involved in CAT or HAZ FCs, as determined by the FTA, is the more exhaustive and consistent regarding the nature of SEE events.

2. At system level, the CMA is not impacted by new SEE assessments. In fact, SEE effects due to normal atmospheric radiation levels could contribute only to random failures within a single equipment and could not concurrently affect several independent hardware equipment (see section 7.4.3.1). Only extreme solar flare events, which produce additional neutrons within the atmosphere and thus increase the overall atmospheric neutron flux for short periods, may be susceptible to severely impacted system architectural features, such as redundancy or monitoring. Therefore, CMA (see section 2.2.2), which focuses on system mitigation means pertaining to common faults impairing independence mechanisms inside a system, will only treat solar flare impacts. To conclude, as recommended by EASA SEE CM [1], mitigation means against solar flare are implemented at aircraft operational level and not at system level.
3. As the normal atmospheric radiation level effects (either for SEU or for MBU types) are expected to be limited to one component perimeter, SEE effects that may propagate from one component to another will be passivated by safety mechanisms already implemented to cover functional effects of intrinsic random failures or errors. Therefore, no specific qualitative assessment of SEE effects propagation is required in the last update of EASA SEE CM [1].

7.4.3.2.2 Focus on Equipment Level

Each piece of equipment is described in terms of its function and materials. For CAT and HAZ FCs, an SEE safety analysis needs be performed. SEE-sensitive components as well as built-in mitigation techniques are identified. From the aircraft mission profile description, the strategy to either fix the SEE (i.e., implement mitigation actions to remove the SEE) or to continue flying without mitigating the SEE can be defined and input into the quantitative SEE safety assessment. This strategy has to be defined with regard to the system safety objectives (e.g., privileging availability or integrity of the function).

Alongside the SEE safety assessment, taking into account built-in test mechanisms, component-level FMEA is performed to verify the compliance of the equipment design with the derived safety objectives.

To verify the compliance of the design, including the SEE safety assessment results, the SEE rates resulting from the quantitative assessment are compared to the failure rates derived from the FMEA for a verified design. If the SEE rates are negligible, the design is compliant; if the SEE rates are not negligible, the compliance is verified with the top-level safety objectives resulting from the system-level quantitative safety assessment for CAT and HAZ FCs. The proposed criteria to determine whether SEE rates are negligible is a difference of an order of magnitude, namely:

$$\text{Error Rate (SEE)} < \frac{\text{Failure Rate (FMEA)}}{10} \tag{11}$$

Note that types of component technology used and previous “in service” history may be taken into account to demonstrate compliance with SEE certification objectives for equipment previously used on certificated aircraft so that this equipment may be out-of-scope of the SEE quantitative assessment [1].

The steps for the SEE analysis method follow:

If there is compliance, the design is considered adequate. Otherwise, redesign needs to be considered either at system level (e.g., implementation of system-level not-built-in mitigation techniques) or at component level (e.g., selection of component that is less SEE-sensitive or SEE-immune, implementation of built-in mitigation techniques).

7.5 SAFETY ANALYSES

7.5.1 Significant Single Failures Analysis

This analysis is documented in the FMEA report, which is typically not within the scope of an SSA because the analysis is performed at the equipment level. Therefore, this report is out of scope. The general methodology for FMEA is described in section 7.4.1.1.

7.5.2 Significant Multiple FCs Analysis

7.5.2.1 Fault-Tree Analysis

Table 52 summarizes the safety quantitative assessment of CDS FCs. Details of a fault tree diagram's structure are provided in appendix D.

In accordance with ARP4761 [4], the probability of occurrence of an FC is calculated for the "Average Flight" defined in section 7.2.4.1 ("Fault-Tree result per flight" column) and is afterwards divided by the "Average Flight" duration in Flight Hours to obtain the "Average Probability per Flight Hour" ("FC Result per Flight Hour" column). This last quantitative value is then used in conjunction with the hazard category/effect established by the FHA to determine if it is compliant with the FC being analyzed.

Table 52. FTA quantitative analysis synthesis

FC ref.	FT ref.	FC	Severity	Quantif. Obj.	Fault-Tree result per flight	FC Result per Flight Hour	Compliant
FC01	FC01 _HAZ	Total loss of cockpit primary displays	HAZ	1E-07	1E-08	3E-09	YES
FC02	FC02 _MAJ	Total loss on primary display of any displayed parameter on both cockpit sides	MAJ	1E-05	7E-08	2E-08	YES
FC03	FC03 _HAZ	Erroneous display on one primary display of any critical parameter (Airspeed, Barometric Altitude, Attitudes)	HAZ	1E-07	4E-07	1E-07	YES
FC04	FC04 _CAT	Erroneous display on primary display of any critical parameter (Airspeed, Barometric Altitude, Attitudes) on both cockpit sides	CAT	1E-09	5E-14	1E-14	YES
FC05	FC05 _MAJ	Erroneous display on primary display of any non-critical (including navigation and engine parameter) parameter	MAJ	1E-05	1E-05	3E-06	YES
FC06	FC06 _HAZ	Total loss of engine parameters display for all engines	HAZ	1E-07	3E-07	7E-08	YES
FC10	FC10 _CAT	Total loss of any critical parameter (Airspeed, Barometric Altitude, Attitudes) display on both cockpit sides combined with loss of standby display	CAT	1E-09	4E-13	1E-13	YES
FC11	FC11 _CAT	Erroneous display on one primary display of any critical parameter (Airspeed, Barometric Altitude, Attitudes) combined with a failure of standby display	CAT	1E-09	4E-11	9E-12	YES

As indicated in the last column of table 52, all results are compliant with the safety objectives.

7.5.2.1.1 Basic Events Used in the Fault Trees

Table 53 synthesizes all the basic events used in the FTA, their associated generic failure rates (see section 7.5.2.1.2), and their probability of occurrence per flight. The trees are included in appendix D.

Table 53. Basic events used in the fault tree diagrams

Basic event	Description	Type of event	Generic failure rate identification	Failure rate (λ)	Exposure period
'CD Err behav'	Erroneous CD Behavior	basic	DU_CPU_Err	1E-06	Flight
'CD Graphic froz'	Graphic Engine Frozen CD	basic	DU_graphic_frozen	5E-07	Flight
'CD inab to detc IR Loss'	Erroneous IR Healthy Status	dormant	DU_healthy_loss	5E-07	AC_Life
'CD LCD Frozen'	CD LCD Frozen	basic	DU_LCD_frozen	1E-07	Flight
'CD LCD Lum Off Loss'	Inability to Switch Off CD LCD Back-Lighting	dormant	DU_LCD_frozen_Mon_loss	5E-07	AC_Life
'CD Loss'	Total Loss of Central DU	basic	DU_Complete_Loss	1E-04	Flight
'CD Reset Loss'	Inability to Reset the DU	dormant	DU_inab_to_reset	5E-07	AC_Life
'Cockpit cooling'	Loss of Cockpit Cooling System	external	-	0E00	Constant
'DC EMER Loss'	DC Emergency Bus Loss	external	-	0E00	Constant
'DC1 ESS Loss'	DC1 Essential Bus Loss	external	-	0E00	Constant
'DC2 Loss'	DC2 Bus Loss	external	-	0E00	Constant
'ENG_SYS param Loss'	Loss of Engine Parameters (out-of CDS scope)	external	5.00E-08	5E-08	Flight
'IESI Err Behav'	Standby Erroneous Behavior	external	1.00E-05	1E-05	Flight
'IESI tot Loss'	Standby Complete Loss	external	1.00E-05	1E-05	Flight

Table 53. Basic events used in the fault tree diagrams (continued)

Basic event	Description	Type of event	Generic failure rate identification	Failure rate (□	Exposure period
'IL A429 loss'	Loss of ARINC 429 Acquisition	basic	DU_ARINC_input_ Loss	2E-06	Flight
'IL Complete Loss'	Inboard Left DU Loss	basic	DU_Complete_Loss	1E-04	Flight
'IL Err behav'	Erroneous IL Behavior	basic	DU_CPU_Err	1E-06	Flight
'IL Eth Loss'	Loss of Ethernet Acquisition	basic	DU_Ethernet_input_ Loss	2E-06	Flight
'IL Feedback loss unan'	Inability for IL to Post the "CHECK" Message & Alert FWS	dormant	DU_inab_to_aware_ of_fdb_trig	5E-07	AC_Life
'IL Graphic froz'	Graphic Engine Frozen IL	basic	DU_graphic_frozen	5E-07	Flight
'IL inab to detc CD Loss'	Erroneous CD Healthy Status	dormant	DU_healthy_loss	5E-07	AC_Life
'IL inab to detc OL Loss'	Erroneous OL Healthy Status	dormant	DU_healthy_loss	5E-07	AC_Life
'IL LCD Frozen'	IL LCD Frozen	basic	DU_LCD_frozen	1E-07	Flight
'IL LCD Lum Off Loss'	Inability to Switch off IL LCD Back-Lighting	dormant	DU_LCD_frozen_M on_loss	5E-07	AC_Life
'IL Reset Loss'	Inability to Reset the DU	dormant	DU_inab_to_reset	5E-07	AC_Life
'IR A429 loss'	Loss of ARINC 429 Acquisition	basic	DU_ARINC_input_ Loss	2E-06	Flight
'IR Err behav'	Erroneous IR Behavior	basic	DU_CPU_Err	1E-06	Flight
'IR Eth Loss'	Loss of Ethernet acquisition	basic	DU_Ethernet_input_ Loss	2E-06	Flight
'IR Feedback loss unan'	Inability for IR to Post the "CHECK" Message & Alert FWS	dormant	DU_inab_to_aware_ of_fdb_trig	5E-07	AC_Life
'IR Graphic froz'	Graphic Engine Frozen IR	basic	DU_graphic_frozen	5E-07	Flight
'IR inab to detc OR Loss'	Erroneous OR Healthy Status	dormant	DU_healthy_loss	5E-07	AC_Life

Table 53. Basic events used in the fault tree diagrams (continued)

Basic event	Description	Type of event	Generic failure rate identification	Failure rate (□	Exposure period
'IR LCD Frozen'	IR LCD Frozen	basic	DU_LCD_frozen	1E-07	Flight
'IR LCD Lum off Loss'	Inability to Switch off IR LCD Back-Lighting	dormant	DU_LCD_frozen_ Mon_loss	5E-07	AC_Life
'IR Loss'	Inboard Right DU Loss	basic	DU_Complete_Los s	1E-04	Flight
'IR Reset Loss'	Inability to Reset the DU	dormant	DU_inab_to_reset	5E-07	AC_Life
'OL A429 Loss'	Loss of ARINC 429 Acquisition	basic	DU_ARINC_input_ Loss	2E-06	Flight
'OL Complete Loss'	Outboard Left DU Loss	basic	DU_Complete_Los s	1E-04	Flight
'OL Err Behav'	Erroneous OL Behavior	basic	DU_CPU_Err	1E-06	Flight
'OL Graphic Froz'	Graphic Engine Frozen OL	basic	DU_graphic_frozen	5E-07	Flight
'OL LCD Frozen'	OL LCD Frozen	basic	DU_LCD_frozen	1E-07	Flight
'OL LCD Lum off Loss'	Inability to Switch off OL LCD Back-Lighting	dormant	DU_LCD_frozen_ Mon_loss	5E-07	AC_Life
'OL Reset Loss'	Inability to Reset the DU	dormant	DU_inab_to_reset	5E-07	AC_Life
'OR A429 Loss'	Loss of ARINC 429 Acquisition	basic	DU_ARINC_input_ Loss	2E-06	Flight
'OR Err Behav'	Erroneous OR Behavior	basic	DU_CPU_Err	1E-06	Flight
'OR Eth Loss'	Loss of Ethernet Acquisition	basic	DU_Ethernet_input _Loss	2E-06	Flight
'OR Feedback Loss Unan'	Inability for OR to Post the "CHECK" Message & Alert FWS	dormant	DU_inab_to_aware _of_fdb_trig	5E-07	AC_Life
'OR Graphic Froz'	Graphic Engine Frozen OR	basic	DU_graphic_frozen	5E-07	Flight
'OR LCD Frozen'	OR LCD Frozen	basic	DU_LCD_frozen	1E-07	Flight

Table 53. Basic events used in the fault tree diagrams (continued)

Basic event	Description	Type of event	Generic failure rate identification	Failure rate (□	Exposure period
'OR LCD Lum off Loss'	Inability to Switch Off OR LCD Back-Lighting	dormant	DU_LCD_frozen_Mon_loss	5E-07	AC_Life
'OR Loss'	Outboard Right DU Loss	basic	DU_Complete_Loss	1E-04	Flight
'OR Reset Loss'	Inability to Reset the DU	dormant	DU_inab_to_reset	5E-07	AC_Life
'RCP Man EWD Left Loss'	RCP Failure Resulting in the Loss of Left EWD Manual Activation	dormant	RCP_XFRreconf_Loss	1E-06	AC_Life
'RCP Man EWD Right Loss'	RCP failure resulting in the loss of Right EWD Manual Activation	dormant	RCP_XFRreconf_Loss	1E-06	AC_Life
'RCP Man MFD Left Loss'	RCP Failure Resulting in the Loss of Left ND/SD Manual Reconfiguration	dormant	RCP_MFD_NDSD_PB_loss	1E-06	AC_Life
'RCP Man MFD Right Loss'	RCP Failure Resulting in the Loss of Left ND/SD Manual Reconfiguration	dormant	RCP_MFD_NDSD_PB_loss	1E-06	AC_Life
'RCP Man PFD/ND Left Loss'	RCP Failure Resulting in the Loss of Left PFD/ND Manual Reconfiguration	dormant	RCP_XFRreconf_Loss	1E-06	AC_Life
'RCP Man PFD/ND Right Loss'	RCP Failure Resulting in the loss of Right PFD/ND Manual Reconfiguration	dormant	RCP_XFRreconf_Loss	1E-06	AC_Life

IESI = integrated electronic standby instrument

7.5.2.1.2 Failure Rates Justification

Table 54 provides the list of failure rates used in the FTA and the justification (LRUs FMEA/ safety analyses) of the figures used in the diagrams (see appendix D).

Table 54. List of failure rates used in the FTA and justification means

Failure rate code	Failure rate budget	Failure rate description	Component	Failure rate verification	Verification source
DU_ARINC_Input_Loss	2.0E-06	Loss of any or all A429 inputs	CPM	1.0E-06	DU FMEA
DU_Complete_Loss	1.0E-04	Complete loss of the DU	All	8.0E-05	DU FMEA
DU_CPU_Err	1E-06	Erroneous behavior of the DU core processor (CPU and A429 acquisition)	CPM	5.0E-07	DU FMEA
DU_Ethernet_Input_Loss	2.0E-06	Loss of Ethernet data reception or transmission	CPM	1.0E-07	DU FMEA
DU_Graphic_Frozen	5.0E-07	Erroneous behavior of the graphic processing inducing erroneous graphic data (frozen data)	GGM	3.0E-07	DU FMEA
DU_Healthy_Loss	5.0E-07	Erroneous healthy status sent by one DU (OK instead of KO) to other DUs	CPM	5.0E-07	DU FMEA
DU_Inab_to_Aware_of_fdb_Trig	5.0E-07	Inability to trigger the feedback sanction (CHECK message)	CPM	5.0E-07	DU FMEA
DU_Inab_to_Reset	5.0E-07	Inability to reset the DU (CBIT sanctions)	CPM	4.0E-07	DU FMEA
DU_LCD_Frozen	1.0E-07	Frozen display due to LCD failure	LAM	1.0E-07	DU FMEA
DU_LCD_Frozen_Mon_Loss	5.0E-07	Loss of LCD monitoring	CPM	4.0E-07	DU FMEA

Table 54. List of failure rates used in the FTA and justification means (continued)

Failure rate code	Failure rate budget	Failure rate description	Component	Failure rate verification	Verification source
RCP_MFD_NDSD_PB_ Loss	1.0E-06	Loss of any RCP pushbutton (stuck to open)	RCP	8.0E-07	Control Panels FMEA
RCP_XFRreconf_Loss	1.0E-06	Loss of any RCP switch pushbutton	RCP	8.0E-07	Control Panels FMEA

CBIT = continuous built-in test

7.5.2.1.3 Dormant Failures

Two types of dormant failures are considered: dormant failures with periodic check and dormant failures not necessitating periodic checks. The former category is not applicable for the example at hand. Table 55 summarizes the basic events that can be dormant without specific periodic check.

Table 55. Dormant failures not requiring periodic check

Basic event	Description	Exposure period
'CD Inab to Detc IR Loss'	Erroneous IR Healthy Status	AC_Life
'CD LCD Lum off Loss'	Inability to Switch off CD LCD Backlighting	AC_Life
'CD Reset Loss'	Inability to Reset the DU	AC_Life
'IL Feedback Loss Unan'	Inability of IL to Post the "CHECK" Message & Alert FWS	AC_Life
'IL Inab to Detc CD Loss'	Erroneous CD Healthy Status	AC_Life
'IL Inab to Detc OL Loss'	Erroneous OL Healthy Status	AC_Life
'IL LCD Lum off Loss'	Inability to Switch off IL LCD Backlighting	AC_Life
'IL Reset Loss'	Inability to Reset the DU	AC_Life
'IR Feedback Loss Unan'	Inability of IR to Post the "CHECK" Message & Alert FWS	AC_Life
'IR Inab to Detc OR Loss'	Erroneous OR Healthy Status	AC_Life
'IR LCD Lum off Loss'	Inability to Switch off IR LCD Backlighting	AC_Life
'IR Reset Loss'	Inability to Reset the DU	AC_Life
'OL LCD Lum off Loss'	Inability to Switch off OL LCD Backlighting	AC_Life
'OL Reset Loss'	Inability to Reset the DU	AC_Life
'OR Feedback Loss Unan'	Inability of OR to Post the "CHECK" Message & Alert FWS	AC_Life

Table 55. Dormant failures not requiring periodic check (continued)

Basic event	Description	Exposure period
'OR LCD Lum off Loss'	Inability to Switch off OR LCD Backlighting	AC_Life
'OR Reset Loss'	Inability to Reset the DU	AC_Life
'RCP Man EWD Left Loss'	RCP Failure Resulting in the Loss of Left EWD Manual Activation	AC_Life
'RCP Man EWD Right Loss'	RCP Failure Resulting in the Loss of Right EWD Manual Activation	AC_Life
'RCP Man MFD Left Loss'	RCP Failure Resulting in the Loss of Left ND/SD Manual Reconfiguration	AC_Life
'RCP Man MFD Right Loss'	RCP Failure Resulting in the Loss of Left ND/SD Manual Reconfiguration	AC_Life
'RCP Man PFD/ND Left Loss'	RCP Failure Resulting in the Loss of Left PFD/ND Manual Reconfiguration	AC_Life
'RCP Man PFD/ND Right Loss'	RCP Failure Resulting in the Loss of Right PFD/ND Manual Reconfiguration	AC_Life

7.5.2.1.4 Events Out-of-Scope

Table 56 summarizes all of the external events interfaced with the CDS system used in the FTA and their assumed failure rates. These interface requirements have to be validated at aircraft level.

Table 56. List of basic events out-of-scope

Basic event	Description	Type of event	Generic failure rate identification	Failure rate (□)	Exposure period
'Cockpit cooling'	Loss of Cockpit Cooling System	external	-	0.00E+00	Constant
'DC EMER Loss'	DC Emergency Bus Loss	external	-	0.00E+00	Constant
'DC1 ESS Loss'	DC1 Essential Bus Loss	external	-	0.00E+00	Constant
'DC2 Loss'	DC2 Bus LOSS	external	-	0.00E+00	Constant
'ENG_SYS param Loss'	Loss of Engine Parameters (out-of CDS scope)	external	5.00E-08	5.00E-08	Flight
'IESI Err Behav'	Standby Erroneous Behavior	external	1.00E-05	1.00E-05	Flight
'IESI tot Loss'	Standby Complete Loss	external	1.00E-05	1.00E-05	Flight

7.5.2.1.5 List of Basic Events Involved in CAT or HAZ FCs

Table 57 presents the CDS equipment that is within the scope of the FTA and the reference of the fault trees associated with the equipment's components.

Table 57. List of CDS equipment in-scope

Equipment involved	Component involved	Fault-Tree reference
DU	CPM	FC01_HAZ
		FC03_HAZ
		FC04_CAT
		FC06_HAZ
		FC10_CAT
		FC11_CAT
	GGM	FC03_HAZ
		FC04_CAT
		FC11_CAT
	LAM	FC03_HAZ
		FC04_CAT
		FC11_CAT
	DU (all modules)	FC01_HAZ
		FC03_HAZ
		FC04_CAT
		FC06_HAZ
		FC10_CAT
		FC11_CAT
RCP	Pushbuttons	FC06_HAZ
		FC10_CAT

Table 58. List of equipment out-of-scope

Systems	LRU involved	Fault-Tree reference
Standby flight instrument	IESI	FC10_CAT
		FC11_CAT
Aircraft cooling system	Cockpit cooling	FC01_HAZ
Aircraft engines	Engines control	FC06_HAZ
Electrical system	DC emergency	FC10_CAT
		FC11_CAT
	DC1 essential	FC01_HAZ
		FC03_HAZ
		FC04_CAT
		FC06_HAZ
		FC10_CAT
		FC11_CAT
	DC2	FC01_HAZ
		FC03_HAZ
		FC04_CAT
		FC10_CAT
		FC11_CAT

IESI = integrated electronic standby instrument

7.5.2.2 The DAL

This section presents the rationale that demonstrates that the CDS software and complex hardware assurance levels are in compliance with the severity of their functions.

Note: The synthesis for the system products DAL allocation is provided in table 59; if different DAL levels are allocated to a same LRU by its implication in several functions, the stringent DAL level will be allocated to the LRU in this synthesis. The DAL allocation methodology is described in section 7.4.2.3.

Table 59. DAL allocation for CDS

Function	LRU	Required DAL	Most severe related FHA failure case		Impact type
			Availability	Integrity	
Cockpit Primary Display	DU	B for display processing, A for monitoring	Essential (H) FC01 FC06	Critical (Airspeed, Baro-altitude, Attitudes) FC04 Essential (M) (other data than above) FC05	Level B required for display availability as combined with the failure of an independent back-up (IESI)
	RCP	C	Essential (M) FC02	N/A	Direct (management of DU formats)
	ECP	C	Essential (M) FC02	N/A	Direct (management of DU formats)

IESI = integrated electronic standby instrument

Table 60 shows the working assumptions for DAL allocation on system out-of-scope equipment.

Table 60. Working assumptions for DAL allocation on system out-of-scope equipment

Function	LRU	Required DAL	Most severe related FHA failure case		Impact type
			Availability	Integrity	
Cockpit Standby Instrument	IESI	B	Critical FC10	Critical FC11	Level B required as combined with the failure of an independent system (CDS)

IESI = integrated electronic standby instrument

According to RTCA DO-254 section 2.3.1 [6], the functional failure path analysis (FFPA) permits "[the justification of] a lower design assurance level for a portion of the hardware item."

Because the integrity of the critical parameter display on both cockpit sides is CAT (see table 59), feedback monitoring (described in section 7.3.2.3) has been implemented to prevent common mode failures between all DUs due to a single cause (software or hardware fault inside DU), leading to an undetected erroneous parameter display on the whole cockpit.

Each function involved in the FFPA is a developed level A or B and is monitored by an independent level A function (in accordance with ARP4754A). At software level, DAL A and DAL B software are segregated inside the DU (through temporal and spatial partitioning– SB_DU2).

All of the monitoring and sanction functions (fatal failure or backlighting switching off) are developed level A, which is compliant with the HAZ level required by the loss of all Cockpit Primary Displays (reference FC01).

The FFPA concerning the undetected erroneous display of critical parameters is provided in figures 62 and 63.

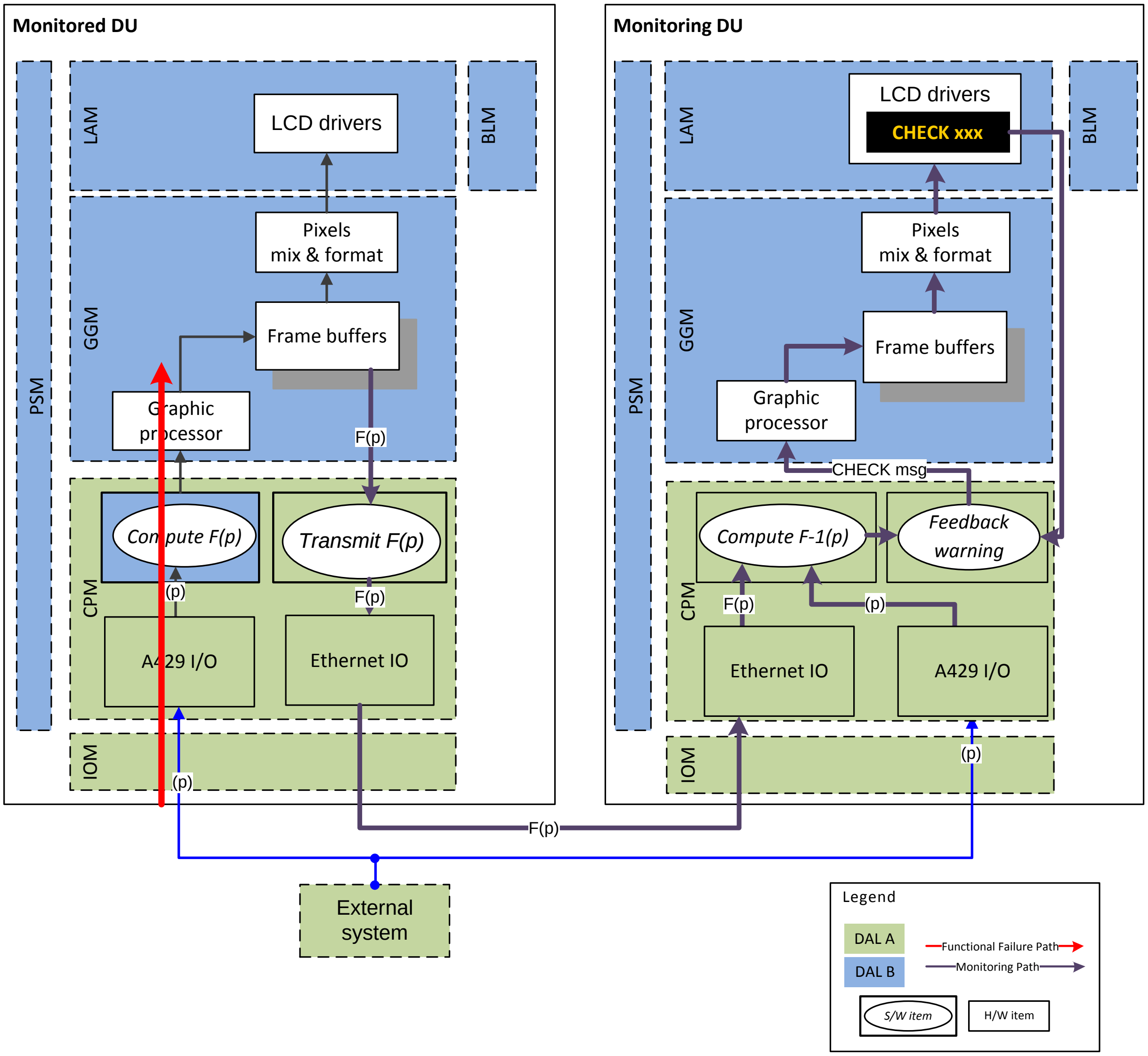


Figure 62. FFPA and DAL allocation at DU level (from IOM to graphic processor)

The red arrow in figure 62 depicts the functional failure path of an undetected erroneous display FC. The failure propagates through the architectural elements from the IOM to the graphic processor in the monitored DUs, as explained in section 7.3.3.1. The elements in blue are allocated a DAL B, whereas the elements in green are allocated a DAL A. The rationale for the allocation is provided below.

Because the IOM acquires raw data (*p*) for both the display channel and the feedback, it is DAL A. Because the CPM computes both *F(p)* in the monitored display and F-1(*p*) in the monitoring display, it is DAL A. According to the FFPA shown in figure 62, graphic processor failures covered by feedback monitoring and the CPM software may be developed DAL B, as monitored by independent hardware and software required DAL A.

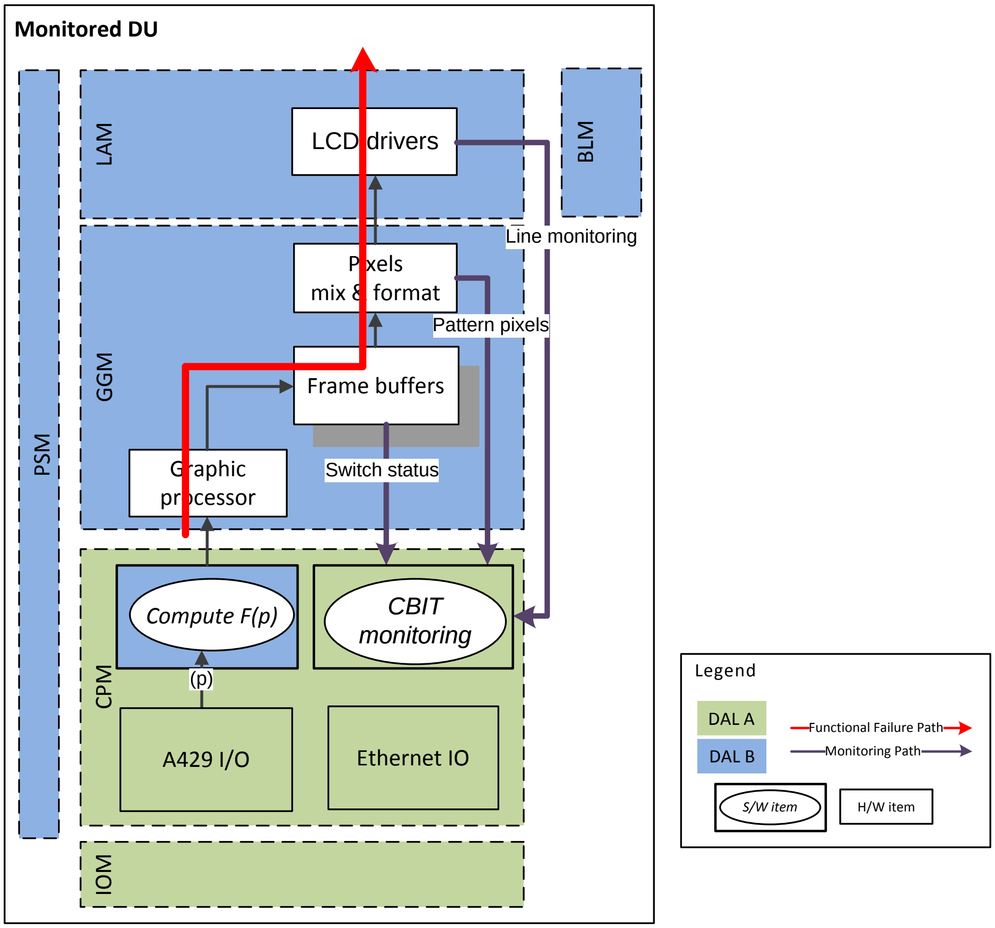


Figure 63. FFPA and DAL allocation at DU level (from GGM to LAM)

Figure 63 is a graphical depiction of the functional failure path regarding the undetected erroneous display FC through the architectural elements, from the graphic processor to LCD drivers inside a DU, as explained in section 7.3.3.1. The elements colored in blue are allocated a DAL B and the elements colored in green are allocated a DAL A. The rationale for the allocation follows.

Because of the independence principle between the graphic generation and display modules (graphic processor, frame buffers, pixels mix and format, and LCD drivers) and the monitoring mechanisms (internal cyclic monitoring mechanisms described in section 7.3.3.4) performed by the processor module that is DAL A, all DAL components included in GGM and LAM are B.

The errors of the other components (PSM, BLM, and non-monitored components of LAM) cannot lead to undetected erroneous display, but only to loss of display (HAZ FCs), so these components are required DAL B.

Table 61 summarizes DAL allocation and justification for all DU items.

Table 61. Summary of DAL allocation for DU components

Module	Component	Required DAL	Justification of DAL level
IOM	IO Acquisition	A	Involved in external feedback monitoring required DAL A
CPM	A429 I/O, Ethernet I/O	A	Involved in external feedback monitoring required DAL A
CPM	Core Computing Processor Hardware	A	Involved in external feedback monitoring and DU cyclic monitoring mechanisms required DAL A
	Monitoring Software	A	Involved in external feedback monitoring and DU cyclic monitoring mechanisms required DAL A
	Display Software	B	Monitored by external feedback (see section 7.3.2.3) performed by DAL A software embedded on DAL A hardware. At software level, DAL A and DAL B software are segregated inside the DU (through temporal and spatial partitioning – SB_DU2)
GGM	Graphic Processor	B	Monitored by external feedback (see section 7.3.2.3) performed by DAL A software embedded on DAL A hardware
	Frame Buffers	B	Monitored by DAL A hardware (see section 7.3.3.4.1)
	Pixels Mix & Format	B	Monitored by DAL A hardware (see section 7.3.3.4.2)
LAM	LCD Drivers	B	Monitored by DAL A hardware (see section 7.3.3.4.3)
	Screen	B	Failure of screen parts cannot lead to undetected erroneous display, but only to loss or degraded display (see section 7.3.3.4.4)
PSM	Secondary Power Supply	B	Failure of secondary power supply cannot lead to undetected erroneous display, but only to loss of display (see FMEA)
BLM	Backlighting	B	Failure of backlighting and dimming cannot lead to undetected erroneous display, but only to loss or degraded display (see section 7.3.3.4.4)

7.5.2.3 CMA

7.5.2.3.1 The SBs

The SBs are mechanisms implemented in the design of the CDS at system or equipment level to comply with the safety objectives defined in the FHA. For each CAT FC associated with the primary displays identified in section 7.2.5, table 62 lists the safety barriers required to achieve the quantitative safety objectives allocated to these displays. Independence principles further justify an AND gate combination of these SBs.

Table 62. The SBs used in fault-tree analysis summary

SB Designation	SB Description	Worst FHA Severity	Ref
SB_CDS1: Segregation between left and right cockpit sides, including aircraft power supply	The five PDUs are physically independent	CAT	FC04
SB_CDS3 feedback monitoring	Independence between monitoring and display chains Feedback monitoring between DUs of airspeed, altitude, and attitude parameters	CAT	FC04
SB_STBY1: Independence and segregation between cockpit primary displays and standby display	Dissimilarity between components used for IESI display part and CDS	CAT	FC10
		CAT	FC11

IESI = integrated electronic standby instrument; STBY = stand-by (display)

Note that SB_DU1 DU specific continuous built-in tests monitoring to cover the DUs functional channel from the graphic stage to the screen stage is not kept as an independence principle to be validated by the CMA, as the quantitative result of the FC FC04 is achieved only because of segregation between the left and right primary display sides (SB_CDS1).

7.5.2.3.2 Independence Assessment

For each independence principle (SB listed in table 62), the CMA analysis establishes the precautions that allow the decreasing of hazard occurrences and avoidance of common mode failure. The hazard checklist provided in table 49 is used as a baseline to perform the analysis.

Note: only an extract of the CMA assessment for SB_CDS3 feedback monitoring is provided here (hazards not related to system design, such as hazards due to operations and maintenance errors, are not analyzed). Table 63 covers mitigation means for the FC “undetected erroneous display.” The CMA assessment aims to verify the requirements of independence between the display channel and its monitoring feature (the feedback monitor).

Table 63. CMA assessment for SB_CDS3 feedback monitoring (extract)

COMMON MODE SUB TYPES	EXAMPLES OF COMMON MODE SOURCES	EXAMPLES OF COMMON MODE FAILURES/ ERRORS	POTENTIAL RISKS	ESTABLISHED PRECAUTIONS	FURTHER INVESTIGATION
DESIGN ARCHITECTURE	Common discharge header	Common discharge failure	None, such common mode does not impact the LRU integrity	N/A	No
	Common external sources (ventilation, electrical power)	Failure of common external sources	a) Failure of the electrical power supply may affect both DUs. b) Possible multiple equipment failure in case of loss of ventilation	a) DUs connected to different electrical buses; each DU monitors its power supply input b) Dissimilarity of data treatment of *p* and *F(p)*, the effect of a common mode failure on both DUs will have different functional effect between monitoring and monitored DU	No
	Equipment protections	Designer failure to predict an event	Possible loss of function or malfunction	Following the ARP 4754 guidance material and developing the equipment to DAL A & B guarantee the highest level of validation, verification, and traceability. Dissimilarity of data treatment of *p* and *F(p)*, the effect of a common mode failure on both DUs will have different functional effect between monitoring and monitored DU.	No
	Operating characteristics (normally running, standby)	Inadequate operating mode	Shutdown of operational mode leads to DU loss; does not impact integrity	N/A	No

Table 63. CMA assessment for SB_CDS3 feedback monitoring (extract) (continued)

COMMON MODE SUB TYPES	EXAMPLES OF COMMON MODE SOURCES	EXAMPLES OF COMMON MODE FAILURES/ ERRORS	POTENTIAL RISK	ESTABLISHED PRECAUTIONS	FURTHER INVESTI-GATION
TECHNOLOGY, MATERIALS, COMPONENT/EQUIPMENT TYPE	New, sensible	General design error	Possible loss of function or malfunction	a) Good service experience on similar avionics equipment b) Quality assurance means to preclude hardware design errors relying on DO-254 development process applied to DAL A equipment	No
	Component type (size material)	Hardware error	Hardware common mode failure may induce simultaneous function loss or malfunction in several equipment	a) Good service experience on similar avionics equipment b) Quality assurance means to preclude hardware design errors relying on DO-254 development process applied to DAL A & B equipment	No
	Software	Software error	Software common mode failure may induce simultaneous function loss or malfunction	a) Good service experience on similar avionics equipment b) Quality assurance means to preclude software design errors relying on DO-178 development process applied to DAL A equipment	No
	Component Use	Use of inadequate component given to specify the operating condition	Possible loss of function or malfunction	Adequate use of component for the intended functions within expected operating conditions	No
	Internal Conditions (T° ranges)	Usage out of operating ranges (T, P)	Internal overheating in one equipment may induce the ambient temperature to exceed the overheat threshold	Two internal monitoring checks of DU temperature	No

Table 63. CMA assessment for SB_CDS3 feedback monitoring (extract) (continued)

COMMON MODE SUB TYPES	EXAMPLES OF COMMON MODE SOURCES	EXAMPLES OF COMMON MODE FAILURES/ ERRORS	POTENTIAL RISK	ESTABLISHED PRECAUTIONS	FURTHER INVESTI-GATION
	Initial Conditions	Pin prog	None, Pin prog does not impact the integrity	N/A	No
MECHANICAL AND THERMAL	Temperature	Fire, lightning, welding eq., cooling system faults, electrical short circuits	Failure of several DUs in case of severe damage to some equipment	Monitoring checks of the internal DU temperature, which shuts it down in case of detected overheat	No
	Grit	Airborne dust, metal fragments generated by moving parts with inadequate tolerances	Contamination of equipment connectors with dust, particles, etc.	Adequate filters in avionics ventilation (aircraft hypothesis)	No
	Impact	Pipe whip, water hammer, missiles, structural failure	None, such common mode does not impact the LRU integrity	N/A	No
	Vibration	Machinery in motion	None, such common mode does not impact the LRU integrity	N/A	No
	Pressure	Explosion, out of tolerance system changes (pump overspeed, flow, blockage)	None, such common mode does not impact the LRU integrity	N/A	No
	Humidity	Steam pipe breaks	Bad contacts, functional failures => loss of functions or malfunction	LRU’s robustness is checked according to specified DO-160 qualification level	No

Table 63. CMA assessment for SB_CDS3 feedback monitoring (extract) (continued)

COMMON MODE SUB TYPES	EXAMPLES OF COMMON MODE SOURCES	EXAMPLES OF COMMON MODE FAILURES/ ERRORS	POTENTIAL RISK	ESTABLISHED PRECAUTIONS	FURTHER INVESTI-GATION
	Moisture	Condensation, pipe rupture, rainwater	Bad contacts, functional failures => loss of functions or malfunction	Robustness of LRUs is checked according to specified DO-160 qualification level	No
	Stress	Thermal stress at welds of dissimilar metals, thermal stresses	Loss of functions or malfunction	Robustness of LRUs is checked according to specified DO-160 qualification level	No

Table 63. CMA assessment for SB_CDS3 feedback monitoring (extract) (continued)

COMMON MODE SUB TYPES	EXAMPLES OF COMMON MODE SOURCES	EXAMPLES OF COMMON MODE FAILURES/ ERRORS	POTENTIAL RISK	ESTABLISHED PRECAUTIONS	FURTHER INVESTI-GATION
ELECTRICAL AND RADIATION	Electromagnetic	Welding equipment, rotating electrical machinery, high-power radio frequency transmitters, lightning, interfaces, power supplies	Common failure of several DUs in case of very strong lightning strike, high- intensity radiated field, or abnormal electrical transient	Robustness of LRUs is checked according to DO-160 qualification	No
	Radiation	Gamma radiation, charged particle radiation	SEE or solar flares leading to failure of multiple DUs (display channel and feedback monitor)	Against SEE: SEE affects only one LRU, so SEE will not affect independence principle between monitored and monitoring DUs, resulting in undetected erroneous display of critical data. SEE affecting only monitored DU will be detected by the monitoring DU (see section 7.2.3). SEE affecting only monitoring DU may result in monitor comparison error and a false "DU X/DU Y DISAGREE" alert detected by the flight crew. Against solar flares: As stated in EASA reference [1], solar flares may affect the independence principle between two DUs, resulting in an undetected erroneous display of critical data. They are mitigated through operational limitations related to the routing of the flight (e.g., avoiding high latitudes in the concerned geographic zones) for the duration of the solar flare event (see EASA information bulletins [108 and 109]).	No
	Conducting medium	Medium moisture, conductive gases	None, such common mode does not impact the LRU integrity	N/A	No
	Out-of-tolerance	Power surge voltage, short circuit, power surge current	None, such common mode does not impact the LRU integrity	N/A	No

7.5.2.3.3 CMA Results

The current analysis of the SBs permits them to demonstrate that the identified common mode failures leading to potential CAT feared events are reduced through the design/production process, architecture design, or procedure precautions:

- Good service experience
- High hardware and software DAL
- Dissimilarity of treatment between p/*F(p)* (CDS feedback monitoring)
- Dissimilarity and functional independence between primary cockpit displays and secondary standby

7.5.3 SEE Analysis

Because this analysis is performed within the framework of the SSA documentation, it will focus on tasks performed at system level (determination of inputs to SEE analysis at equipment level, SEE mitigation mechanisms collection, SEE quantitative assessment summary, and validation face to system top-level safety objectives).

7.5.3.1 SEE Neutron Flux Assessment

Based on the aircraft typical mission profile (latitude, flight level, etc.) provided in section 7.2.4.3, the computed neutron flux to be used in the SEE safety assessment is given in table 64.

Table 64. Neutron flux assessment

Maximum Altitude	Latitude	Neutron Flux
40,000 ft	45º	6000 n/cm^2/h in the 10–800 MeV range

7.5.3.2 List of SEE-Sensitive Components Inside the System

Table 65 provides the component list for the equipment involved in CAT or HAZ FCs (identified in section 7.5.2.1.5) that are considered SEE-sensitive. In particular, the following components/ technologies may be affected by SEE:

- Memories (RAM, flash memory, or ROM with large size are considered as non-sensitive technologies)
- Components with volatile parts (memory bits, registers, or latches) like FPGA, PLD, ASIC, and system-on-chip
- Microprocessor with cache memory

Table 65. List of CDS SEE-sensitive components

Module	Function	Item	SEE-sensitive?
IOM	DU in/out interfaces with external equipment, protection, and filtering	DU connectors	Not sensitive
		Passive components (resistances, diodes, capacitors)	Not sensitive
CPM	A429 IO interface	ASIC + RAM	Sensitive
	Ethernet IO interface	Ethernet bus	Not sensitive
	Processing resource for image computation	Microprocessor with on-chip cache memory	Sensitive
	Interfacing core processing unit with GGM and controlling memories	PLD BRIDGE	Sensitive
	Controlling microprocessor	Watch dog	Not Sensitive
	Memories	SDRAM	Sensitive
	Code memory unit	Flash PROM	Sensitive
	Non-volatile memory	EEPROM (with large feature size)	Not sensitive
GGM	Graphic processing	Graphic microprocessor	Sensitive
	Symbology memories	SDRAM	Sensitive
	Frame buffer 1	EPLD	Sensitive
	Frame buffer 2	EPLD	Sensitive
	Internal bus	Internal bus	Not sensitive
	Pixels mix & format	Graphical core	Not sensitive
PSM	Primary control	Filters, diodes	Not sensitive
	Secondary control	DC/DC convertor	Not sensitive
LAM	Non-volatile memory	EEPROM (with large size)	Not sensitive
	Internal bus	Internal bus	Not sensitive
	LCD drivers	Line/Column drivers	Not sensitive
	LCD matrix	LCD Matrix	Not sensitive
BLM	LCD illumination	Optical components	Not sensitive
	Time counter	EPLD + EEPROM	Sensitive
	Overheat protection	Thermal sensors	Not sensitive

SDRAM = synchronous dynamic random access memory

Knowing ECP/RCP architecture is limited to switches, buttons, and knobs transmission to dedicated DU; no SEE-sensitive component has been identified within the equipment.

7.5.3.3 SEE Mitigation Mechanisms

Table 66 identifies the SEE built-in mitigation mechanisms implemented in the DU for SEE-sensitive components and the assessment of SEU effects on the functional behavior of the DU (taking into account mitigation means). In particular, the following mitigation techniques are efficient against SEE impacting integrity or availability:

- Hardware mitigations:
  - Parity checks, cyclic redundancy checks on memory to protect integrity of critical data: they allow detection of SEU but will lead a reset of the impacted microprocessor → impact on the availability of the equipment
  - ECC: allows the detection and correction of the SEU → low impact on the availability of the equipment
  - ECC with scrambling: arrangement of bits of memory to guarantee that all MBU produce only "logical" SEU
  - FPGA RAM-based: internal triplication, scrubbing (periodic inspections and corrections)
- System mitigations:
  - Cyclic checksum, comparison, and voting mechanisms: cover impacts on system integrity (comparison with two pieces of equipment) and availability (vote with at least three pieces of equipment)
- Software defensive programming techniques:
  - Minimize the use of cache memory and provide a high refreshing period for critical data and status (prohibit latched status).
  - Periodic cyclic checksum of critical areas of memory.
  - Checks variable range, repeated calculations, and confirms critical data several times to overcome transient errors.
  - Provide external memory instruction cache to avoid erroneous writing on the memory.

The result of SEU in an electronic device is a change of state of one bit from 1 to 0 or vice versa. This bit flip can lead, if nothing is done, to different consequences, depending on where the bit is located. At the CDS level, the result can be an erroneous data or erroneous behavior of the program—leading to an undetected erroneous parameter display or inappropriate behaviors (e.g., false CHECK alerts raised).

Table 66. Identification of SEE built-in mitigation mechanisms

Module	Function	Item	Built-in mitigation mechanism	Potential effects of SEE (note 1)
CPM	A429 IO interface	ASIC + RAM	SEE impacting A429 IO interfaces may lead to erroneous data acquisition on one DU. No specific SEE monitoring is implemented as the effects are detected by the feedback monitoring for critical parameters (section 3.2.3).	Effects are detected through feedback monitoring for critical parameters and may lead in some cases to loss of the DU after cross-check of DUs by the pilots (minor). Effects are not detected for non-critical parameters and may then impact DU integrity (major).
	Processing resource for image computation	Microprocessor with on-chip cache memory	Protected by ECC on cache 1 and parity bit on cache 2. Critical data are stored on cache 1. Protected by system feedback monitoring (section 7.3.2.3).	Detected by equipment and system built-in mechanism and, without effects on integrity, may lead in some cases to loss of DU (minor)
	Interfacing core processing unit with GGM and controlling memories	PLD BRIDGE	EDAC (Reed Salomon algorithm) – section 7.5.3.3.1	Detected by equipment built-in mechanism and without effects
	Memories	SDRAM	EDAC (Reed Salomon algorithm), section 7.5.3.3.1, and spatial partitioning, section 7.5.3.3.2	Detected by equipment built-in mechanism and without effects
	Code memory unit	Flash PROM	FPROM code is loaded on SDRAM at DU start-up (on-ground)	Without effects: no impact on safety

Table 66. Identification of SEE built-in mitigation mechanisms (continued)

Module	Function	Item	Built-in mitigation mechanism	Potential effects of SEE (note1)
GGM	Graphic processing	Graphic microprocessor	None	Not detected: potential impact on safety (integrity effects)
	Symbology Memories	SDRAM	EDAC (Hamming algorithm) – section 7.5.3.3.1	Detected by equipment built-in mechanism and, without effects on integrity, may lead in some cases to loss of DU (minor)
	Frame Buffer 1	EPLD	RAM containing frequently refreshed data and frame buffer redundancy (different memories addressed) to build a complete image (7.3.3.4.1 and 7.3.3.4.2). Switching status sent to processing module is periodically refreshed to avoid inoperative sanction of monitoring.	Detected and, without effects on integrity, may lead in some cases to detected degradation (flickering) of image display (minor). RAM is frequently refreshed and the frame buffer is switched at each cycle. Some temporary SEE may not be detected if they impact the redundant frame buffer during a short time. This case has no safety impact on the DU.
	Frame Buffer 2	EPLD		
BLM	Time Counter	EPLD + EEPROM	CRC on EPLDs-RAM-based checks the code and reloads it in case of a detected problem.	Detected by equipment built-in mechanism and loss of DU (minor)

The design precautions are consistent with safety objectives to ensure the best function integrity/availability ratio.

Note1: the term “detected” used in the last column of table 66 refers to detection by the system and not a direct detection by the flight crew. In some cases, the detection by the system leads to an alert for the flight crew and procedures for them to apply, but the flight crew is not relied on to detect anomalies in the display.

7.5.3.3.1 Specific Volatile Memory Monitoring

The use of large volatile memory in the DU increases the need for the implementation of a specific mechanism for the detection of a possible corruption.

A correcting code is associated with each memory word of the processing data memory. Thanks to this code, an alteration of the memory word or correcting code content will be detected. Moreover, the correcting code contains a redundancy of the information so that the corrupted data (memory word or correcting code) can be restored in case of a single- or two-bit error.

The EDAC mechanism is performed by an EPLD or ASIC, which check and possibly correct the data in memory during the reading task of the CPU and send them to the processing CPU (see figure 64). During the writing task, the data are coded and stored in the memory. An EDAC mechanism also increases availability because any single bit failure has no effect on the software behavior.

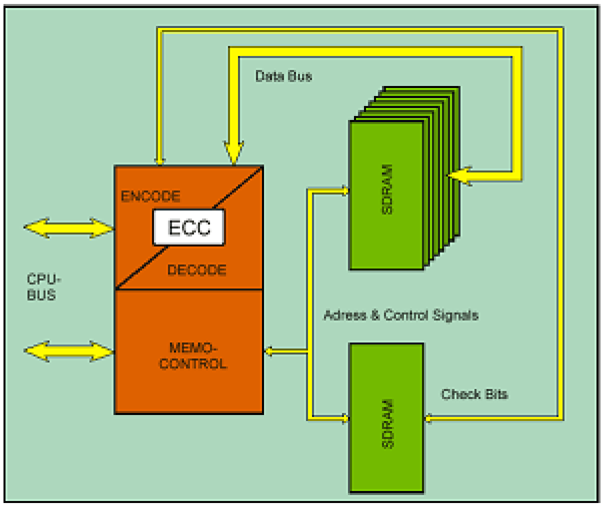


Figure 64. EDAC principle

With an EDAC Hamming algorithm, all the failures leading to the modification of one bit in a word are detected and corrected, all the failures leading to the modification of two bits in a word are detected, and some failures leading to the modification of more than two bits in a word are detected by the mechanism.

With an EDAC Reed Solomon algorithm, all the failures leading to the modification of all the bits in a word are detected by the mechanism. Then, a failure on a memory device has no impact on the equipment. All the failures leading to the modification of two bits in a word are detected and corrected.

On the DUs, an EDAC Reed Solomon algorithm is implemented on CPM (to cover SEE effects on SDRAM and PLD bridge) and an EDAC Hamming algorithm is implemented on GGM (to cover SEE effects on SDRAM).

7.5.3.3.2 The PLD Bridge Monitoring

A specific mechanism performed by the PLD bridge ensures that the spatial partitioning made by the memory management of the processor implemented on CPM will not be violated (fault propagation between partitions or between partition data and operating system data).

This window mechanism implemented in the PLD bridge protects memory areas from spurious write fault propagation from other partitions due to memory management failures by checking physical write access in SDRAM. Therefore, only a double failure of the microprocessor and the hardware PLD bridge may lead to erroneous spatial memory corruption of the CPM.

7.5.3.4 SEE Quantitative Assessment

The qualitative SEE safety analysis concluded that not all SEE-sensitive components were completely covered by SEE mitigation means. A quantitative SEE assessment is needed for the residual SEE-sensitive components that either are not covered or are only partially covered.

A quantitative computation of residual error rates based on the neutron flux identified in section 7.5.3.1 and technological characteristics of the component (supply voltage, bits number, cross-section) have been performed at component level. The following table summarizes the quantitative impact of SEE effects on FMEA/FMES analyses and FTA budgets and address the compliance with system safety objectives.

SEE impacting the residual non- or partially mitigated items that may have availability impacts or integrity impacts (only for the graphic processor) on the DU are detailed in table 67. Computations are performed with the assumption of an SEU rate, as their probability of occurrence is much higher than the MBU rate (which, by definition, must affect several bits and needs to lead to integrity issues).

Note that the traceability among the fault trees, FMEA failure rates, and SEU error rates is explained in appendix D.

Table 67. SEE quantitative assessment

Module	Item	Potential effects of SEE	SEU error rate (/fh)	FMEA failure rate (/fh)	Failure rate code	FTA budget (/fh)	Acceptable?
CPM	ASIC + RAM	Availability (MIN)	5.0E-07	1.0E-06	DU_ARINC_Input _Loss	2.0E-06	Yes, as covered by the FTA budget
		Integrity (MAJ)		5.0E-07	DU_CPU_Err	1.0E-06	Yes, as SEE error rate plus FMEA failure rate covered by the FTA budget
	Micro-processor with on-chip cache memory	Availability (MIN)	5.0E-07	8.0E-05	DU_Complete_Loss	1.0E-04	Yes, as negligible vs. FMEA failure rate
GGM	Graphic micro-processor	Integrity (HAZ)	Not computed as highly dependent on internal architecture	5.0E-07	DU_Graphic_Froze n	3.0E-07	See testing results
	SDRAM	Availability (MIN)	2.0E-07	8.0E-05	DU_Complete_Loss	1.0E-04	Yes, as negligible vs. FMEA failure rate
BLM	EPLD + EEPROM	Availability (MIN)	1.0E-05	8.0E-05	DU_Complete_Loss	1.0E-04	Yes, as SEE error rate plus FMEA failure rate covered by the FTA budget

Tests have been performed in the Theodor Svedberg Laboratory (TSL) at Uppsala University, Uppsala, Sweden. The testing conditions were:

- ASER-accelerated testing (accelerated soft error rate).
- With quasi mono-energetic neutron source (at 20, 50, 100, and 150 MeV).
- Neutron flux recorded based on a fission-based monitor.

These tests have shown that the behavior of the graphic processor under test, which is not covered by any SEE mitigation mechanism, is not affected by SEU or MBU. Although this GPU embeds internal memory units (registers, shared memory), these results are due to the unit's internal structure (as GPU is designed to accomplish several elementary tasks in parallel, rapidly manipulating a high number of memory locations).

7.5.3.5 SEE Assessment Conclusion

Qualitative and quantitative SEE assessments show that SEE are correctly mitigated at equipment and system level to comply with system safety objectives.

This quantitative assessment has been performed taking into account the contribution of external system malfunctions. These contributions are based on interface requirements detailed in section 7.2 and have to be validated at aircraft level.

7.5.4 Outcomes of Safety Assessment

7.5.4.1 Periodic Ground Check

This section addresses the assumptions and constraints stemming from the safety assessment related to aircraft maintenance.

No candidate certification maintenance requirements have been identified after the completion of the fault-tree analysis.

7.5.4.2 Aircraft Flight Manual Procedures

This section addresses the assumptions and constraints stemming from the safety assessment related to aircraft operations.

No specific assumptions related to aircraft operation have been identified after the completion of the safety analysis.

7.6 CONCLUSION ON SEE SSA FOR CDS

The objective of the research was to demonstrate the performance of an SEE analysis on an avionics system. The selected candidate was a CDS because it is involved in CAT and HAZ/MAJ FCs and comprised of components and integrated circuits impacted by different SEE types.

The implementation of the SEE analysis resulted in the demonstration that, given the current definition of the primary display system, no single failure induces a CAT event and the primary display system complies with all associated FCs, as required by AC 25.1309:

- The fault-tree analysis (see section 7.5.2.1) demonstrates that:
  - The architecture design of the primary display system based on the equipment FMEAs is compliant with all the safety objectives allocated in section 7.2.5.
  - No single hardware failure mode leads to a CAT FC.
- The qualitative CMA (see section 7.5.2.3) demonstrates that the identified common mode failures leading to potential CAT feared events are reduced through architecture principle, design, production processes, or procedure precautions.

8. RECOMMENDATIONS

8.1 INTRODUCTION

Table 68 lists the intermediate research deliverables associated with the steps of the safety assessment process in figure 2, for which each deliverable is identified with a numbered yellow circle. The detailed findings of these project deliverables are summarized in sections 3–7.

Table 68. Identification of project deliverables in SSA process

Circle ID	Project Deliverable and Content
1	Selection of SEE-sensitive components within aircraft/rotorcraft systems; documented in reference; see detailed research reported in section 3.
2	Description of SEE-sensitivity at component level, testing environment to obtain SEE rates, collection of mitigation technique(s); see detailed research reported in section 4.
3	Selection of SEE built-in mitigation technique(s); see detailed research reported in section 5.
4	Selection of SEE not-built-in mitigation technique(s); see detailed research reported in section 6.

Table 69 elicits a common format for the recommendations whereby the rationale is traced to the research and specific section of this report. Moreover, the recommendations are organized according to explicit elements of the safety assessment process.

Table 69. Proposed format for recommendations

Recommendation unique identifier SEE-Rec-NNN	Title
	Text for the recommendation
	Rationale for the recommendation, including reference to project deliverable(s).

8.2 SYSTEM AND OPERATIONAL FUNCTIONS

This category will also include the collection of information relative to the mission and, therefore, the determination of the radiation environment as it pertains to SEE.

8.2.1 Identification of System Functions

Recommendation unique identifier SEE-Rec-001	FCs requiring SEE analysis
	Require an SEE analysis for safety-critical equipment involved in FCs defined as CAT or HAZ
	Research reference: Section 3. subsections 3.2.2 and 3.3.3.2 ; section 7. subsection 7.4.3.2 Other reference: EASA CM [1] EASA CM initially required the performance of SEE analysis only for systems contributing to a CAT FC. The EASA position has evolved to include SEE analysis for equipment of DAL A to C (based on their contribution to CAT or HAZ FCs). This approach is coherent with the assimilation of SEE to quantifiable random failures rather than to defaults [109].

Note: The contribution of each piece of equipment to the FCs is to be identified as part of the SSA using cut-sets and fault-tree methods.

Recommendation unique identifier SEE-Rec-002	Level of details of system description
	When identifying system subfunctions relevant for the SEE analysis, the system description should have enough depth to include embedded micro-controllers within a traditionally mechanical structure.
	Research reference: Section 3. subsection 3.3.1 Integrating microcontrollers in mechanical elements is more common. Mechanical/hardware components are by nature SEE-immune, so by omitting the embedded circuits, the SEE analysis will be incomplete. This is in particular valid for rotorcraft.

8.2.2 Operational Functions

Recommendation unique identifier SEE-Rec-003	Reporting FCs from FHA
	The FCs resulting from the system-level FHA need to be reported as input to the SEE analysis
	Research reference: Section 7. subsection 7.4.3.2 Recommendation SEE-Rec-001 for selecting systems with CAT/HAZ FCs.

Recommendation unique identifier SEE-Rec-004	Inclusion of transitory functional failure in assessment
	The FHA needs to take into account transitory functional failures
	Research reference: Section 7. subsection 7.4.3.2 This recommendation is derived from the above because SEEs can generate such failures.

An example of the above recommendation is that the FHA of a fail-passive autopilot system needs to consider the erroneous operation of the monitored passive system.

Recommendation unique identifier SEE-Rec-005	Inclusion of human in the loop/level of automation considerations
	The description of system operations should include whether a human is in the loop or whether the system is fully automated
	Research reference: Section 5. subsection 5.3.2.3 The consequences of a non-detected/non-corrected SEE can be worse if the system is not accessible to the flight crew. Simple actions, such as reset or power cycling, can eliminate some SEEs. If the system is fully automated, a more rigorous estimation should be required for the determination of the SEE rate.

Recommendation unique identifier SEE-Rec-006	Consideration of interrupted operations
	The description of system operations should include whether the operations can be interrupted
	Research reference: Section 5. subsection 5.4.2.1 Some mitigation techniques will affect availability of the device. To make a judgment on the applicability and consequences of the mitigation on the system, knowledge of whether the device operations can be interrupted is relevant.

8.2.3 Mission Profile

Recommendation unique identifier SEE-Rec-007	Minimum mission profile information
	The information of the mission profile should include: - Vehicle type - Typical operating flight envelope: latitude and maximum altitude - Typical operating time - Life expectancy
	Research reference: Section 4. subsection 4.3.1.4 The justification for the estimation of neutron flux and the SEE rates is dependent on altitude/latitude/longitude and number of hours of operation. The mission profile is typically defined by the customer and includes operating flight envelope, type (aircraft, rotorcraft), typical operating time, and life expectancy.

8.2.4 Radiation Flux Estimation

The assumptions and references for the computation of the neutron flux value are a key element in the determination of SEE rates in the qualitative analysis. The justification for the flux value(s) should be part of the documentation provided by the system developer. The quantitative analysis is likely to require some level of testing. The reader is directed to section 8.5.

Recommendation unique identifier SEE-Rec-008	Usage of a single value for neutron flux
	The selection of a single value for neutron flux as applicable to the entire flight envelope should be accompanied by justification. In particular: - Applicability in terms of neutron flux energies - Applicability in terms of mission profile (e.g., altitude, latitude, longitude)
	Research reference: Section 5. subsection 5.3.1.1 Current norm recommends using 6000n/cm2 per hour as a conservative value for integrated flux. It is applicable to neutron energies greater than 10MeV and flight envelope up to 40,000 ft altitude and 45º latitude. When a more rigorous estimation of neutron flux is required, scaling and adjustments need to be applied.

Recommendation unique identifier SEE-Rec-009	Usage of scaling and/or adjustment(s) to neutron flux value
	Scaling and/or adjustments should be made on single conservative neutron flux value referenced in normative documents in some cases, including: - Extension of flight envelope (altitude and/or longitude) beyond the assumptions associated with the conservative flux value - Requirement for rigorous neutron flux estimation (e.g., related to criticality level) - Extension to include low-energy neutrons (thermal neutrons) - Semiconductor recommendation - Justification and source data for the adjustment to be provided.
	Research reference: Section 5. subsection 5.3.1.1 Justification for the estimation of flux regarding adjustment may include the use of a different data model, an update of the standard, in-situ measurement campaign results, or integration of proton influence. Other reference: draft AIR6219 [110] If the component integrates Boron-10, SEU may be caused by thermal neutrons (low energy neutrons) and not high-energy neutrons (that interact with silicon)

The following recommendation is generating some discussion. It is indeed very likely that the addition of a single worst-case scenario for solar flare will generate a non-compliance with the safety objectives. It is preferred that solar activity be addressed beyond the occasional level integrated in the neutron flux values using operational limitations (e.g., avoidance of higher altitude during strong solar activity).

Recommendation unique identifier SEE-Rec-010	Consideration of solar flares
	Depending on the mission profile, solar flare may be addressed separately from the neutron radiation analysis. It can be through the development of a single worst-case scenario for solar flare or the provision of operational limitations.
	Research reference: Section 4. subsection 4.3.1.4 The sun can affect the intensity of the neutron flux during high solar flare activity. Normally, the flux density in the analysis includes occasional periods of solar flares. Other reference: draft AIR6219 [110] A single worst-case scenario for solar flare may be required. Other reference: EASA SIB [109] Operators should be aware of a potential increase in apparent random failures.

8.3 IDENTIFICATION OF SEE-SENSITIVE COMPONENTS

8.3.1 Types of SEE

Recommendation unique identifier SEE-Rec-011	Types of SEE to be considered for analysis
	All types of SEE should be considered. The analysis should provide justification when an SEE type was not considered.
	Research reference: Section 3. subsection 3.3.2.1 All integrated circuits should be considered for SEE. High-voltage components (> 200V) should be included in SET and SEB analysis. Other reference: draft AIR6219 [110] All types of SEE should be considered as an input to the design phase (to select the part and determine appropriate mitigation(s)). The analysis should start with all types of SEE and justify when a certain type was not considered.

Recommendation unique identifier SEE-Rec-012	Types of SEE error rates to be considered for analysis
	Both soft and hard SEE error rates need to be considered in the analysis.
	Research reference: Sections 2 and 5. SEE error rates can be soft or hard: both types need to be considered. The SEFI and SEL (non-destructive) may be recovered by cycling/resetting, reloading configuration register, etc. This may not be considered as a failure but needs to be covered in the analysis.

Recommendation unique identifier SEE-Rec-013	Description of SEE impact
	The description of the SEE impact on the system needs to be stated.
	Research reference: Section 2. Description of impact is relevant to assess the criticality of the SEE on the operation of the component (note, for example, if SEE is removed with reset/cycling, need to check that the system in which the component is used can sustain the number of resets/cycling).

Not all electronic components are affected by all SEEs. It is therefore relevant to analyze which SEE types are relevant to the components in the system. Table 4 proposes a rolled-up view of the relationship between SEE types and several electronic components most commonly used to perform main functionalities in a circuit. This may help the system designer sub-select the analysis to be performed based on the circuit functions to be protected. Furthermore, the sub-selection of applicable types of SEEs and circuit functions may guide the designer toward mitigation technique(s) most likely to be employed. This table, as well as the previous one, is not exhaustive.

Recommendation unique identifier SEE-Rec-014	Coherence between SEE types, technology, and environmental conditions
	The consideration of SEE should be coherent with the technology and environmental factors that affect their likelihood of occurrence.
	Research reference: Section 3. subsection 3.3.3.1 and section 4. subsection 4.3.1.1

Table 1 proposes the major dependencies that exist between SEE types, technology, and environmental factors. Not all SEE types have evident correlation, such as SEFI, which can stem from various sources. The table can be used by system developers as a reminder to pay specific attention when obtaining substantiation information (e.g., temperature testing for SEL and SEB).

8.3.2 Architecture and Design Information

The development lifecycle phase called “requirement capture” is paramount to the completeness and design-to-fit aspects; if the requirements are unclear, then SEE analysis is likely to be incomplete, uncertainty leads to over-conservatism in the design, and design becomes unfeasible or no longer affordable (see section 4).

Recommendation unique identifier SEE-Rec-015	Minimum design elements to be collected for SEE analysis
	Design elements that need to be collected for the estimation of SEE error rates include: - Manufacturer - Part number - Feature size - Density (e.g., number of bits for a memory cell) - Component usage (including aging)
	Research reference: Section 5. subsection 5.3.2.1 Improvement of mitigation at component level can be offset by increased density. For example, DRAMs improved by a factor of 4–5 with each generation of cell, yet the system error rate remained unchanged because of the concurrent increase in density. For SRAM, lower power consumption and scaling led to an increased bit error rate with each generation until saturation with DSM technology, but the increase in memory density maintained the increase in system error rate. Research reference: Section 6. subsection 6.2.1 Aging should be taken into account so as to not underestimate FIT value. Research reference: Section 6. subsection 6.2.3.1 The identification of usage of the component is part of the identification of risk areas on the component (e.g., for memory: static, read-only, read/write, user programmable).

Recommendation unique identifier SEE-Rec-016	Claiming attenuation factors based on design
	Design elements that can be used to claim attenuation factors when computing SEE error rate include: - Exposure time (e.g., usage time, modes of operation) - Number of critical bits (“critical” needs to be further defined; for example, as “in use” or having a direct impact on instruction execution) - Derating factor from the manufacturer.
	Research reference: Section 5. subsection 5.4.1.1

Recommendation unique identifier SEE-Rec-017	Additional design information for SET analysis
	For SET sensibility assessment, the following design information should be collected: - Logic paths - Activation time windows (for clocked elements)
	Research reference: Section 4. subsection 4.2.1.1.4 SET can be masked by three items: logic masking (SET on non-sensitized path), latch window or timing masking (affects outside latching time window), and electrical masking (SET attenuated by subsequent logic gates until filtered out).

8.3.3 Collection of Existing SEE Information

Recommendation unique identifier SEE-Rec-018	Computation of a conservative “raw” SEE rate
	As a starting point to the SEE rate estimation, a conservative “raw” rate can be used; it is defined as: Raw SEE rate = neutron cross-section x integrated neutron flux (for device) Raw SEE rate = nb bits x neutron cross-section x integrated neutron flux (for cell)
	Research reference: Section 5. subsection 5.3.1 It is important to start with a conservative (but not overly conservative) value that can be estimated. In the quantitative phase, SEE rates should be provided by testing because analytical methods are unlikely to address all SEE and some SEE (e.g., SEL) are difficult to predict. In this case, the quantitative analysis will be detailed by SEE type for the types identified as critical. Research reference: Section 6. subsection 6.2.3.3.1 A raw assessment may be sufficient given the order of magnitude of the MTBF associated with the component; no further analysis refinement using derating is needed.

Recommendation unique identifier SEE-Rec-019	Acceptable units for SEE rate
	The units to express the SEE rate should be coherent with the level of depth of the analysis (e.g., cell, component, equipment), SEE type, and environmental assumptions.
	Research reference: Section 5. section 5.3.1.3 For SEE affecting bits (SEU, MBU), the cross-section is expressed in cm^2/bit. For SEE visible in the component response (SEL, SEFI, SET, SEB), the cross-section is expressed in cm^2/device. When using FIT/Mbit, the conversion factor of 7.1E17 Mbit.cm^2/FIT.bit should be used and carries an assumption of energy greater than 10MeV at New York City. At the equipment level, the SEE rate is characterized using MTBUR and/or MTBF.

Recommendation unique identifier SEE-Rec-020	Acceptable test data for the quantitative SEE analysis
	In the quantitative phase, SEE rates should be supported by testing data commensurate with the criticality of the system, environment (e.g., neutron flux), and types of SEE identified as critical.
	Research reference: Section 5. subsection 5.3.1 It is important to start with a conservative (but not overly conservative) value that can be estimated. In the quantitative phase, SEE rates should be provided by testing because analytical methods are unlikely to address all SEE—and some SEE (e.g., SEL) are difficult to predict. Research reference: Section 5. subsection 5.3.1.2 The cross-section is a function of the technology: the guidance on the determination of conservative cross-sections is wide. Datasheets from manufacturers should be sought whenever possible. Research reference: Section 5. subsection 5.3.1.4 When using simplified models applied across vendors and/or technologies, limit use to qualitative phase. SEE rates depend on technology (indigenous factors) and on design (exogenous).

Recommendation unique identifier SEE-Rec-021	Estimating SEE rate at equipment level from component rates
	The SEE rate value at the LRU level can be claimed to be the aggregate of the SEE rates of all SEE-sensitive components on the LRU.
	Research reference: Section 5. subsection 5.3 Typically, the SEE value at the LRU level is the aggregate of SEE rate(s) of all SEE-sensitive components that are used on the LRU. Research reference: Section 6. subsection 6.2.4.2 The contributions of the three sensitive elements to the overall chain SEU cross-section, σ, are assumed to be independent. This assumption is deemed reasonable based on the fact that the FF storage nodes are isolated by a built-in inverter and the gate capacitance of the transistors in the combinatorial logic does not affect the capacitance of the FF storage nodes.

8.3.4 Justification of SEE-Immunity

Recommendation unique identifier SEE-Rec-022	Substantiation of SEE immunity
	Claims of SEE-immunity should be substantiated by testing data.
	Research reference: Section 3. subsection 3.3.2.2 Immunity is typically demonstrated via testing because it is specific to the integrated circuit and semiconductor component. For immunity claims based on heavy ion testing and for silicon-based components, the reported LET should be higher than 15MeV-cm^2. High-energy neutron testing should report the absence of observed SEE (see issues with testing).

Recommendation unique identifier SEE-Rec-023	Claiming SEE immunity based on service experience data.
	Claims of SEE-immunity based on service experience data should be applied to systems for which the no-fault-found rate is very low.
	Research reference: Section 3. subsection 3.3.2.2 Other reference: EASA CM [1] EASA CM indicates that in-service experience can be used to claim credit on the quantitative analysis.

Recommendation unique identifier SEE-Rec-024	Indirect claims of SEE immunity
	Indirect claims of SEE-immunity can be based on the following information: - Similar related part of the same technology and feature size from the same manufacturer was successfully tested - Older non-volatile memories such as EEPROM and flash with larger feature sizes - Advanced alternative technologies (e.g., less sensitive material)
	Research reference: Section 3. subsection 3.3.2.2

8.4 ASSESSMENT OF SEE MITIGATION TECHNIQUES

The selection of the appropriate mitigation technique(s) is predicated on the development of SEE failure rates. The determination of these rates is a complex process that contains implicit clauses pertaining to the usability of the reliability data [111]. Furthermore, the availability of reliability data is widely varying according to the device manufacturers. Because these rates drive the selection of the device and its mitigation technique(s), substantiation of the approach should be commensurate with the safety objectives for the system (see section 6.7).

8.4.1 Justification for Selection of Mitigation Technique(s)

The challenges associated with the implementation of the mitigation technique(s) include the adequate assessment of the required safety and reliability values. To address potential tradeoffs, the designer must understand the intended use of the system to judge the acceptable time for detection of an SEE; the acceptable time to recover from an error; the acceptable level of penalty (performance, area, power, and monetary cost); the overall required level of performance at system level; and how the selection of mitigation technique(s) may impact the system design.

Recommendation unique identifier SEE-Rec-025	Elements to justify selection of mitigation technique(s)
	Justification for the selection of mitigation technique(s) include: • The prescribed or derived by allocation FIT rate or MTBF (safety and reliability). • The detection time of events (may impact the device time performance). • The means of detecting the event (may impact the device performance through penalties). • The recovery time after event detection (considering sensitivity to disruption). • The performance penalty, area penalty, and monetary cost of the mitigation solution(s). • The overall system performance. • The implications at system design level.
	Research reference: Section 5. subsection 5.4.2 and section 5.7

8.4.2 SEE Coverage

The research conducted under this task order collected mitigation techniques and investigated redundancy and ECCs in more detail. Table 5 proposes a concise view of the applicability of categories of mitigation to SEE types. The table is not exhaustive but is sufficient to direct the system developer toward a family type of mitigation to address certain SEEs. Section 2.3.3 provides additional details with regard to specific implementations within the family of mitigation techniques.

8.4.3 Specific Implementations

The type of SEE and the impacts to be mitigated lead to different implementations of the same family of mitigation.

8.4.3.1 Protection Against Excessive Current

This mitigation will directly impact the availability of the circuit when the power is switched off. If loss of data is an issue when the power in the circuit is re-established, additional mitigation to restore the data needs to be added. See table 6 for examples of implementations.

8.4.3.2 Horizontal Hardening

Horizontal hardening techniques require collaborating with the manufacturer when the product is not off-the-shelf. See table 7 for examples of implementations.

8.4.3.3 Vertical Hardening

Similar to horizontal hardening, vertical hardening techniques require collaborating with the manufacturer when the product is not off-the-shelf. See table 8 for examples of implementations.

8.4.3.4 Spatial Redundancy

Spatial redundancy provides reliability in the execution of instructions and computations because the operation is replicated and its results compared and (possibly) voted out. This mitigation technique is best-suited for computation-based applications. See table 9 for examples of implementations.

8.4.3.5 Temporal Redundancy

Implementation of temporal redundancy implies a negligible or small timing penalty, which is an advantage over spatial redundancy. Temporal redundancy is well-suited for communication-based applications. See table 10 for examples of implementations.

8.4.3.6 Parity Bits

Parity bits provide error detection but no error correction, so the affected area may no longer be usable after detection. If the error detection is followed by a mechanism to recopy data, then the technique introduces a timing penalty. See table 11 for examples of implementations.

8.4.3.7 ECCs

Simple ECCs do not protect against MCU and/or MBU. The fact that MBU and MCU are increasing may lead to the increase in complexity of the codes to a point at which cost, as well as non-compatibility with memories requiring fast access, becomes an issue. See table 12 for examples of implementations.

8.4.3.8 Scrubbing

Scrubbing is used for SEU/MBU in conjunction with ECCs or TMR to avoid an error accumulation beyond the capability of the mitigation technique.

8.4.3.9 Interleaving

Interleaving introduces complexity and delay in the circuit to the point at which the technique may not be compatible with access speed requirements. See table 13 for examples of implementations.

8.4.3.10 Reset/Cycling

The circuit is no longer available during reset or power cycling. In addition, the frequency of reset/cycling should be compatible with the component (e.g., aging). See table 14 for examples of implementations.

8.4.3.11 Design Margins

The margins are indicated in normative documents. Despite the implementation of margins, SEB have been observed. See table 15 for examples of design margins.

8.4.4 Trade-Space and Limitations

The determination of the effectiveness of the mitigation at the equipment level cannot be generalized; it is specific to the equipment because it depends on the code. However, a good starting point is the analysis at the elemental resources of the system.

As shown in table 5, the solution to mitigate SEE is a combination of mitigation techniques to balance SEE-type coverage with safety objectives and penalties. Sections 8.4.4.1 through 8.4.4.3 recall some common combinations and tradeoffs.

8.4.4.1 Spatial Redundancy

Research reference: Section 4. subsections 4.3.2.1 , 4.3.2.2, and 4.3.2.3.

The TMR is the most used mitigation technique and is highly efficient. However, its cost may limit its implementation to applications requiring high reliability. When the reliability requirements are lower, a mix of spatial redundancy and other techniques allows for the reduction of the penalties associated with TMR.

Figure 7 shows a tradeoff that can be performed on the voter in a redundant architecture for which protection against voter fault is not warranted.

Figure 8 illustrates the tradeoff analysis that can be performed in FFs to alleviate penalties from a fully triplicated architecture. Two approaches are shown: one to reduce the redundancy from triplication to duplication and accepting to lose protection after one instance is faulty, the other to focus the protection on critical elements and not the full circuit. With the latter, the proportion of SET is going to increase and glitch filtering needs to be added.

Figure 9 illustrates the tradeoff that can be analyzed for the logic circuit. The analysis consists of identifying parts of the circuit that can perform more than one function. It requires access to circuit design.

Figure 10 shows the tradeoff analysis that can be performed on asynchronous communication networks. The timing penalty is the key performance to be maintained—therefore, the replacement of spatial redundancy by temporal redundancy. This introduces sensitivity in the handshake to SEU and SET, which will require additional protection.

8.4.4.2 Soft Error Protection

Research reference: Section 4. subsection 4.3.3.

Figure 11 shows the tradeoff analysis that can be conducted on memory cells to achieve a satisfactory error-correction level and extend the SEE coverage to MBU and MCU types.

8.4.4.3 Summary Considerations for Tradeoffs

The tradeoffs are performed based on an assessment of the required reliability, the need to address only certain types of SEE, and the tolerance to penalties. Note that the tradeoff requires knowledge of the type of circuit (e.g., for communications, data storage, logic); its operations; and, for MCU risk assessment, knowledge of the cell layout is required.

Recommendation unique identifier SEE-Rec-026	Arguments to justify tradeoffs in selecting mitigation technique(s)
	Tradeoff in the selection of mitigation technique(s) can be justified by considering: - Required performance (reliability, availability, timing/speed) - Identification of critical types of SEE - Identification of critical subcomponents in the circuit
	Research reference: Section 4. subsections 4.3.2 and 4.3.3

When circuit layout is designed using tools (e.g., ASIC, FPGA), the user needs to be aware of the optimization options. Typically, these options will fight against redundancy. Moreover, verification of the proper implementation of redundancy, such as TMR, may not be sufficient with the tools and require verification at the netlist level using formal tools, fault injection/simulation, or ground radiation testing.

Recommendation unique identifier SEE-Rec-027	Impact of redundancy on verification method
	When a circuit is designed using redundancy as a mitigation technique, special care should be given to the method applied to the verification of the implementation of the redundancy.
	Research reference: Section 4. subsection 4.3.2.4.3

In performing the mitigation effectiveness assessment, the user should be aware of how the built-in data error and correction schemes are implemented and decide to implement the mitigation in the user-design or avoid the use of these schemes.

Recommendation unique identifier SEE-Rec-028	Additional information when using built-in ECCs with user-selectable feature
	System designer should obtain from the component manufacturer detailed information related to built-in error and correction schemes implementation, in particular when it includes user-selectable features.
	Research reference: Section 6. subsection 6.2.3.3.2 Built-in ECCs with user selectable feature impact the effectiveness of the mitigation and the design of the circuit around the component.

8.5 METHODS FOR ESTIMATION/TESTING

In general, the process for determining the impact of neutron particle flux on avionics is a combination of analysis, simulation, and testing. The ratio of each is dependent on the criticality of the system. In order of accuracy, these are: in the loop testing, LRU irradiation (propagation such as SEFI and SEL), and datasheet and static test compendiums for key elements (see section 2.4.7).

The measurement of the effectiveness is dependent on the testing method used. The methods exhibit various levels of fidelity that may forbid their use according to DAL. In addition, the number of hours in the testing facility and the number of testing facilities used to build the SEE rate play a role in the quality of the data.

Recommendation unique identifier SEE-Rec-029	Testing evidence as a function of DAL
	Evidence of testing should be commensurate with the FC or DAL of the system for which the SEE analysis is performed. In particular: - Testing at component and LRU level is recommended for DAL A. - Use of testing data on similar parts is acceptable for DAL B. - SEE fault modeling can be used for DAL C. - No SEE screening is required for DAL D and DAL E.
	Research reference: Section 5. subsection 5.3.2.2 The higher the DAL, the more rigorous the computation for the SEE rate needs to be.

Recommendation unique identifier SEE-Rec-030	Assessment of critical bits
	When a rigorous assessment of the SEE rate is required, critical bits can be assessed using the following three methods: - Computation of used resources - Fault-injection testing - Radiation testing
	Research reference: Section 5. subsection 5.4.1 A conservative method for an aggregated SEE rate is to multiply the single-bit SEE rate by the total number of bits. However, this does not qualify as rigorous because not all bits are equal. Critical bits are estimated by three methods: used resources, fault-injection, and radiation testing. Usage can be a conservative value for critical bits.

Recommendation unique identifier SEE-Rec-031	Additional justification when using heavy ion testing
	When heavy ion is used as the testing method to obtain the SEE rate, a reference for the transfer function used to obtain the neutron cross-section needs to be provided.
	Research reference: Section 5. subsection 5.5.3 Heavy ion testing cannot be used for neutron cross-section without model-based transformation.

Recommendation unique identifier SEE-Rec-032	Limiting laser beam testing
	Laser beam testing should be limited to determining SEU rates in the initial qualitative phase or in the monitoring phase.
	Research reference: Section 5. subsection 5.5.3 Laser beam testing results need to be transformed into SEU rates; there is, however, only limited correlation data to be referenced.

Recommendation unique identifier SEE-Rec-033	Using margins on static SEE rate
	If the data used to substantiate the SEE rate are built from generic static SEE data to which margins are applied, justification for the definition of the margins should be provided.
	Research reference: Section 5. subsection 5.5.4

Recommendation unique identifier SEE-Rec-034	Additional information when using service experience data
	If the data used to substantiate the SEE rate are obtained from in-service experience, the following information should be provided: - Justification that error is monitored on the component - Circumstantial data - Justification of an auditable process
	Research reference: Section 5. subsection 5.5.4 In-service data may be limited to components with ECC because it includes monitoring of error. Issues include the absence of the circumstantial data that impact the usability of the error rate and the quality in the data that would come from an auditable process.

Recommendation unique identifier SEE-Rec-035	Information on scope of testing and limitations
	Scope of testing and limitations should be provided with the test data, in particular with respect to how well the testing environment is representative of the operational environment.
	Research reference: Section 5. subsection 5.7 Finally, testing cannot encompass the full operational environment in which the device or LRU will be irradiated. Adequate consideration should be given to the determination and substantiation of transfer functions between the testing conditions and the operational environment.

8.6 REDESIGN LOOPS

The source for redesign is the non-achievement of a safety target. The redesign can be performed at the component level and/or at the system level.

The component redesign includes the addition of built-in mitigation techniques of a higher level of protection if the penalties are acceptable. A redesign may also investigate new technology choices that are less SEE-sensitive when applicable to the aerospace domain. Note, however, that technology choices for power components to address SEB are limited; a system-level redesign is more likely (more details can be found in section 4).

With the growing risk of MBU/MCU, the cost of ECC is rising with the complexity—such that other prevention techniques are being investigated, including semiconductor material improvement and the introduction of FETs in the nanometer scale (more details can be found in section 4).

8.7 SEE RECOMMENDATION SUMMARY DISCUSSION

The requirement to perform an SEE safety analysis as part of the system-level safety assessment is dependent on the system criticality and contribution of the system to CAT and/or HAZ FCs. The analysis results in determination of whether or not the SEE error rate is acceptable with regard to the safety objectives.

The determination of an SEE error rate can be made at different levels of system integration (e.g., electronic component, integrated circuit, system, equipment) and with different levels of accuracy. The system designer needs to ensure that all data supporting the determination of the SEE rate are commensurate with the criticality of the system to be assessed, the implementing technology as it is differently impacted by SEE, and the envisaged operations. The vast majority of the recommendations in this document are related to the acceptable level of scrutiny to be applied.

Similarly, the selection and effectiveness of mitigation techniques are dependent on the type of SEE to be mitigated and the function(s) of the component to be protected. All mitigations carry penalties and no mitigation covers the full range of SEE. The system developer will use its knowledge of the circuit layout, critical elements, and function(s) to determine tradeoffs between protection coverage, level of effectiveness of the mitigation, and associated penalties. This is specific to each design. The document provides commonly used design tradeoffs and typical limitations in protection.

Finally, although there is no one-fit-all strategy to address SEE, there are recommended avenues and minimum substantiation to be provided by the system designer as part of the demonstration of compliance with SEE safety assessment.

9. GENERAL REPORT RESULTS AND FURTHER WORK

9.1 RESULTS

The research objectives were to articulate the criteria to select components for SEE analysis and to collect considerations pertaining to SEE mitigation techniques. A proposed process to integrate the SEE analysis that incorporates this information is defined at the system and equipment level. The following information highlights the main takeaway findings.

The requirement to perform an SEE safety analysis, as part of the system level safety assessment, is dependent on the system criticality, contribution of the system to CAT, and/or HAZ FCs. The analysis results in the determination of whether the SEE error rate is acceptable with regard to the safety objectives.

The determination of an SEE error rate can be made at different levels of system integration (e.g., electronic component, integrated circuit, system, and equipment) and with different levels of accuracy. The system designer needs to ensure that all data supporting the determination of the SEE rate are commensurate with the criticality of the system to be assessed, implementing technology as it is differently impacted by SEE, and envisioned operations. The vast majority of the recommendations in section 8 are related to the acceptable level of scrutiny to be applied.

Similarly, the selection and effectiveness of mitigation techniques are dependent on the type of SEE to be mitigated and the function(s) of the component to be protected. All mitigations carry penalties and no mitigation covers the full range of SEE. The system developer will use knowledge of the circuit layout, critical elements, and function(s) to determine tradeoffs between protection coverage, level of effectiveness of the mitigation, and associated penalties. This is specific to each design.

To conclude, there is no one-fit-all strategy to address SEE, but there are recommended avenues and there is minimum substantiation to be provided by the system designer as part of the demonstration of compliance with SEE safety assessment.

9.2 FURTHER WORK

9.2.1 Aspects of the SSA

The last steps of the SSA—the component-level redesign loop and system-level redesign loop—were not covered in detail. More research is needed to develop guidelines with regard to the different strategies for redesign and the challenges arising from the newer semiconductor technologies. The latter may be broader than the technical aspects as challenges concern the market size, conditions of reusability from other domains, and impact on aeronautical manufacturing processes.

9.2.2 Gap Analysis With Current Standards

The objective of the research was to support the development of guidance regarding the acceptance of microelectronic components and, in particular, to focus on the mitigation techniques. Normative documents, such as the JEDEC and IEC documents, exist and may be updated based on experimental results. The European regulatory document [1] seems to go further or sideways with respect to these standards. A consolidated view would be beneficial to understand the differences and potential for convergence of guidance in the future, whether the misalignment was created by the newer regulatory document or is to be achieved.

9.2.3 Guidelines for Previously Developed Hardware

The aeronautical market does not have the critical mass to drive the market of microelectronics and cannot sustain the cost of custom-made components as the space segment does. Recent strategies have seen OEMs partner directly with semiconductor electronics manufacturers for specific equipment, whereas other manufacturers focus on the consumer electronics market. The research topic would allow the addressing of the business jet, high-end general aviation, and helicopter markets.

10. REFERENCES

1. EASA, Proposed Certification Memorandum, “Single Event Effects (SEE) Caused by Atmospheric Radiation,” CM-AS draft version 8.

2. Velazco, R., “Methods, Prediction Tools and SEE Soft Mitigations,” CNRS/TIMA tutorial, 2006.

3. 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,” 2006.

4. SAE, ARP4761, “Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment,” December 1996.

5. SAE, ARP4754A, “Guidelines for Development of Civil Aircraft and Systems,” December 2010.

6. Xilinx, tabulated adjustments for neutron flux, downloadable from www.xilinx.com (accessed on 05/11/15).

7. Jones, R. et al., “Comparison between SRAM SEE Cross-Sections From the Ion Beam Testing With Those Obtained Using a New Picosecond Pulsed Laser Facility,” IEEE Transactions on Nuclear Sciences, Vol. 47, No. 3, June 2000.

8. Srikanth, K. et al., “Study of Single Event Upsets in Different Double Gate FinFET Based SRAM Topologies,” IEEE Conference on Emerging Trends in Computing, Communication and Nanotechnology (ICECCN), 2013.

9. Ikeda, N. et al., “Single Event Burnout of Super Junction Power MOSFETs,” IEEE Transactions on Nuclear Science, Vol. 51, No. 6, December 2004.

10. O’Bryan, A.M. et al., “Compendium of Current Single Event Effects Results for Candidate Spacecraft Electronics for NASA,” IEEE Radiation Effects Data Workshop, 2007.

11. Nuns, T. et al., “Evaluation of Recent Technologies of Nonvolatile RAM,” IEEE Transactions on Nuclear Science, Vol. 55, pp.1982–1991, 2008.

12. Regis, D., Hubert, G., Bayle, F., and Gatti, M., “IC Components Reliability Concerns for Avionics End-Users,” Proceedings of the 32nd Digital Avionics Systems Conference, Syracuse, New York, October 2013.

13. Kaminski, N. and Kopta, A., “Failure Rates of HiPak Modules Due to Cosmic Rays,” Application Note 5SYA 204204, ABB Switzerland Ltd., 2011.

14. EASA, CM-SWCEH-001,“Development Assurance of Airborne Electronic Hardware,” August 2011.

15. Federal Aviation Administration, TSO-C198, “Automatic Flight Guidance and Control System (AFGCS) Equipment,” May 27, 2015.

16. Federal Aviation Administration, TSO-C169a, “VHF Radio Communications Transceiver Equipment Operating Within Radio Frequency Range 117.975 to 137.000 Megahertz,” July 14, 2010.

17. Federal Aviation Administration, TSO-C170, “High Frequency (HF) Radio Communications Transceiver Equipment Operating Within the Radio Frequency Range 1.5 to 30 Megahertz,” December 11, 2014.

18. Federal Aviation Administration, TSO-C59a, “Airborne Selective Calling (Selcal) Equipment,” June 8, 2011.

19. Federal Aviation Administration, TSO-C158, “Aeronautical Mobile High Frequency Data Link (HFDL) Equipment,” August 19, 2004.

20. Federal Aviation Administration, TSO-C178, “Single Phase 115VAC, 400Hz Arc Fault Circuit Breakers,” March 3, 2006.

21. Federal Aviation Administration, TSO-C79, “Fire Detectors (Radiation Sensing Type),” November 8, 2005.

22. Federal Aviation Administration, TSO-C113a, “Airborne Multipurpose Electronic Displays,” December 1, 2014.

23. Federal Aviation Administration, TSO-C63d, “Airborne Weather Radar Equipment,” March 14, 2014.

24. Federal Aviation Administration, TSO-C119d, “Traffic Alert and Collision Avoidance System (TCAS) Airborne Equipment, TCASII with Hybrid Surveillance,” September 5,
25. 2013.

26. Federal Aviation Administration, TSO-C151c, “Terrain Awareness and Warning System (TAWS),” January 26, 2015.

27. Federal Aviation Administration, TSO-C194, “Helicopter Terrain Awareness and Warning System (HTAWS),” May 27, 2015.

28. Federal Aviation Administration, TSO-C74d, "Air Traffic Control Radar Beacon System (ATCRBS) Airborne Equipment," February 12, 2014.

29. Federal Aviation Administration, TSO-C112e, "Air Traffic Control Radar Beacon System/Mode Select (ATCRBS/Mode S) Airborne Equipment," June 18, 2015.

30. Federal Aviation Administration, TSO-C115c, "Flight Management System (FMS) Using Multi-Sensor Inputs," May 27, 2015.

31. Federal Aviation Administration, TSO-C146c, "Stand-Alone Airborne Navigation Equipment Using the Global Positioning System Augmented by the Satellite Based Augmentation System," January 4, 2013.

32. Federal Aviation Administration, TSO-C153, "Integrated Modular Avionics Hardware Elements," February 17, 2009.

33. Federal Aviation Administration, TSO-C44c, "Fuel Flowmeters," September 26, 2013.

34. Federal Aviation Administration, TSO-C45b, "Manifold Pressure Instruments," January 22, 2015.

35. Federal Aviation Administration, TSO-C47a, "Fuel, Oil and Hydraulic Pressure Instruments," September 26, 2013.

36. ECSS-E-ST-10-12C, "Methods for the Calculation of Radiation Received and Its Effects, and a Policy for Design Margins," Space Engineering Standards, Chapter 9.

37. Furuta, J. et al., "Evaluation of Bipolar Effects on Neutron-Induced SET Rates for Logic Gates," *IEEE International Reliability Physics Symposium (IRPS)*, 2012.

38. Diehl-Nagle, S., "A New Class of Single Event Soft Errors," *IEEE Transactions on Nuclear Science*, Vol. NS-31, No. 6, 1984.

39. European Space Agency, Components Division, "EEE Component Engineering Training for Engineers and Procurement Personnel," 2007.

40. European Space Agency, "Single Event Effect Mitigation in Digital Integrated Circuits for Space," *Topical Workshop on Electronics for Particle Physics*, Aachen, Germany, September 21, 2010.

41. Marquez, F. et al., "Automatic Inspection of SET Sensitivity in Analog Cells," *Proceedings of the International Conference on Synthesis, Modeling, Analysis and Simulation Methods and Applications to Circuit Design (SMACD)*, Seville, Spain, September 19–21, 2012.

42. Irom, F. and Agarwal, S., “Compendium of Single-Event Latchup and Total Ionizing Dose Test Results of Commercial Analog to Digital Converters,” *IEEE Radiation Effects Data Workshop* (REDW), Tucson, Arizona, July 16–20, 2012.

43. O’Bryan, M.V. et al., “Compendium of Single Event Effects for Candidate Spacecraft Electronics for NASA,” *IEEE Radiation Effect Data Workshop* (REDW), Tucson, Arizona, July 16–20, 2012.

44. Northum, J. and Guetersloh, S., “Geometric Optimization for Radiation Hardness Assurance,” *Proceedings of the IEEE Aerospace Conference*, Big Sky, Montana, March 2–9, 2013.

45. Furuta, J. et al., “Impact of Cell Distance and Well-Contact Density on Neutron-Induced Multiple Cell Upsets,” *IEEE International Reliability Physics Symposium* (IRPS), Monterey, California, April 14–18, 2013.

46. Nepal, K. et al., “Using Implications for Online Error Detection,” *Proceedings of the International Test Conference (ITC),* Santa Clara, California, October 28–30, 2008.

47. Sanchez-Clemente, A. et al., “Logic Masking for SET Mitigation Using Approximate Logic Circuits,” *IEEE 18th International On-Line Testing Symposium (IOLTS),* Sitges, Spain, June 27–29, 2012.

48. Pontes, J. et al., “Adding Temporal Redundancy to Delay Insensitive Codes to Mitigate Single Event Effects,” *Proceedings of the 18th IEEE International Symposium on Asynchronous Circuits and Systems (ASYNC),* Copenhagen, Denmark, May 7–9, 2012.

49. Mitra, S. et al., “Built-In Soft Error Resilience for Robust System Design,” *IEEE International Conference on Circuit Design and Technology (ICICDT)*, 2007.

50. Bessot, D. and Velazco, R., “Design of SEU-Hardened CMOS Memory Cells: the HIT Cell,” Second European Conference on Radiation and Its Effects on Components and Systems (RADECS), 1993.

51. Shi, Q. and Maki, G., “New Design Techniques for SEU-Immune Circuits,” NASA Symposium on VLSI Design, November 2000.

52. Naser, R. and Draper, J., “DF-DICE: A Scalable Solution for Soft-Error Tolerant Circuit Design,” *Proceedings of the 49th IEEE International Symposium on Circuits and Systems (ISCAS),* Island of Kos, Greece, May 21–24, 2006.

53. Maniatakos, M. et al., “Vulnerability-Based Interleaving for Multi-Bit Upset (MBU) Protection in Modern Microprocessors,” *Proceedings of the IEEE International Test Conference*, Anaheim, California, November 5–8, 2012.

54. Sarkar, Sudipta et al., "SEU-Tolerant SRAM cell," *Proceedings of the 12th International Symposium on Quality Electronic Design (ISQED)*, Santa Clara, California, March 14–16, 2011.

55. Shayan, M. et al., "SEU-Tolerant Robust Memory Cell Design," *Proceedings of the IEEE 18th International On-Line Testing Symposium (IOLTS)*, Sitges, Spain, June 27–29, 2012.

56. Srikanth, K. et al., "Study of Single Event Upsets in Different Double Gate FinFET based SRAM Topologies," *IEEE Conference on Emerging Trends in Computing, Communication and Nanotechnology (ICECCN)*, Tirunelveli, India, March 25–26, 2013.

57. Gaspard, N. et al., "Estimation of Hardened Flip-Flop Neutron Soft Error Rates Using SRAM Multiple-Cell Upset Data in Bulk CMOS," *IEEE International Symposium on Reliability Physics (IRPS)*, Monterey, California, April 14–18, 2013.

58. Rockett, L.R., "A SEU Hardened CMOS Latch Design," IEEE Transactions on Nuclear Science, Vol. 35, No. 6, December 1988.

59. Kumar, J. and Tahoori, M.B., "Use of Pass Transistor Logic to Minimize the Impact of Soft Errors in Combinational Circuits," IEEE Workshop on System Effects of Logic Soft Errors, April 2005.

60. Lin, S. et al., "A Novel Design Technique for Soft Error Hardening of Nanoscale CMOS Memory," *IEEE International Midwest Symposium on Circuits and Systems*, Cancun, Mexico, August 2–5, 2009.

61. Lutzel, S. and Siemers, C., "A Novel Soft Error Mitigation Approach for SRAM-Based FPGAs," *Proceedings of the World Automation Congress*, Puerto Vallarta, Mexico, June 24–28, 2012.

62. Stamenkovic, Z. et al., "Design Flow and Techniques for Fault-Tolerant ASIC," *Proceedings of the 20th IEEE International Symposium on the Physical and Failure Analysis of Integrated Circuits (IPFA)*, Suzhou, China, July 15–19, 2013.

63. Koga, R. et al., "Single Event Functional Interrupt (SEFI) Sensitivity in Microcircuits," *Proceedings of the 4th European Conference on Radiation and its Effect on Components and Systems*, Palm Beach, Cannes, France, September 15–19, 1997.

64. Rech, P. et al., "Neutron Radiation Test of Graphic Processing Units," *Proceedings of the 2012 IEEE 18th International On-Line Testing Symposium (IOLTS)*," Sitges, Spain, June 27–29, 2012.

65. Normand, E. et al., "Neutron Induced Single Event Burnout in High Voltage Electronics," *IEEE Transactions on Nuclear Science*, Vol. 44, 1997.

66. DoD, MIL-STD-975M, "NASA Standard Electrical, Electronic, and Electromechanical (EEE) Parts List," August 1994.

67. Edwards, R. and Woodhouse, B., "Determination of High Energy Neutron Voltage Stress Margins for High Voltage IGBT and Diode Pairs from Two Manufacturers Using Energetic Particle Induced Charge Spectroscopy, EPICS," *Proceedings of IEEE Radiation Effects Data Workshop*, Ponte Vedra Beach, Florida, July 17–21, 2006.

68. Hands, A. et al., "Single Event Effects in Power MOSFETs Due to Atmospheric and Thermal Neutrons," *IEEE Transactions on Nuclear Science*, Vol. 58, No. 6, December 2011.

69. Griffoni, A. et al., "Neutron-Induced Failure in Silicon IGBTs, Silicon Super-Junction and SiC MOSFETs," *IEEE Transactions on Nuclear Science*, 2012.

70. Ikeda, N. et al., "Single-Event Burnout of Super-Junction Power MOSFETs," *IEEE Transactions on Nuclear Science*, Vol. 51, No. 6, December 2004.

71. Dodge, J., "Reduce Circuit Zapping From Cosmic Radiation," *Power Electronic Technology*, September 2007.

72. Normand, E. and Baker, T.J., "Altitude and Latitude Variations in Avionics SEU and Atmospheric Neutron Flux," *IEEE Transactions on Nuclear Science*, Vol. 40, 1993.

73. JEDEC, JESD89A, "Measurement and Reporting of Alpha Particle and Terrestrial Cosmic Ray-Induced Soft Errors in Semiconductor Devices," August 2001.

74. Xilinx FPGA products, downloaded from www.xilinx.com/products/silicon-devices/fpga (accessed on 05/12/15).

75. ON Semiconductor, digital ASIC, downloaded from www.onsemi.com (accessed on 05/12/15).

76. Baumann, R., "Soft Errors in Advanced Computer Systems," *IEEE Design and Tests of Computers*, September 2005, pp. 305–316..

77. Xilinx, "Xilink FPGA Overcome the Side Effects of sub-90nm Technology," downloaded from www.xilinx.com (accessed on 05/12/15).

78. Priore, M. and Farrell, J., "Plastic Microcircuit Packages: a Technology Review," Report No. CRTA-PEM, Reliability Analysis Center, Rome, New York, March 1992.

79. Kretzschmar, U. et al., "Compact and Fast Fault Injection System for Robustness Measurements on SRAM-based FPGAs," *IEEE Transactions on Industrial Electronics*, Vol. 61, No.5, May 2014.

80. Chapman, K. and Jones, L., “SEU Strategies for Virtex-5 Devices,” Xilinx Corp. document XAPP864 downloadable from http://www.xilinx.com (accessed on 05/12/15).

81. Xilinx website, http://www.xilinx.com/applications/aerospace-and-defense/avionics (accessed on 05/12/15).

82. Collins, N. and Wirthlin, M., “Software Fault-Tolerant Techniques for Softcore Processors in Commercial SRAM-based FPGAs,” NSF Center for High-Performance Reconfigurable Computing, Brigham Young University, 2011.

83. Asadi, G. and Tahoori, M.B., “An Analytical Approach for Soft Error Rate Estimation of SRAM-FPGAs,” Military and Aerospace Applications of Programmable Logic Devices (MAPLD), Washington, 2004.

84. Wang, Z.M. et al., “The Reliability and Availability Analysis of SEU Mitigation Techniques in SRAM-based FPGAs,” *European Conference on Radiation and its Effects on Components and Systems (RADECS)*, Bruges, Belgium, September 14–18, 2009.

85. Defense Electronics, “Teamwork Yields ASIC for Flight Control Computer,” available at http://defenseelectronicsmag.com/components/teamwork-yields-asic-flight-control-computer (accessed on 05/12/15).

86. Yui, C. et al., “SEU Mitigation Testing of Xilinx Virtex II FPGAs,” *IEEE Radiation Effects Data Workshop (REDW)*, Monterey, California, July 25, 2003.

87. Eure, K. et al., “Closed-Loop Neutron Particle Effects Testing on a Recoverable Flight Control Computer,” Proceedings of the 23rd Digital Avionics Systems Conference (DASC), Salt Lake City, Utah, October 24–28, 2004.

88. Hansen, D.L. et al., “Clock, Flip-Flop, and Combinatorial Logic Contributions to the SEU Cross-Section in 90nm ASIC Technology,” *IEEE Transactions on Nuclear Science*, Vol. 56, No. 6, December 2009.

89. Hamming, R., “Error Correcting and Error Detecting Codes,” *Bell System Technology Journal*, Vol. 29, 1950.

90. Hsiao, M.Y., “A Class of Optimal Minimum Odd-Weight-Column SEC-DED Codes,” *IBM Journal of Resource Development*, Vol. 14, No. 4, 1970.

91. Berg, M., “Assessing and Mitigating Radiation Effects in Xilinx FPGAs,” JPL Publication, 2008.

92. Xilinx, “NSEU Mitigation in Avionics Applications,” application note XAPP1073, May 2010.

93. Georgakos, G. et al., "Investigation of Increased Multi-bit Failure Rate Due to Neutron Induced SEU in Advanced Embedded SRAMs," *Symposium on VLSI Circuits Digest of Technical Papers*, Kyoto, Japan, June 14–16, 2007.

94. Berg, M. et al., "Effectiveness of Internal Versus External Scrubbing Mitigation Strategies in a Xilinx FPGA: Design, Test and Analysis," *IEEE Transactions on Nuclear Science*, Vol. 55, No. 4, 2008.

95. Zhao, Q. et al., "A Novel Soft Error Detection and Correction Circuit for Embedded Reconfigurable Systems," *IEEE Embedded Systems Letters*, Vol. 3, No. 3, 2011.

96. Naseer, R. and Draper, J., "Parallel Double Error Correcting Code Design to Mitigate Multi-Bit Upsets in SRAMs," *Proceedings of the 34th European ESSCIR Conference*, Edinburgh, Scotland, UK, September 15–19, 2008.

97. Naeimi, H. and DeHon, A., "Fault Secure Encoder and Decoder for Nanomemory Applications," *IEEE Transactions on Very Large Scale Integrated Systems*, Vol. 17, No. 4, 2009.

98. Dutta, A. and Touba, N., "Multiple Bit Upset Tolerant Memory Using a Selective Cycle Avoidance Based SEC-DED-DAEC Code," *Proceedings of the 25th IEEE VLSI Test Symposium*, Berkeley, California, May 6–10, 2007.

99. Sanchez, A. et al., "Enhanced Detection of Double and Triple Adjacent Errors in Hamming Codes Through Selective Bit Placement," *IEEE Transactions on Device and Materials Reliability*, Vol. 12, No. 2, 2012.

100. Neale, A. and Sachdev, M., "A New SEC-DED Error Correction Code Subclass for Adjacent MBU Tolerance in Embedded Memory," *IEEE Transactions on Device and Materials Reliability*, Vol. 13, No. 1, 2013.

101. Abbas, S. et al., "An Efficient Multiple Cell Upsets Tolerant Content Addressable Memory," accepted for publication in *IEEE Transactions*, 2013.

102. Pontarelli, S. et al., "Analysis and Evaluations of Reliability of Reconfigurable FPGAs," *Journal of Electronic Testing*, Vol. 24, No. 1, 2008.

103. Iturbe, X. et al., "A Novel SEU, MBU and SHE Handling Strategy for Xilinx Virtex-4 FPGAs," IEEE International Conference on Field Programmable Logic and Applications, 2009.

104. Allen, G.R. et al., "Single-Event Upset (SEU) Results of Embedded Error Detect and Correct Enabled Block Random Access Memory (Block RAM) Within the Xilinx XQR5VFX130," *IEEE Transactions on Nuclear Science*, Vol. 57, No. 6, December 2010.

105. FAA, AC25-11A, “Advisory Circular – Electronic Flight Deck Displays.”

106. RTCA, DO-178B, “Software Considerations in Airborne Systems and Equipment Certification,” December 1992.

107. EASA, AMC 25-1309, “System Design and Analysis,” CS-25 Amendment 14, Book 2, December 2013.

108. RTCA, DO-254, “Design Assurance Guidance for Airborne Electronic Hardware,” April 2000.

109. EASA, SIB No. 2012-09, “Safety Information Bulletin—Effects of Space Weather,” 2012.

110. EASA, SIB No. 2012-10, “Safety Information Bulletin—Single Event Effects (SEE) on Aircraft Systems Caused by Cosmic Rays,” 2012.

111. SAE, AIR6219, “Development of Atmospheric Neutron Single Event Effect Analysis for Use in Safety Assessment,” draft, June 17, 2013.

112. Xilinx, “Device Reliability Report, Second Quarter 2013,” UG116 v9.5, August 2013.

APPENDIX A—AIR TRANSPORT ASSOCIATION CHAPTER NUMBERING

The Air Transport Association (ATA) chapter numbers provide a common reference standard for all commercial aircraft documentation, regardless of the aircraft make and model. The standard is controlled and published by Airlines for America under specification document 100.

In this appendix, the ATA chapters are provided for completeness beyond the chapters and sections applicable to the SEE analysis highlighted in section 3.

Aircraft General

ATA number	Chapter name
ATA 05	Periodic inspections
ATA 06	Dimensions and areas
ATA 07	Lifting and shoring
ATA 08	Leveling and weighing
ATA 09	Towing and Taxiing
ATA 10	Parking, mooring, storage, and return to service
ATA 11	Placards and markings
ATA 12	Servicing—routine maintenance
ATA 18	Vibration and noise analysis (helicopter only)

Airframe Systems

ATA number	Chapter name
ATA 20	Standard practices—airframe
ATA 21	Air conditioning
ATA 22	Auto-flight
ATA 23	Communications
ATA 24	Electrical power
ATA 25	Equipment/furnishings
ATA 26	Fire protection
ATA 27	Flight controls
ATA 28	Fuel
ATA 29	Hydraulic power
ATA 30	Ice and rain protection
ATA 31	Indicating/recording system
ATA 32	Landing gear
ATA 33	Lights
ATA 34	Navigation
ATA 35	Oxygen

ATA number	Chapter name
ATA 36	Pneumatic
ATA 37	Vacuum
ATA 38	Water/waste
ATA 39	Electrical—electronic panels and multi-purpose components
ATA 40	Multi-system
ATA 41	Water ballast
ATA 42	Integrated modular avionics
ATA 44	Cabin systems
ATA 45	Diagnostic and maintenance system
ATA 46	Information systems
ATA 47	Nitrogen generation system
ATA 48	In flight fuel dispensing
ATA 49	Airborne auxiliary power
ATA 50	Cargo and accessory compartments

Structure

ATA number	Chapter name
ATA 51	Standard practices and structures—general
ATA 52	Doors
ATA 53	Fuselage
ATA 54	Nacelles/pylons
ATA 55	Stabilizers
ATA 56	Windows
ATA 57	Wings

Propeller/rotor

ATA number	Chapter name
ATA 60	Standard practices—propellers/propulsors
ATA 61	Propellers/propulsors
ATA 62	Main rotor(s)
ATA 63	Main rotor drive(s)
ATA 64	Tail rotor
ATA 65	Tail rotor drive
ATA 66	Rotor blade and tail pylon folding
ATA 67	Rotors flight control

Power Plant

ATA number	Chapter name
ATA 70	Standard practices—engine
ATA 71	Power plant—general
ATA 72	Engine 72(T) Engine—turbine/turboprop, ducted fan/unducted fan 72(R) Engine—reciprocating
ATA 73	Engine—fuel and control
ATA 74	Ignition
ATA 75	Bleed air
ATA 76	Engine controls
ATA 77	Engine indicating
ATA 78	Exhaust
ATA 79	Oil
ATA 80	Starting
ATA 81	Turbines (reciprocating engines)
ATA 82	Water injection
ATA 83	Accessory gearboxes (engine driven)
ATA 84	Propulsion augmentation
ATA 91	Charts
ATA 92	Electrical system installation

APPENDIX B—EXAMPLE FAILURE IN TIME RATES FOR XILINX PRODUCTS

Xilinx is the manufacturer that perhaps most widely and openly disseminates its results on single event effect (SEE) testing of its devices. It also has a continuously running project called the Rosetta experiment, which collects and tests in-flight SEE data. The result is a database updated and published quarterly (see www.xilinx.com) and a specific model for SEE rate estimation.

Table B-1 is excerpted from Xilinx's second quarterly report for 2013 [80] and aims to provide the reader with orders of magnitude.

The soft error rates are determined from real-time system-level measurements in various locations and altitudes and corrected for New York City [72] (from the Rosetta experiment). The neutron cross-section data are obtained from testing at the Los Alamos Neutron Science Center (LANSCE).

The estimation of critical bits is 5% on average and never higher than 10%; these values are predicted using Xilinx tools.

Table B-1. Neutron cross-sections and soft error rates for Xilinx products

Technology	Product	Neutron Cross-section per bit			Real-time Soft Error Rate FIT/Mb		
		Configuration memory	Block RAM	Error	Configuration memory	Block RAM	Error[1]
250nm	Virtex	$9.90\ 10^{-15}$	$9.90\ 10^{-15}$	±10%	160	160	±20%
180nm	Virtex-E	$1.12\ 10^{-14}$	$1.12\ 10^{-14}$	±10%	181	181	±20%
150nm	Virtex-II	$2.56\ 10^{-14}$	$2.64\ 10^{-14}$	±10%	405	478	±8%
130nm	Virtex-II Pro	$2.74\ 10^{-14}$	$3.91\ 10^{-14}$	±10%	437	770	±8%
90nm	Virtex-4	$1.55\ 10^{-14}$	$2.74\ 10^{-14}$	±10%	263	484	±11%
90nm	Spartan-3	$2.40\ 10^{-14}$	$3.48\ 10^{-14}$	N/A	190	373	-50/+80%
90nm	Spartan-3E/3A	$1.31\ 10^{-14}$	$2.73\ 10^{-14}$	N/A	104	293	-80/+90%
65nm	Virtex-5	$6.70\ 10^{-15}$	$3.96\ 10^{-14}$	±10%	165	692	-13/+15%
45nm	Spartan-6	$1.00\ 10^{-14}$	$2.20\ 10^{-14}$	N/A	190	399	-12/+14%
40nm	Virtex-6	$1.26\ 10^{-14}$	$1.14\ 10^{-14}$	±10%	97	213	-14/+17%
28nm	7 series FPGAs	$6.99\ 10^{-15}$	$6.32\ 10^{-15}$	N/A	84	76	-16/+19%

[1] The Soft Error Rate error is indicated for the 90% confidence interval.

APPENDIX C—STATIC MEMORY CONTENT OF VIRTEX-5 FPGA

P/N	Config. Bits (less block RAM)	Slices	CLB Flip-Flops	Max Distributed RAM (Kb)	Block RAM	
					Block	Max (Kb)
XC5VLX30	7,030,528	4,800	19,200	320	32	1152
XC5VLX50	10,541,440	7,200	28,800	480	48	1728
XC5VLX85	17,815,168	12,960	51,840	840	96	3456
XC5VLX110	23,750,656	17,280	69,120	1120	128	4608
XC5VLX155	32,987,136	24,320	97,280	1640	192	6912
XC5VLX220	45,078,528	34,560	138,240	2280	192	6912
XC5VLX330	67,613,440	51,840	207,360	3420	288	10,368
XC5VLX20T	6,251,200	3120	12,480	210	26	936
XC5VLX30T	9,371,136	4800	19,200	320	36	1296
XC5VLX50T	14,052,352	7200	28,800	480	60	2160
XC5VLX85T	23,341,312	12,960	51,840	840	108	3888
XC5VLX110T	31,118,848	17,280	69,120	1120	148	5328
XC5VLX155T	43,042,304	24,320	97,280	1640	212	7632
XC5VLX220T	55,133,696	34,560	138,240	2280	212	7632
XC5VLX330T	82,696,192	51,840	207,360	3420	324	11,664
XC5VSX35T	9,318,656	5440	21,760	520	84	3024
XC5VSX50T	13,973,632	8160	32,640	780	132	4752
XC5VSX95T	24,968,192	14,720	58,880	1520	244	8764
XC5VSX240T	57,442,816	37,440	149,760	4200	516	18,576
XC5VFX30T	9,318,656	23,200	92,800	1500	228	8208
XC5VFX70T	18,964,480	37,440	149,760	2400	324	11,664
XC5VFX100T	27,298,304	5120	20,480	380	68	2448
XC5VFX130T	34,120,704	11,200	44,800	820	148	5328
XC5VFX200T	48,689,152	16,000	64,000	1240	228	8208
XC5VTX150T	43,278,464	20,480	81,920	1580	298	10,728
XC5VTX240T	65,755,648	30,720	122,880	2280	456	16,416

CLB = configurable logic block

APPENDIX D—FAULT TREE DIAGRAMS

This appendix explains the traceability among fault tree analysis (FTA) events, FMEA failure rates, and SEE error rates.

Figure D-1 provides additional guidance to help the reader navigate the information in tables 66, 53, and 52, and the fault trees provided in this appendix.

FMEA failure rates (green circles) are used to verify the failure rate budgets (red circles) used in the FTA (see table 53). The failure rates' budgets (red circles) are linked to FTA basic events (purple circles) via the failure rate code: one failure rate code may be shared among several basic events, as explained in section 7.5.2.1.1 (e.g., the basic events related to duplicated LRUs [such as "Center Display Loss," or "OR Loss"] use the same failure rate code, "DU_Complete_Loss").

Basic events (purple circles) are used in fault-trees. Their probability of occurrence is computed over the flight time (4 hours in our example; see section 7.2.4.1) with the following formulae:

$$P \text{ (Flight Duration)} = \text{Failure Rate (per Flight Hour)} \times \text{Failure Exposure Time} \qquad \text{(D-1)}$$

This explains why the probability displayed on the fault tree is four times higher than the failure rate.

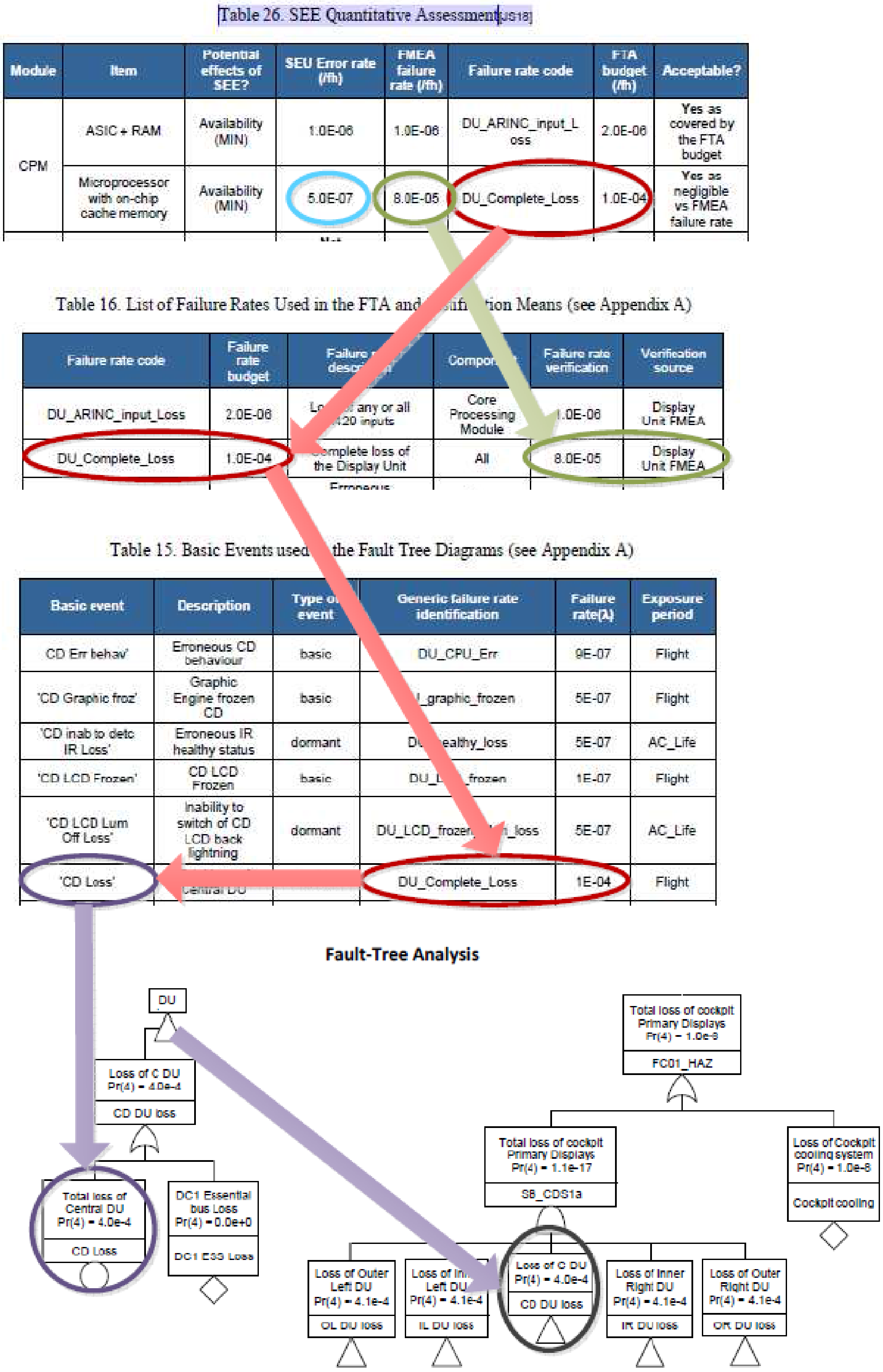


Table 26. SEE Quantitative Assessment[JS18]

Module	Item	Potential effects of SEE?	SEU Error rate (/fh)	FMEA failure rate (/fh)	Failure rate code	FTA budget (/fh)	Acceptable?
CPM	ASIC + RAM	Availability (MIN)	1.0E-06	1.0E-06	DU_ARINC_input_Loss	2.0E-06	Yes as covered by the FTA budget
	Microprocessor with on-chip cache memory	Availability (MIN)	5.0E-07	8.0E-05	DU_Complete_Loss	1.0E-04	Yes as negligible vs FMEA failure rate
			Not				

Table 16. List of Failure Rates Used in the FTA and Verification Means (see Appendix A)

Failure rate code	Failure rate budget	Failure rate description	Component	Failure rate verification	Verification source
DU_ARINC_input_Loss	2.0E-06	Lo any or all 120 inputs	Core Processing Module	1.0E-06	Display Unit FMEA
DU_Complete_Loss	1.0E-04	Complete loss of the Display Unit	All	8.0E-05	Display Unit FMEA
		Erroneous			

Table 15. Basic Events used in the Fault Tree Diagrams (see Appendix A)

Basic event	Description	Type of event	Generic failure rate identification	Failure rate(λ)	Exposure period
CD Err behav'	Erroneous CD behaviour	basic	DU_CPU_Err	9E-07	Flight
'CD Graphic froz'	Graphic Engine frozen CD	basic	_graphic_frozen	5E-07	Flight
'CD inab to detc IR Loss'	Erroneous IR healthy status	dormant	DU ealthy_loss	5E-07	AC_Life
'CD LCD Frozen'	CD LCD Frozen	basic	DU_L _frozen	1E-07	Flight
'CD LCD Lum Off Loss'	Inability to switch of CD LCD back lightning	dormant	DU_LCD_frozen n_loss	5E-07	AC_Life
'CD Loss'	central DU		DU_Complete_Loss	1E-04	Flight

Fault-Tree Analysis

Figure D-1. Process to relate fault tree allocations, events, and failure rates

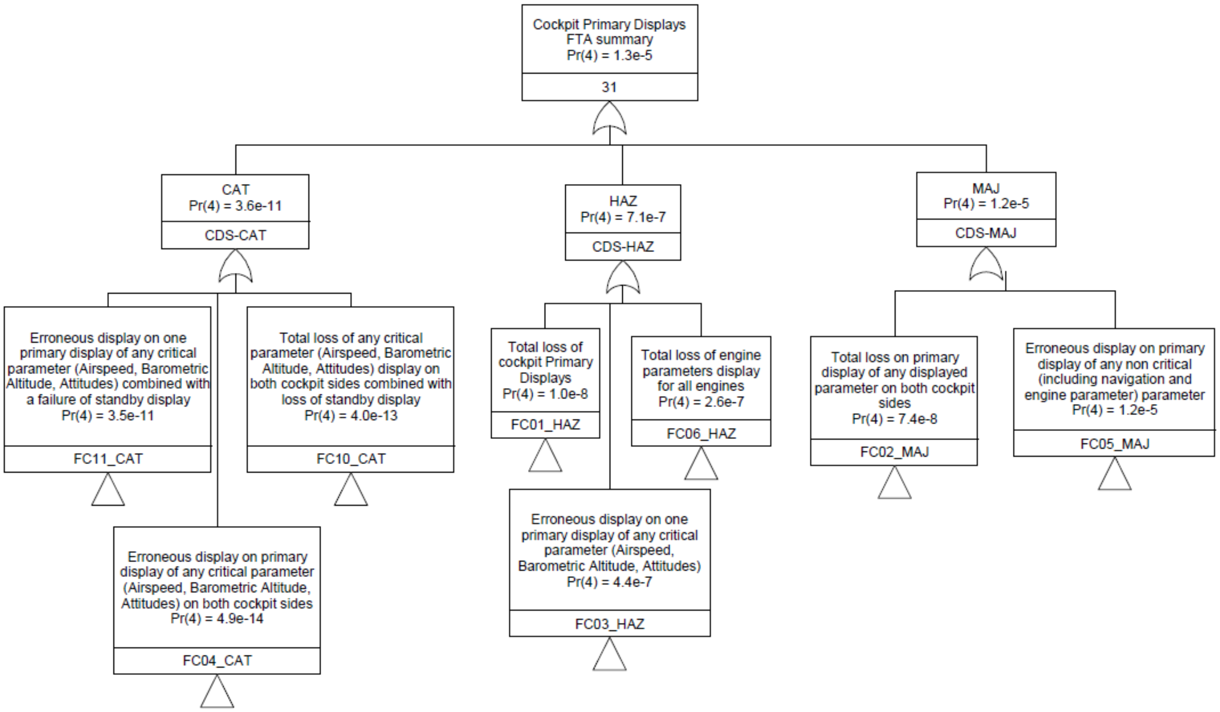
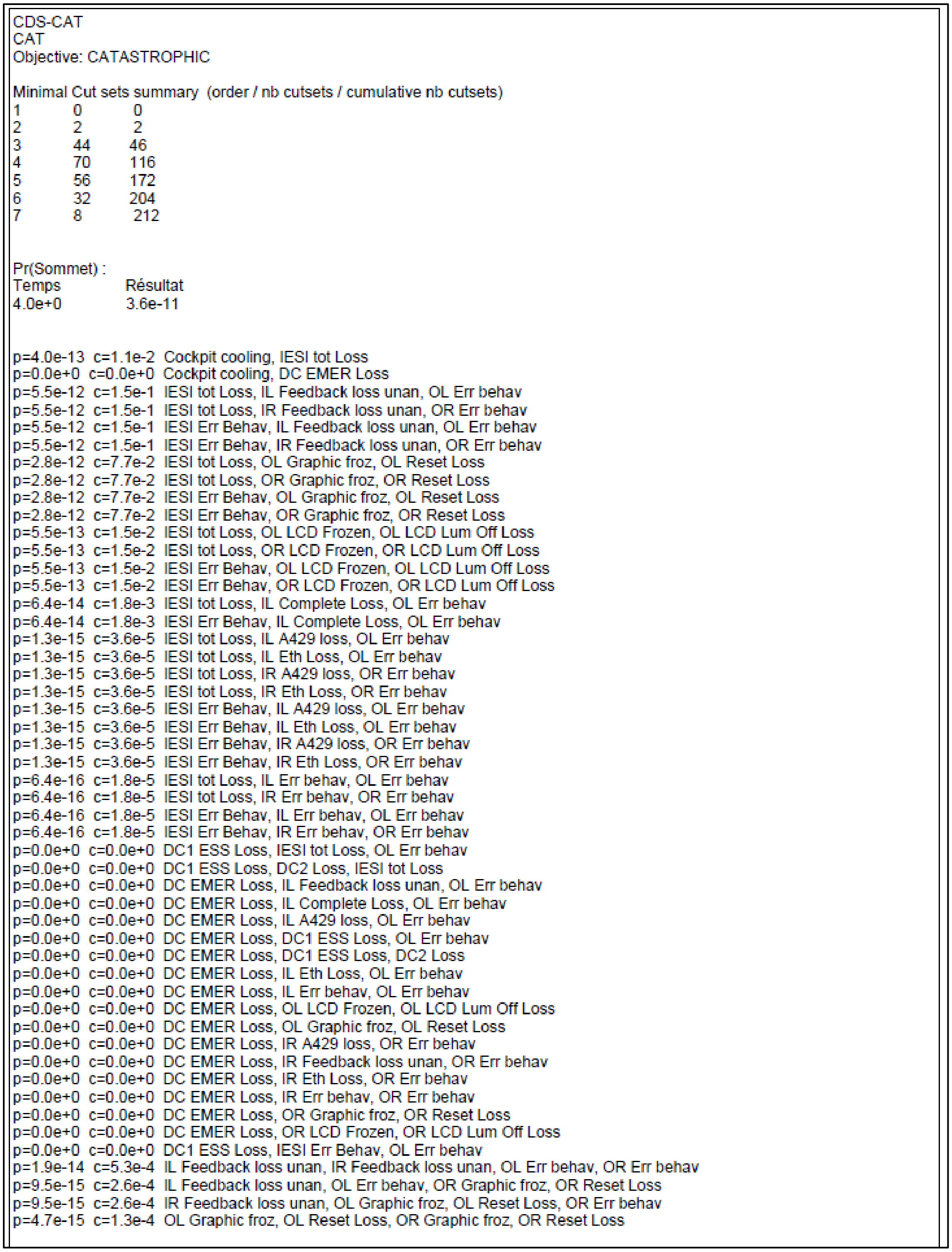

Cockpit Primary Displays
FTA summary
Pr(4) = 1.3e-5
31
CAT
Pr(4) = 3.6e-11
CDS-CAT
HAZ
Pr(4) = 7.1e-7
CDS-HAZ
MAJ
Pr(4) = 1.2e-5
CDS-MAJ
Erroneous display on one primary display of any critical parameter (Airspeed, Barometric Altitude, Attitudes) combined with a failure of standby display
Pr(4) = 3.5e-11
FC11_CAT
Total loss of any critical parameter (Airspeed, Barometric Altitude, Attitudes) display on both cockpit sides combined with loss of standby display
Pr(4) = 4.0e-13
FC10_CAT
Erroneous display on primary display of any critical parameter (Airspeed, Barometric Altitude, Attitudes) on both cockpit sides
Pr(4) = 4.9e-14
FC04_CAT
Total loss of cockpit Primary Displays
Pr(4) = 1.0e-8
FC01_HAZ
Total loss of engine parameters display for all engines
Pr(4) = 2.6e-7
FC06_HAZ
Erroneous display on one primary display of any critical parameter (Airspeed, Barometric Altitude, Attitudes)
Pr(4) = 4.4e-7
FC03_HAZ
Total loss on primary display of any displayed parameter on both cockpit sides
Pr(4) = 7.4e-8
FC02_MAJ
Erroneous display on primary display of any non critical (including navigation and engine parameter) parameter
Pr(4) = 1.2e-5
FC05_MAJ

Figure D-2. Cockpit display system FTA summary

Note: SEE could affect the standby instrument. No assessment has been performed for this report regarding the standby display because it was considered to be an external equipment out-of-scope of the system (see section 7.5.2.1.1 for the list of basic events involved in CAT or HAZ FCs).

Moreover, a system supplier may not be able to perform an SEE assessment for equipment provided by other suppliers if it is not the integrator of these pieces of equipment. In that case, the following may apply:

- The airframer manages to provide to the system supplier the SEE analyses for all other equipment to be integrated in the system safety analysis.
- Working assumptions related to the external equipment must be listed in the conclusion of the system SEE assessment.



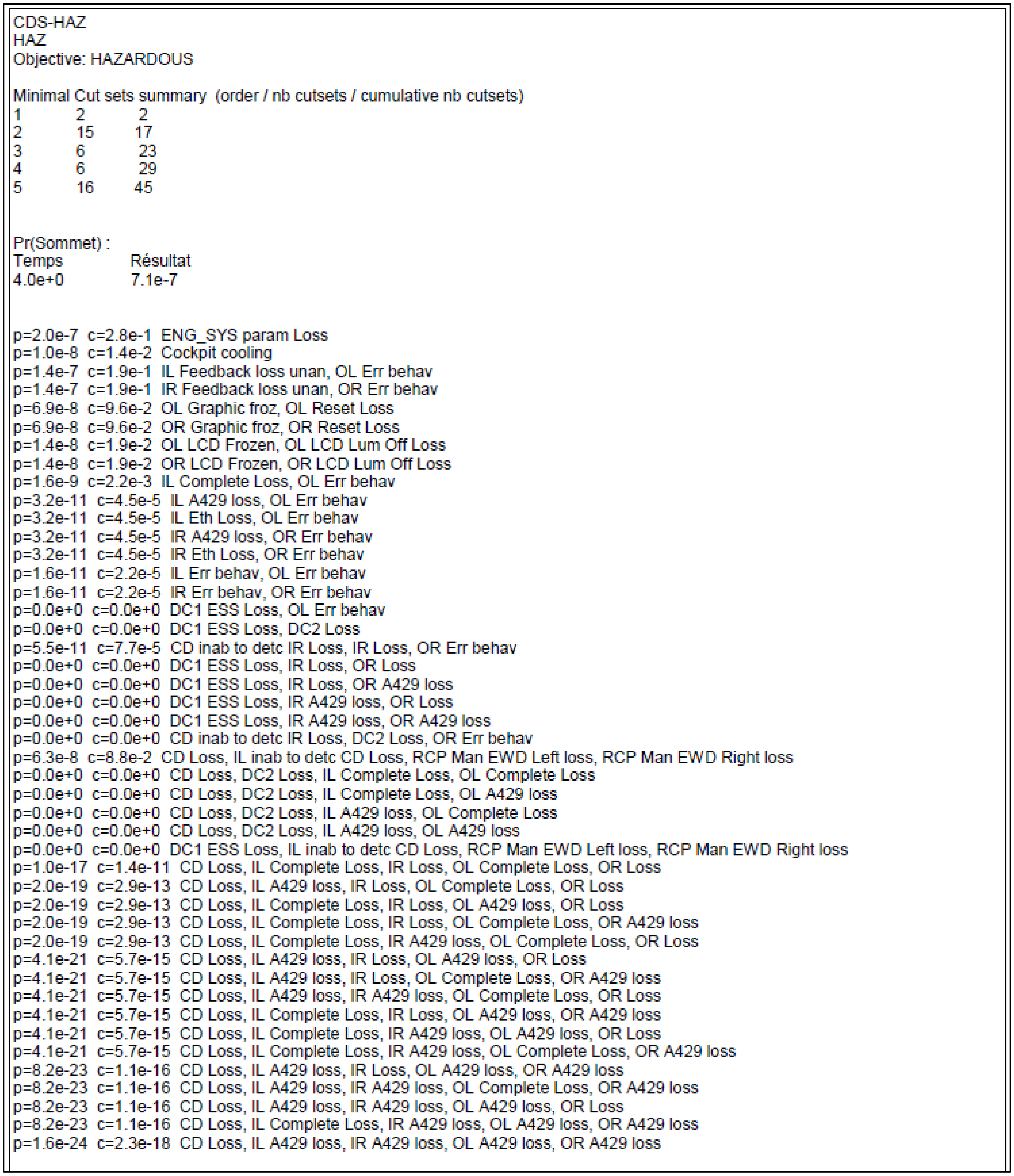
```
CDS-CAT
CAT
Objective: CATASTROPHIC

Minimal Cut sets summary  (order / nb cutsets / cumulative nb cutsets)
1         0         0
2         2         2
3         44        46
4         70        116
5         56        172
6         32        204
7         8         212


Pr(Sommet) :
Temps           Résultat
4.0e+0          3.6e-11


p=4.0e-13  c=1.1e-2  Cockpit cooling, IESI tot Loss
p=0.0e+0  c=0.0e+0  Cockpit cooling, DC EMER Loss
p=5.5e-12  c=1.5e-1  IESI tot Loss, IL Feedback loss unan, OL Err behav
p=5.5e-12  c=1.5e-1  IESI tot Loss, IR Feedback loss unan, OR Err behav
p=5.5e-12  c=1.5e-1  IESI Err Behav, IL Feedback loss unan, OL Err behav
p=5.5e-12  c=1.5e-1  IESI Err Behav, IR Feedback loss unan, OR Err behav
p=2.8e-12  c=7.7e-2  IESI tot Loss, OL Graphic froz, OL Reset Loss
p=2.8e-12  c=7.7e-2  IESI tot Loss, OR Graphic froz, OR Reset Loss
p=2.8e-12  c=7.7e-2  IESI Err Behav, OL Graphic froz, OL Reset Loss
p=2.8e-12  c=7.7e-2  IESI Err Behav, OR Graphic froz, OR Reset Loss
p=5.5e-13  c=1.5e-2  IESI tot Loss, OL LCD Frozen, OL LCD Lum Off Loss
p=5.5e-13  c=1.5e-2  IESI tot Loss, OR LCD Frozen, OR LCD Lum Off Loss
p=5.5e-13  c=1.5e-2  IESI Err Behav, OL LCD Frozen, OL LCD Lum Off Loss
p=5.5e-13  c=1.5e-2  IESI Err Behav, OR LCD Frozen, OR LCD Lum Off Loss
p=6.4e-14  c=1.8e-3  IESI tot Loss, IL Complete Loss, OL Err behav
p=6.4e-14  c=1.8e-3  IESI Err Behav, IL Complete Loss, OL Err behav
p=1.3e-15  c=3.6e-5  IESI tot Loss, IL A429 loss, OL Err behav
p=1.3e-15  c=3.6e-5  IESI tot Loss, IL Eth Loss, OL Err behav
p=1.3e-15  c=3.6e-5  IESI tot Loss, IR A429 loss, OR Err behav
p=1.3e-15  c=3.6e-5  IESI tot Loss, IR Eth Loss, OR Err behav
p=1.3e-15  c=3.6e-5  IESI Err Behav, IL A429 loss, OL Err behav
p=1.3e-15  c=3.6e-5  IESI Err Behav, IL Eth Loss, OL Err behav
p=1.3e-15  c=3.6e-5  IESI Err Behav, IR A429 loss, OR Err behav
p=1.3e-15  c=3.6e-5  IESI Err Behav, IR Eth Loss, OR Err behav
p=6.4e-16  c=1.8e-5  IESI tot Loss, IL Err behav, OL Err behav
p=6.4e-16  c=1.8e-5  IESI tot Loss, IR Err behav, OR Err behav
p=6.4e-16  c=1.8e-5  IESI Err Behav, IL Err behav, OL Err behav
p=6.4e-16  c=1.8e-5  IESI Err Behav, IR Err behav, OR Err behav
p=0.0e+0  c=0.0e+0  DC1 ESS Loss, IESI tot Loss, OL Err behav
p=0.0e+0  c=0.0e+0  DC1 ESS Loss, DC2 Loss, IESI tot Loss
p=0.0e+0  c=0.0e+0  DC EMER Loss, IL Feedback loss unan, OL Err behav
p=0.0e+0  c=0.0e+0  DC EMER Loss, IL Complete Loss, OL Err behav
p=0.0e+0  c=0.0e+0  DC EMER Loss, IL A429 loss, OL Err behav
p=0.0e+0  c=0.0e+0  DC EMER Loss, DC1 ESS Loss, OL Err behav
p=0.0e+0  c=0.0e+0  DC EMER Loss, DC1 ESS Loss, DC2 Loss
p=0.0e+0  c=0.0e+0  DC EMER Loss, IL Eth Loss, OL Err behav
p=0.0e+0  c=0.0e+0  DC EMER Loss, IL Err behav, OL Err behav
p=0.0e+0  c=0.0e+0  DC EMER Loss, OL LCD Frozen, OL LCD Lum Off Loss
p=0.0e+0  c=0.0e+0  DC EMER Loss, OL Graphic froz, OL Reset Loss
p=0.0e+0  c=0.0e+0  DC EMER Loss, IR A429 loss, OR Err behav
p=0.0e+0  c=0.0e+0  DC EMER Loss, IR Feedback loss unan, OR Err behav
p=0.0e+0  c=0.0e+0  DC EMER Loss, IR Eth Loss, OR Err behav
p=0.0e+0  c=0.0e+0  DC EMER Loss, IR Err behav, OR Err behav
p=0.0e+0  c=0.0e+0  DC EMER Loss, OR Graphic froz, OR Reset Loss
p=0.0e+0  c=0.0e+0  DC EMER Loss, OR LCD Frozen, OR LCD Lum Off Loss
p=0.0e+0  c=0.0e+0  DC1 ESS Loss, IESI Err Behav, OL Err behav
p=1.9e-14  c=5.3e-4  IL Feedback loss unan, IR Feedback loss unan, OL Err behav, OR Err behav
p=9.5e-15  c=2.6e-4  IL Feedback loss unan, OL Err behav, OR Graphic froz, OR Reset Loss
p=9.5e-15  c=2.6e-4  IR Feedback loss unan, OL Graphic froz, OL Reset Loss, OR Err behav
p=4.7e-15  c=1.3e-4  OL Graphic froz, OL Reset Loss, OR Graphic froz, OR Reset Loss
```

Figure D-3. Cockpit display system failure rate computations for CAT FC



```
CDS-HAZ
HAZ
Objective: HAZARDOUS

Minimal Cut sets summary  (order / nb cutsets / cumulative nb cutsets)
1          2          2
2          15         17
3          6           23
4          6           29
5          16         45


Pr(Sommet) :
Temps            Résultat
4.0e+0           7.1e-7


p=2.0e-7  c=2.8e-1  ENG_SYS param Loss
p=1.0e-8  c=1.4e-2  Cockpit cooling
p=1.4e-7  c=1.9e-1  IL Feedback loss unan, OL Err behav
p=1.4e-7  c=1.9e-1  IR Feedback loss unan, OR Err behav
p=6.9e-8  c=9.6e-2  OL Graphic froz, OL Reset Loss
p=6.9e-8  c=9.6e-2  OR Graphic froz, OR Reset Loss
p=1.4e-8  c=1.9e-2  OL LCD Frozen, OL LCD Lum Off Loss
p=1.4e-8  c=1.9e-2  OR LCD Frozen, OR LCD Lum Off Loss
p=1.6e-9  c=2.2e-3  IL Complete Loss, OL Err behav
p=3.2e-11  c=4.5e-5  IL A429 loss, OL Err behav
p=3.2e-11  c=4.5e-5  IL Eth Loss, OL Err behav
p=3.2e-11  c=4.5e-5  IR A429 loss, OR Err behav
p=3.2e-11  c=4.5e-5  IR Eth Loss, OR Err behav
p=1.6e-11  c=2.2e-5  IL Err behav, OL Err behav
p=1.6e-11  c=2.2e-5  IR Err behav, OR Err behav
p=0.0e+0  c=0.0e+0  DC1 ESS Loss, OL Err behav
p=0.0e+0  c=0.0e+0  DC1 ESS Loss, DC2 Loss
p=5.5e-11  c=7.7e-5  CD inab to detc IR Loss, IR Loss, OR Err behav
p=0.0e+0  c=0.0e+0  DC1 ESS Loss, IR Loss, OR Loss
p=0.0e+0  c=0.0e+0  DC1 ESS Loss, IR Loss, OR A429 loss
p=0.0e+0  c=0.0e+0  DC1 ESS Loss, IR A429 loss, OR Loss
p=0.0e+0  c=0.0e+0  DC1 ESS Loss, IR A429 loss, OR A429 loss
p=0.0e+0  c=0.0e+0  CD inab to detc IR Loss, DC2 Loss, OR Err behav
p=6.3e-8  c=8.8e-2  CD Loss, IL inab to detc CD Loss, RCP Man EWD Left loss, RCP Man EWD Right loss
p=0.0e+0  c=0.0e+0  CD Loss, DC2 Loss, IL Complete Loss, OL Complete Loss
p=0.0e+0  c=0.0e+0  CD Loss, DC2 Loss, IL Complete Loss, OL A429 loss
p=0.0e+0  c=0.0e+0  CD Loss, DC2 Loss, IL A429 loss, OL Complete Loss
p=0.0e+0  c=0.0e+0  CD Loss, DC2 Loss, IL A429 loss, OL A429 loss
p=0.0e+0  c=0.0e+0  DC1 ESS Loss, IL inab to detc CD Loss, RCP Man EWD Left loss, RCP Man EWD Right loss
p=1.0e-17  c=1.4e-11  CD Loss, IL Complete Loss, IR Loss, OL Complete Loss, OR Loss
p=2.0e-19  c=2.9e-13  CD Loss, IL A429 loss, IR Loss, OL Complete Loss, OR Loss
p=2.0e-19  c=2.9e-13  CD Loss, IL Complete Loss, IR Loss, OL A429 loss, OR Loss
p=2.0e-19  c=2.9e-13  CD Loss, IL Complete Loss, IR Loss, OL Complete Loss, OR A429 loss
p=2.0e-19  c=2.9e-13  CD Loss, IL Complete Loss, IR A429 loss, OL Complete Loss, OR Loss
p=4.1e-21  c=5.7e-15  CD Loss, IL A429 loss, IR Loss, OL A429 loss, OR Loss
p=4.1e-21  c=5.7e-15  CD Loss, IL A429 loss, IR Loss, OL Complete Loss, OR A429 loss
p=4.1e-21  c=5.7e-15  CD Loss, IL A429 loss, IR A429 loss, OL Complete Loss, OR Loss
p=4.1e-21  c=5.7e-15  CD Loss, IL Complete Loss, IR Loss, OL A429 loss, OR A429 loss
p=4.1e-21  c=5.7e-15  CD Loss, IL Complete Loss, IR A429 loss, OL A429 loss, OR Loss
p=4.1e-21  c=5.7e-15  CD Loss, IL Complete Loss, IR A429 loss, OL Complete Loss, OR A429 loss
p=8.2e-23  c=1.1e-16  CD Loss, IL A429 loss, IR Loss, OL A429 loss, OR A429 loss
p=8.2e-23  c=1.1e-16  CD Loss, IL A429 loss, IR A429 loss, OL Complete Loss, OR A429 loss
p=8.2e-23  c=1.1e-16  CD Loss, IL A429 loss, IR A429 loss, OL A429 loss, OR Loss
p=8.2e-23  c=1.1e-16  CD Loss, IL Complete Loss, IR A429 loss, OL A429 loss, OR A429 loss
p=1.6e-24  c=2.3e-18  CD Loss, IL A429 loss, IR A429 loss, OL A429 loss, OR A429 loss
```

Figure D-4. Cockpit display system failure rate computations for HAZ FC

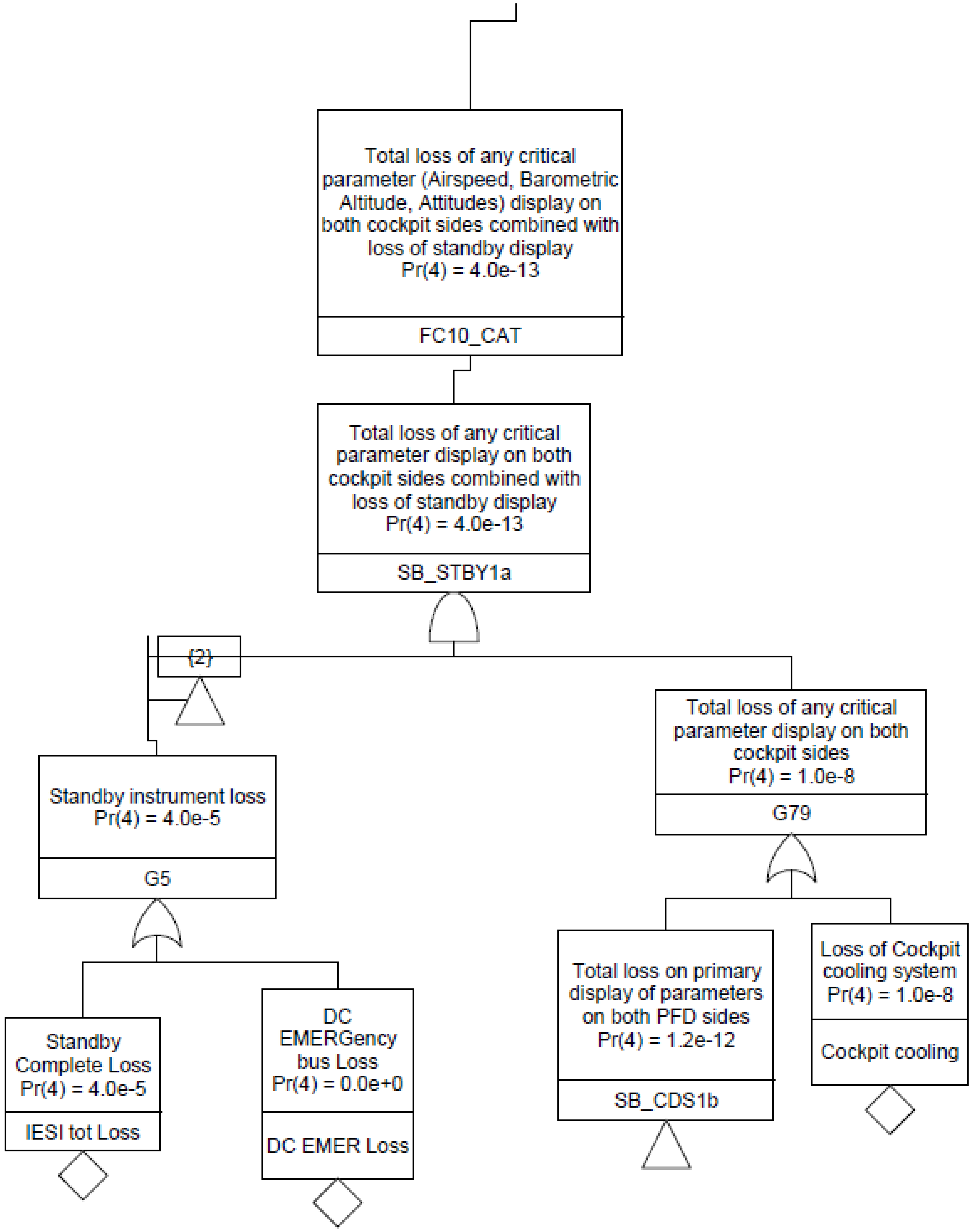

Total loss of any critical parameter (Airspeed, Barometric Altitude, Attitudes) display on both cockpit sides combined with loss of standby display
Pr(4) = 4.0e-13
FC10_CAT
Total loss of any critical parameter display on both cockpit sides combined with loss of standby display
Pr(4) = 4.0e-13
SB_STBY1a
{2}
Standby instrument loss
Pr(4) = 4.0e-5
G5
Total loss of any critical parameter display on both cockpit sides
Pr(4) = 1.0e-8
G79
Standby Complete Loss
Pr(4) = 4.0e-5
IESI tot Loss
DC EMERGency bus Loss
Pr(4) = 0.0e+0
DC EMER Loss
Total loss on primary display of parameters on both PFD sides
Pr(4) = 1.2e-12
SB_CDS1b
Loss of Cockpit cooling system
Pr(4) = 1.0e-8
Cockpit cooling

Figure D-5. Detailed fault tree diagram for FC10_CAT

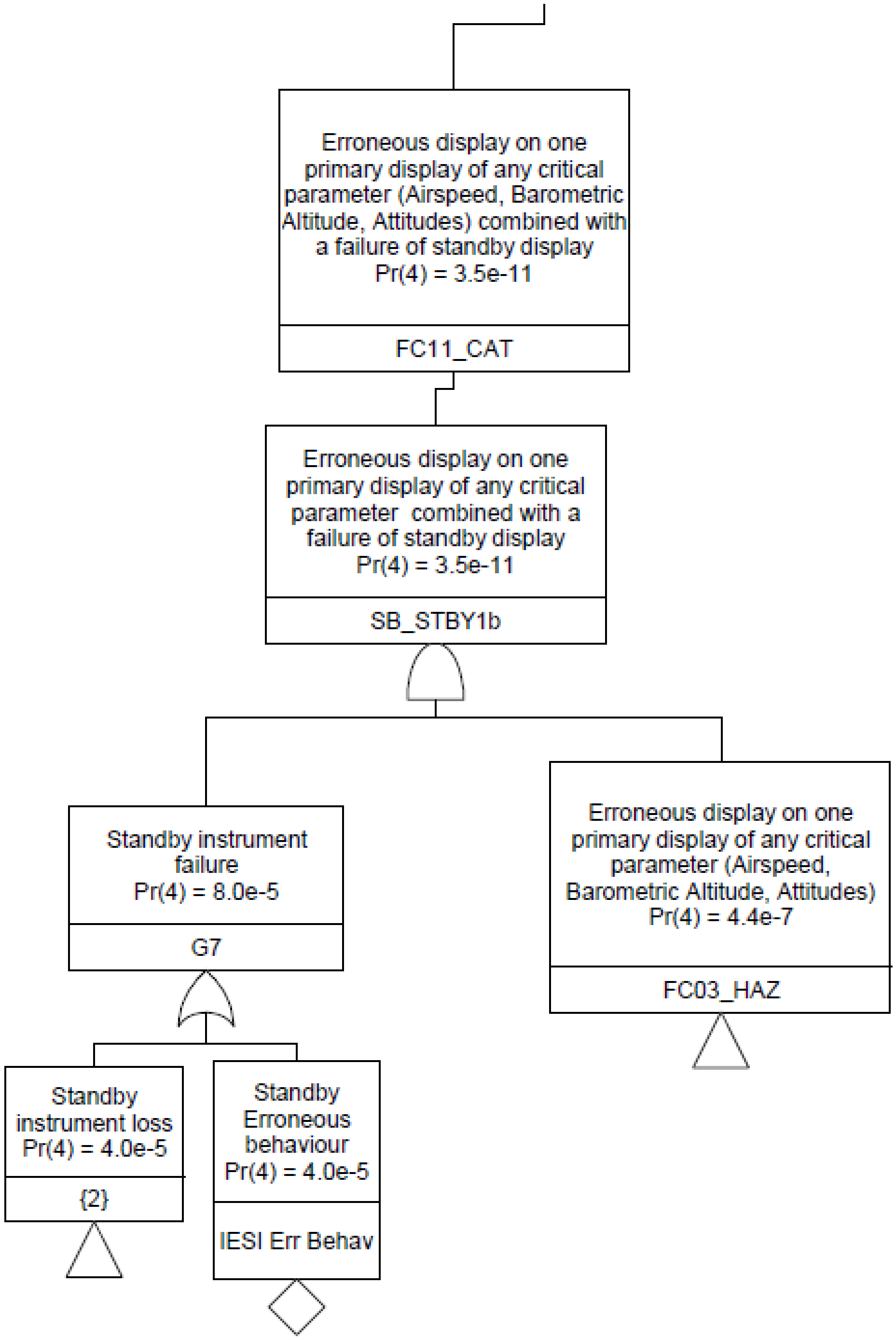

Erroneous display on one primary display of any critical parameter (Airspeed, Barometric Altitude, Attitudes) combined with a failure of standby display
Pr(4) = 3.5e-11
FC11_CAT
Erroneous display on one primary display of any critical parameter combined with a failure of standby display
Pr(4) = 3.5e-11
SB_STBY1b
Standby instrument failure
Pr(4) = 8.0e-5
G7
Erroneous display on one primary display of any critical parameter (Airspeed, Barometric Altitude, Attitudes)
Pr(4) = 4.4e-7
FC03_HAZ
Standby instrument loss
Pr(4) = 4.0e-5
{2}
Standby Erroneous behaviour
Pr(4) = 4.0e-5
IESI Err Behav

Figure D-6. Detailed fault tree diagram for FC11_CAT

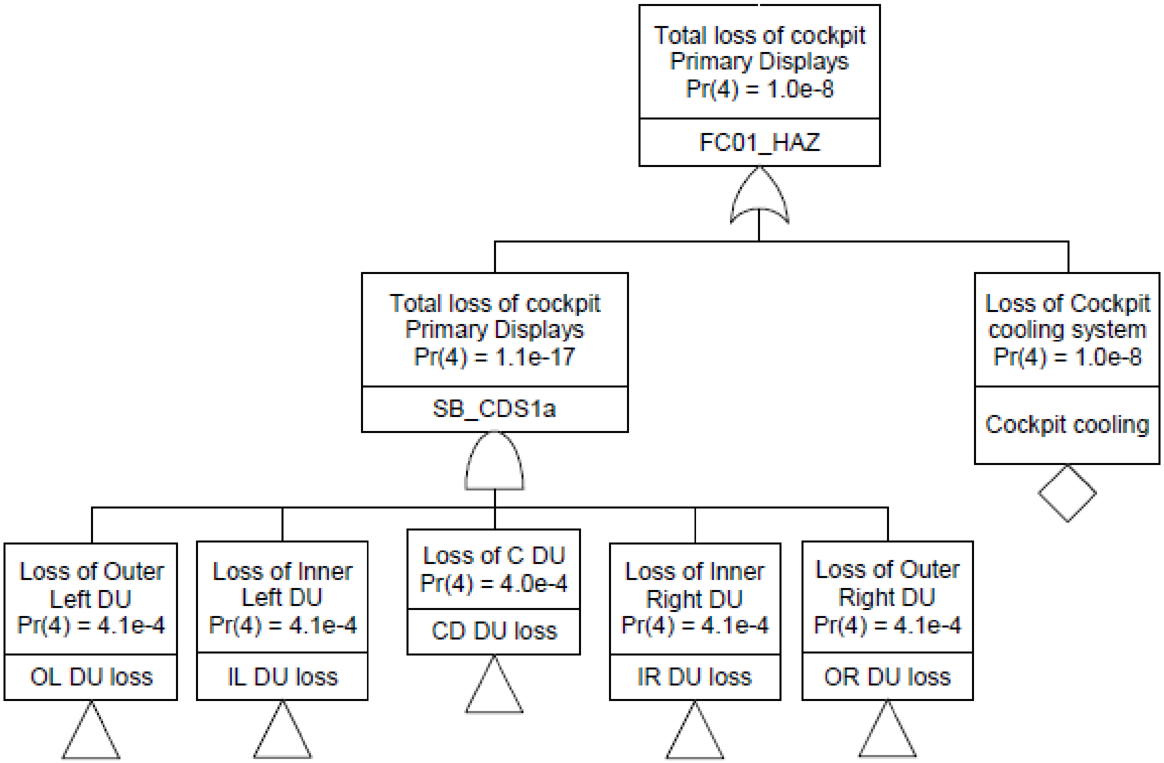

Total loss of cockpit Primary Displays Pr(4) = 1.0e-8
FC01_HAZ
Total loss of cockpit Primary Displays Pr(4) = 1.1e-17
SB_CDS1a
Loss of Cockpit cooling system Pr(4) = 1.0e-8
Cockpit cooling
Loss of Outer Left DU Pr(4) = 4.1e-4
OL DU loss
Loss of Inner Left DU Pr(4) = 4.1e-4
IL DU loss
Loss of C DU Pr(4) = 4.0e-4
CD DU loss
Loss of Inner Right DU Pr(4) = 4.1e-4
IR DU loss
Loss of Outer Right DU Pr(4) = 4.1e-4
OR DU loss

Figure D-7. Detailed fault tree diagram for FC01_HAZ

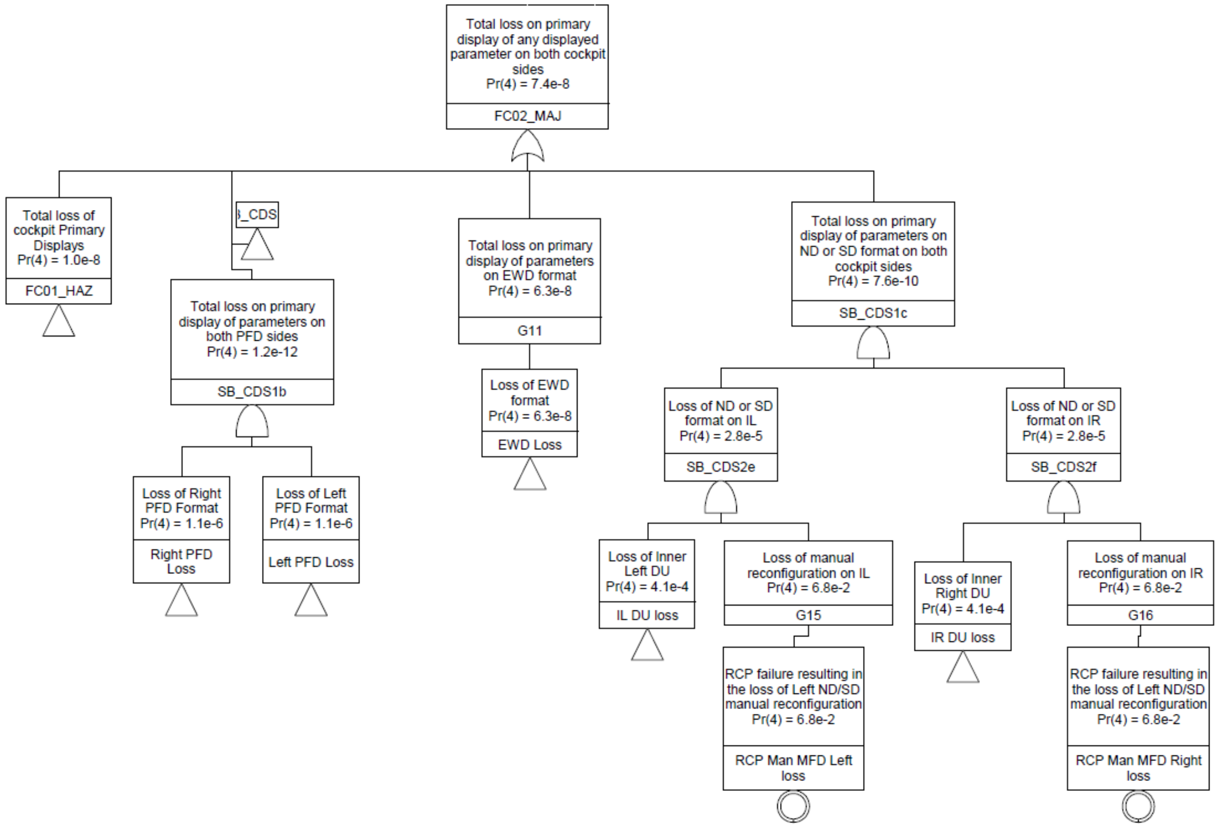

Total loss on primary display of any displayed parameter on both cockpit sides
Pr(4) = 7.4e-8
FC02_MAJ
Total loss of cockpit Primary Displays
Pr(4) = 1.0e-8
FC01_HAZ
_CDS
Total loss on primary display of parameters on both PFD sides
Pr(4) = 1.2e-12
SB_CDS1b
Loss of Right PFD Format
Pr(4) = 1.1e-6
Right PFD Loss
Loss of Left PFD Format
Pr(4) = 1.1e-6
Left PFD Loss
Total loss on primary display of parameters on EWD format
Pr(4) = 6.3e-8
G11
Loss of EWD format
Pr(4) = 6.3e-8
EWD Loss
Total loss on primary display of parameters on ND or SD format on both cockpit sides
Pr(4) = 7.6e-10
SB_CDS1c
Loss of ND or SD format on IL
Pr(4) = 2.8e-5
SB_CDS2e
Loss of ND or SD format on IR
Pr(4) = 2.8e-5
SB_CDS2f
Loss of Inner Left DU
Pr(4) = 4.1e-4
IL DU loss
Loss of manual reconfiguration on IL
Pr(4) = 6.8e-2
G15
RCP failure resulting in the loss of Left ND/SD manual reconfiguration
Pr(4) = 6.8e-2
RCP Man MFD Left loss
Loss of Inner Right DU
Pr(4) = 4.1e-4
IR DU loss
Loss of manual reconfiguration on IR
Pr(4) = 6.8e-2
G16
RCP failure resulting in the loss of Left ND/SD manual reconfiguration
Pr(4) = 6.8e-2
RCP Man MFD Right loss

Figure D-8. Detailed fault tree diagram for FC02_MAJ

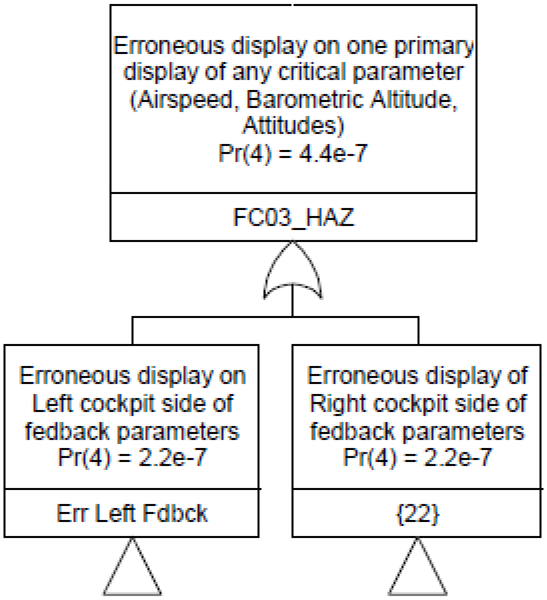

Erroneous display on one primary display of any critical parameter (Airspeed, Barometric Altitude, Attitudes)
Pr(4) = 4.4e-7
FC03_HAZ
Erroneous display on Left cockpit side of fedback parameters
Pr(4) = 2.2e-7
Err Left Fdbck
Erroneous display of Right cockpit side of fedback parameters
Pr(4) = 2.2e-7
{22}

Figure D-9. Detailed FTA for FC03_HAZ

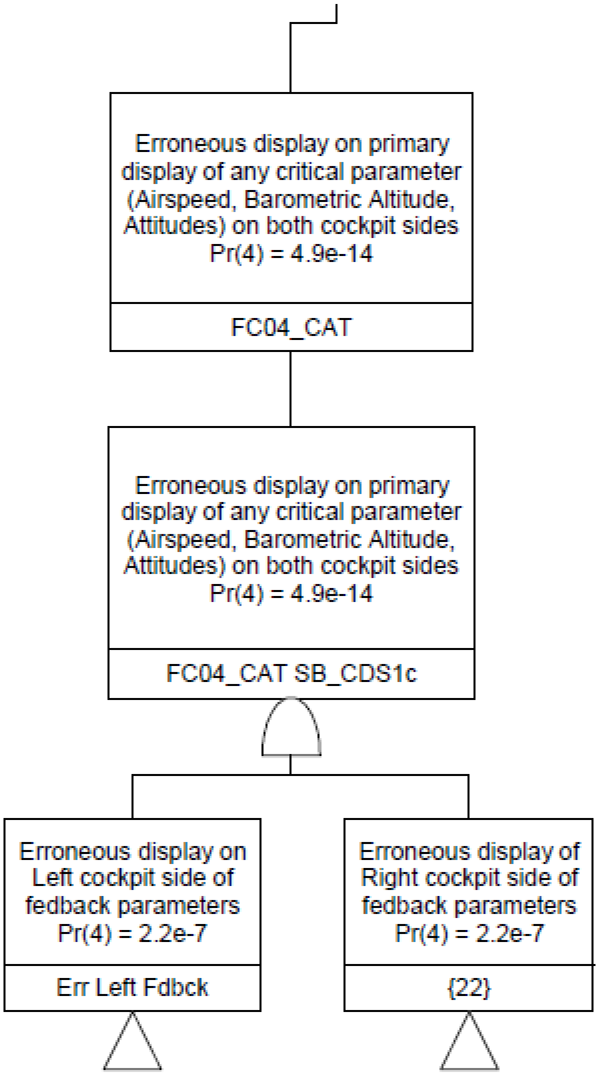

Erroneous display on primary display of any critical parameter (Airspeed, Barometric Altitude, Attitudes) on both cockpit sides
Pr(4) = 4.9e-14
FC04_CAT
Erroneous display on primary display of any critical parameter (Airspeed, Barometric Altitude, Attitudes) on both cockpit sides
Pr(4) = 4.9e-14
FC04_CAT SB_CDS1c
Erroneous display on Left cockpit side of fedback parameters
Pr(4) = 2.2e-7
Err Left Fdbck
Erroneous display of Right cockpit side of fedback parameters
Pr(4) = 2.2e-7
{22}

Figure D-10. Detailed FTA for FC04_CAT

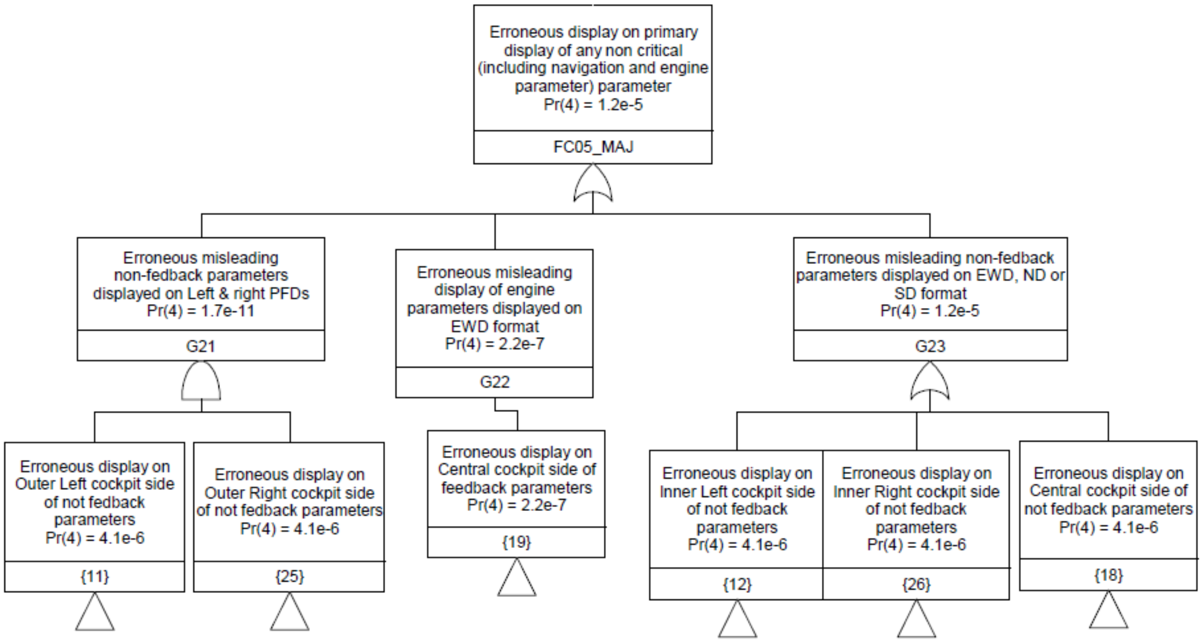

Erroneous display on primary display of any non critical (including navigation and engine parameter) parameter
Pr(4) = 1.2e-5
FC05_MAJ
Erroneous misleading non-fedback parameters displayed on Left & right PFDs
Pr(4) = 1.7e-11
G21
Erroneous misleading display of engine parameters displayed on EWD format
Pr(4) = 2.2e-7
G22
Erroneous misleading non-fedback parameters displayed on EWD, ND or SD format
Pr(4) = 1.2e-5
G23
Erroneous display on Outer Left cockpit side of not fedback parameters
Pr(4) = 4.1e-6
{11}
Erroneous display on Outer Right cockpit side of not fedback parameters
Pr(4) = 4.1e-6
{25}
Erroneous display on Central cockpit side of feedback parameters
Pr(4) = 2.2e-7
{19}
Erroneous display on Inner Left cockpit side of not fedback parameters
Pr(4) = 4.1e-6
{12}
Erroneous display on Inner Right cockpit side of not fedback parameters
Pr(4) = 4.1e-6
{26}
Erroneous display on Central cockpit side of not fedback parameters
Pr(4) = 4.1e-6
{18}

Figure D-11. Detailed FTA for FC05_MAJ

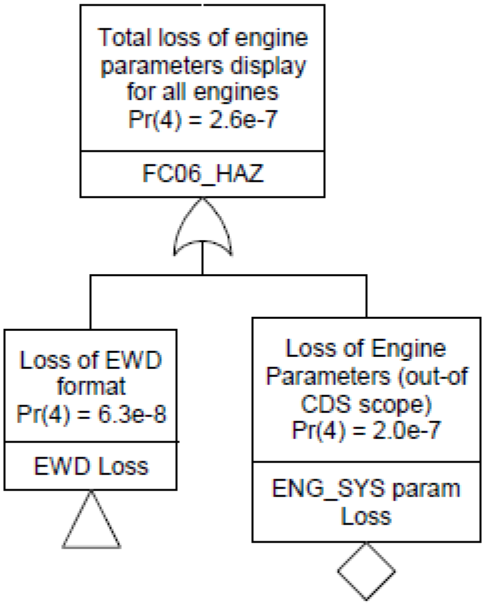

Total loss of engine parameters display for all engines
Pr(4) = 2.6e-7
FC06_HAZ
Loss of EWD format
Pr(4) = 6.3e-8
EWD Loss
Loss of Engine Parameters (out-of CDS scope)
Pr(4) = 2.0e-7
ENG_SYS param Loss

Figure D-12. Detailed FTA for FC06_HAZ

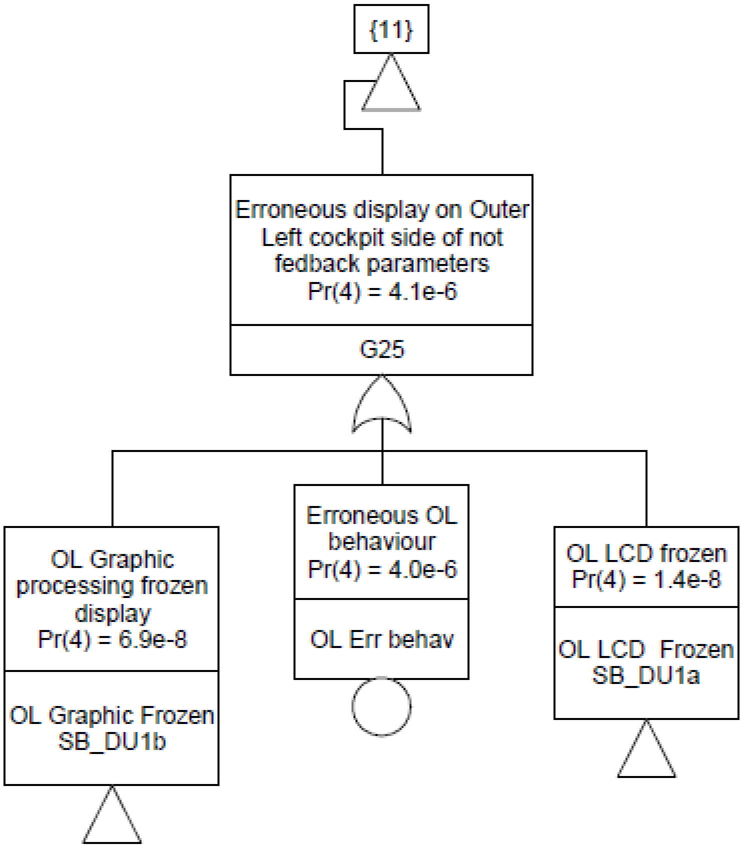


Figure D-13. Detailed FTA for event {11} of figure D-11

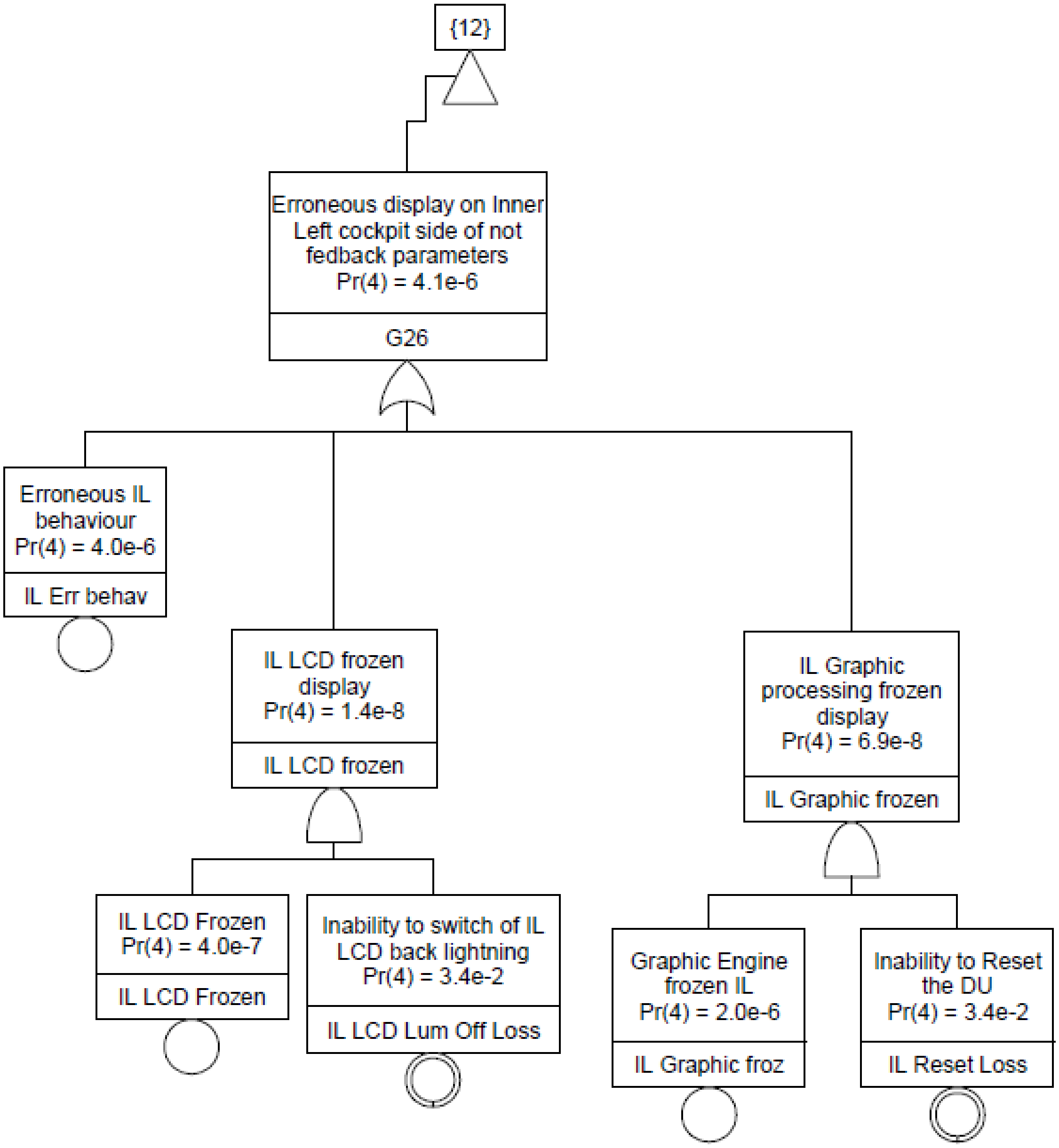


Figure D-14. Detailed FTA for event {12} of figure D-11

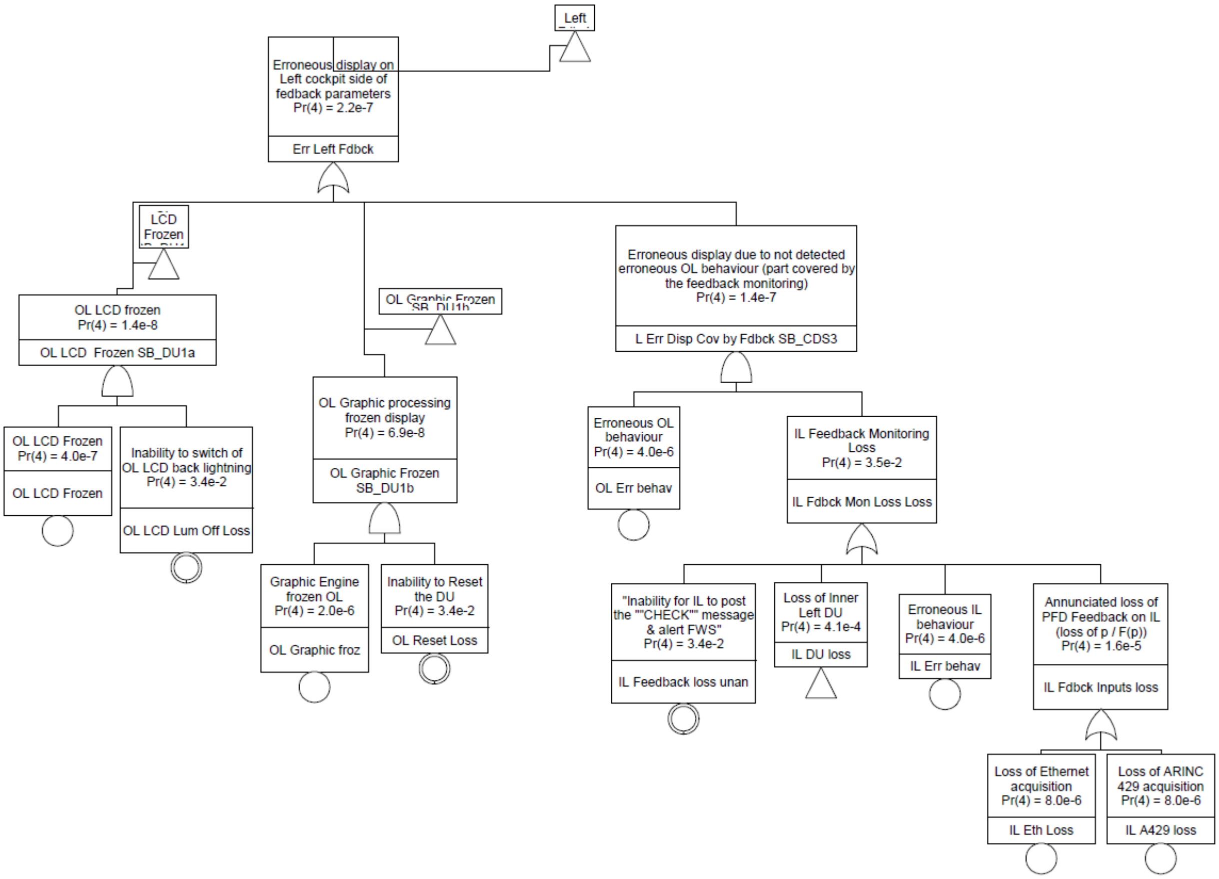

Left
Erroneous display on Left cockpit side of fedback parameters Pr(4) = 2.2e-7
Err Left Fdbck
LCD Frozen
OL LCD frozen Pr(4) = 1.4e-8
OL LCD Frozen SB_DU1a
OL LCD Frozen Pr(4) = 4.0e-7
OL LCD Frozen
Inability to switch of OL LCD back lightning Pr(4) = 3.4e-2
OL LCD Lum Off Loss
OL Graphic Frozen SB_DU1b
OL Graphic processing frozen display Pr(4) = 6.9e-8
OL Graphic Frozen SB_DU1b
Graphic Engine frozen OL Pr(4) = 2.0e-6
OL Graphic froz
Inability to Reset the DU Pr(4) = 3.4e-2
OL Reset Loss
Erroneous display due to not detected erroneous OL behaviour (part covered by the feedback monitoring) Pr(4) = 1.4e-7
L Err Disp Cov by Fdbck SB_CDS3
Erroneous OL behaviour Pr(4) = 4.0e-6
OL Err behav
IL Feedback Monitoring Loss Pr(4) = 3.5e-2
IL Fdbck Mon Loss Loss
"Inability for IL to post the ""CHECK"" message & alert FWS" Pr(4) = 3.4e-2
IL Feedback loss unan
Loss of Inner Left DU Pr(4) = 4.1e-4
IL DU loss
Erroneous IL behaviour Pr(4) = 4.0e-6
IL Err behav
Annunciated loss of PFD Feedback on IL (loss of p / F(p)) Pr(4) = 1.6e-5
IL Fdbck Inputs loss
Loss of Ethernet acquisition Pr(4) = 8.0e-6
IL Eth Loss
Loss of ARINC 429 acquisition Pr(4) = 8.0e-6
IL A429 loss

Figure D-15. Detailed FTA for erroneous left cockpit feedback parameters

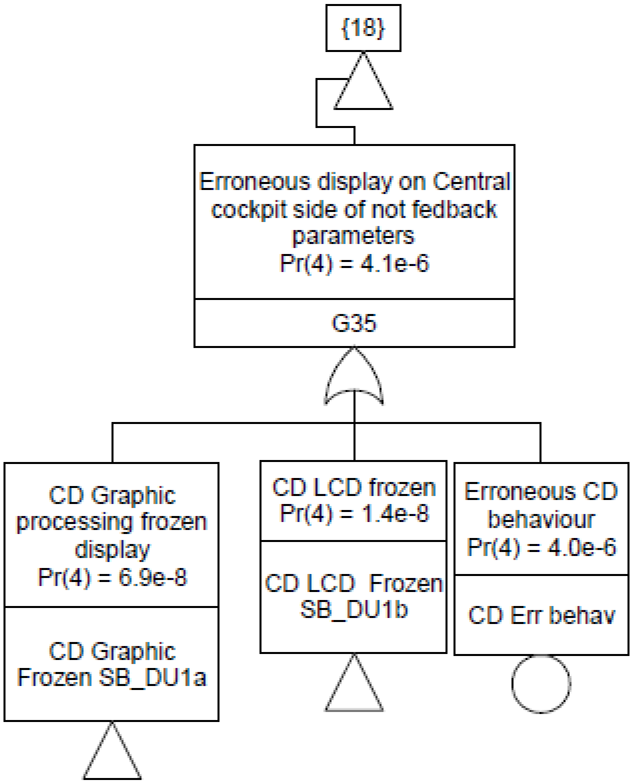


Figure D-16. Detailed FTA of event {18} of figure D-11

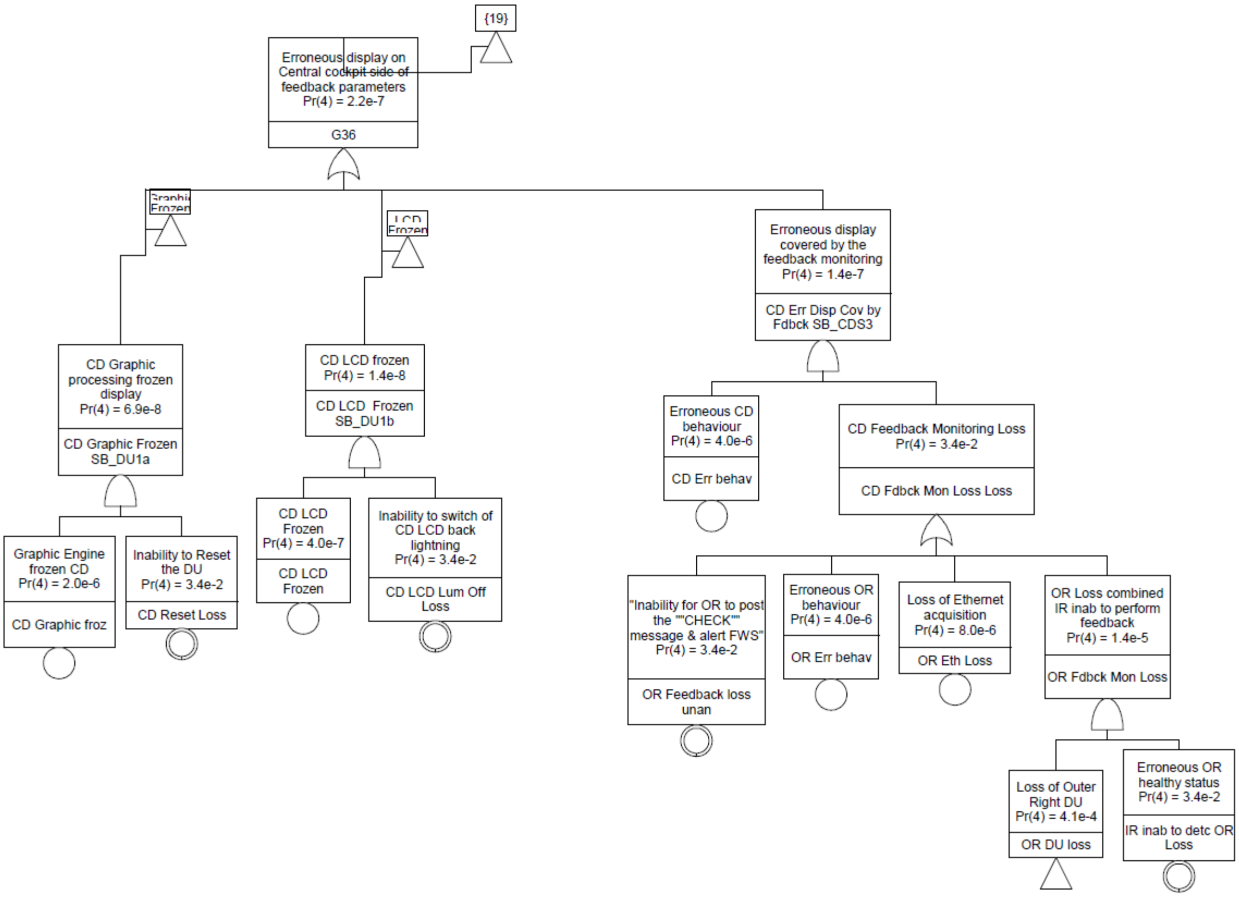

{19}
Erroneous display on Central cockpit side of feedback parameters Pr(4) = 2.2e-7
G36
Graphic Frozen
LCD Frozen
Erroneous display covered by the feedback monitoring Pr(4) = 1.4e-7
CD Err Disp Cov by Fdbck SB_CDS3
CD Graphic processing frozen display Pr(4) = 6.9e-8
CD Graphic Frozen SB_DU1a
CD LCD frozen Pr(4) = 1.4e-8
CD LCD Frozen SB_DU1b
Erroneous CD behaviour Pr(4) = 4.0e-6
CD Err behav
CD Feedback Monitoring Loss Pr(4) = 3.4e-2
CD Fdbck Mon Loss Loss
Graphic Engine frozen CD Pr(4) = 2.0e-6
CD Graphic froz
Inability to Reset the DU Pr(4) = 3.4e-2
CD Reset Loss
CD LCD Frozen Pr(4) = 4.0e-7
CD LCD Frozen
Inability to switch of CD LCD back lightning Pr(4) = 3.4e-2
CD LCD Lum Off Loss
"Inability for OR to post the ""CHECK"" message & alert FWS" Pr(4) = 3.4e-2
OR Feedback loss unan
Erroneous OR behaviour Pr(4) = 4.0e-6
OR Err behav
Loss of Ethernet acquisition Pr(4) = 8.0e-6
OR Eth Loss
OR Loss combined IR inab to perform feedback Pr(4) = 1.4e-5
OR Fdbck Mon Loss
Loss of Outer Right DU Pr(4) = 4.1e-4
OR DU loss
Erroneous OR healthy status Pr(4) = 3.4e-2
IR inab to detc OR Loss

Figure D-17. Detailed FTA of event {19} of figure D-11

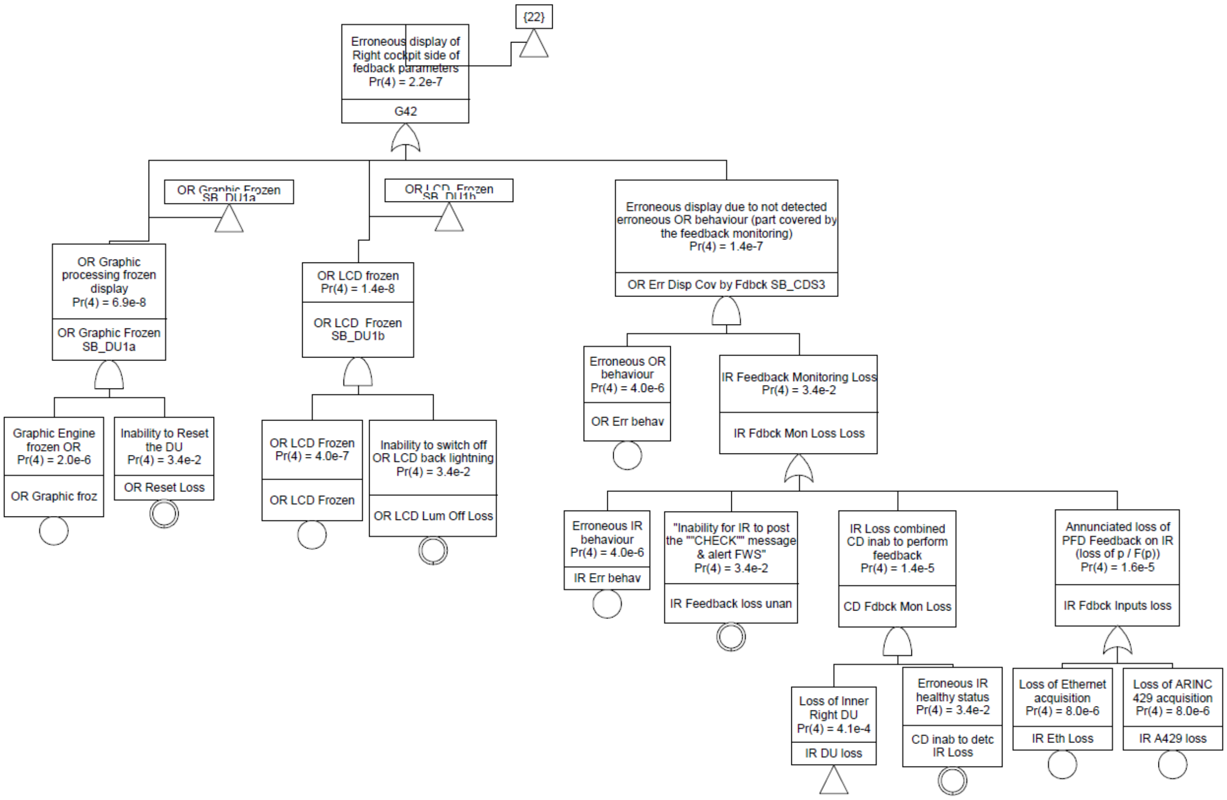


Figure D-18. Detailed FTA of event {22} of figure D-10

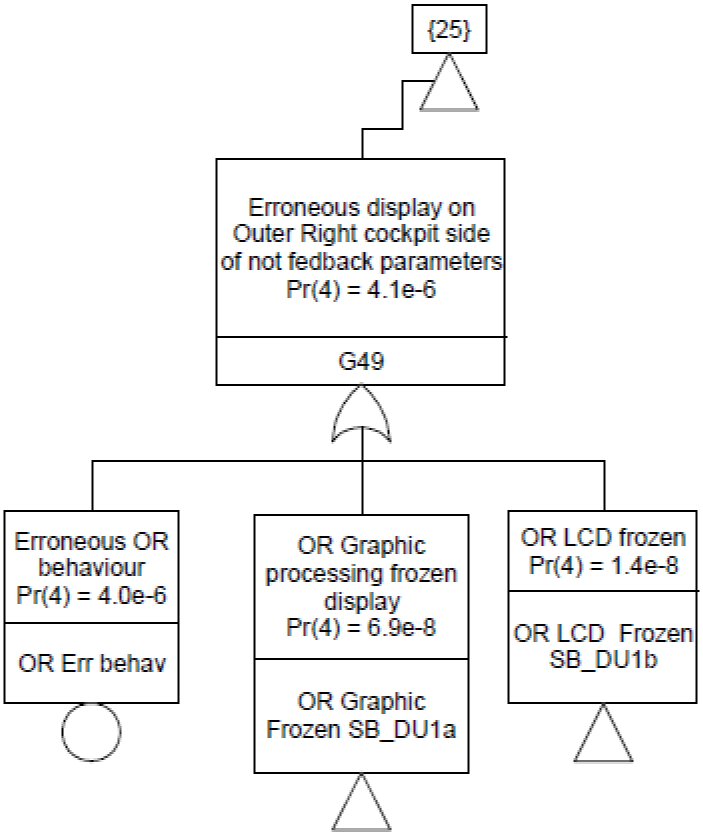

{25}
Erroneous display on Outer Right cockpit side of not fedback parameters
Pr(4) = 4.1e-6
G49
Erroneous OR behaviour
Pr(4) = 4.0e-6
OR Err behav
OR Graphic processing frozen display
Pr(4) = 6.9e-8
OR Graphic Frozen SB_DU1a
OR LCD frozen
Pr(4) = 1.4e-8
OR LCD Frozen SB_DU1b

Figure D-19. Detailed FTA of event {25} of figure D-11

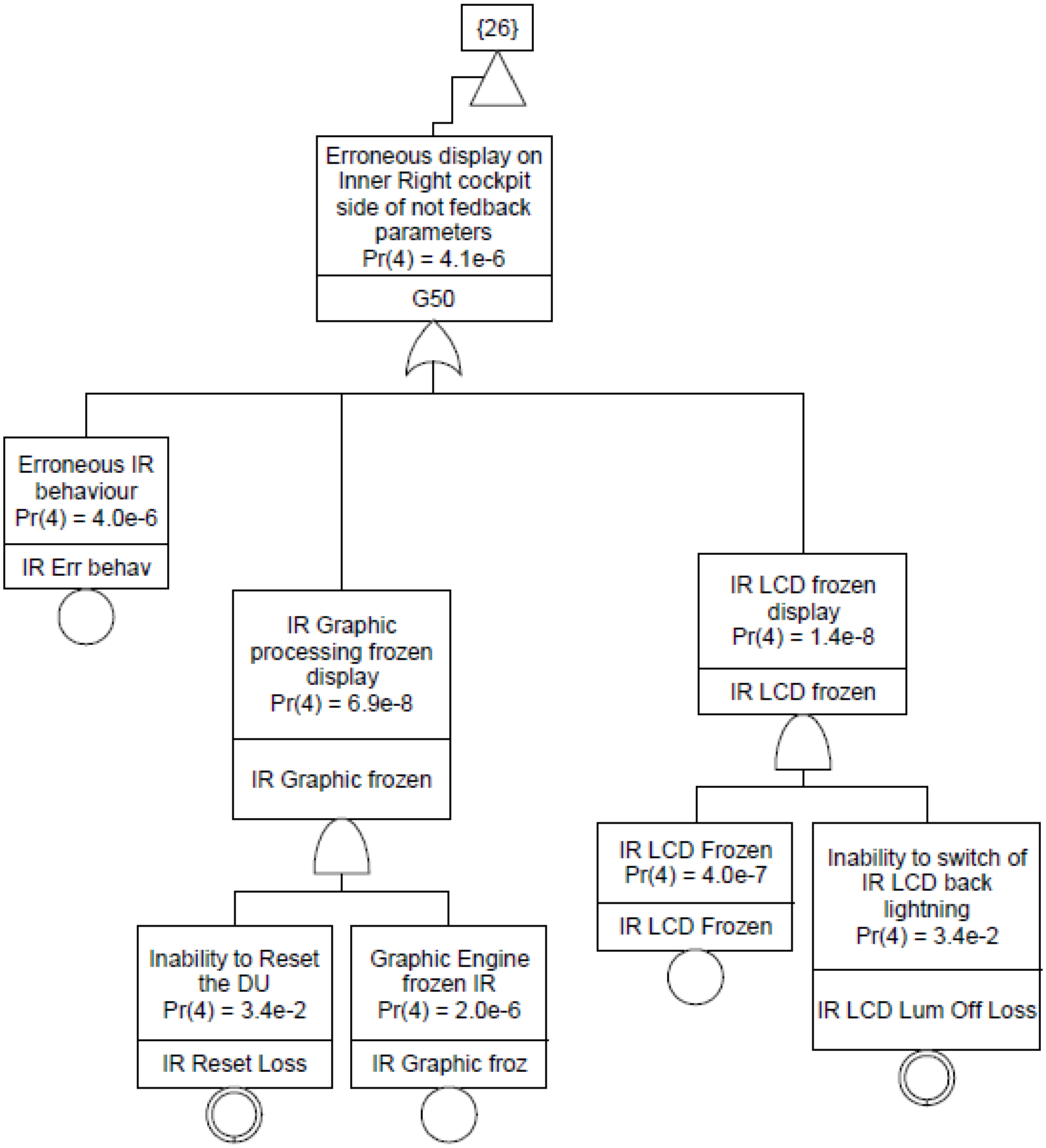


Figure D-20. Detailed FTA of event {26} of figure D-11

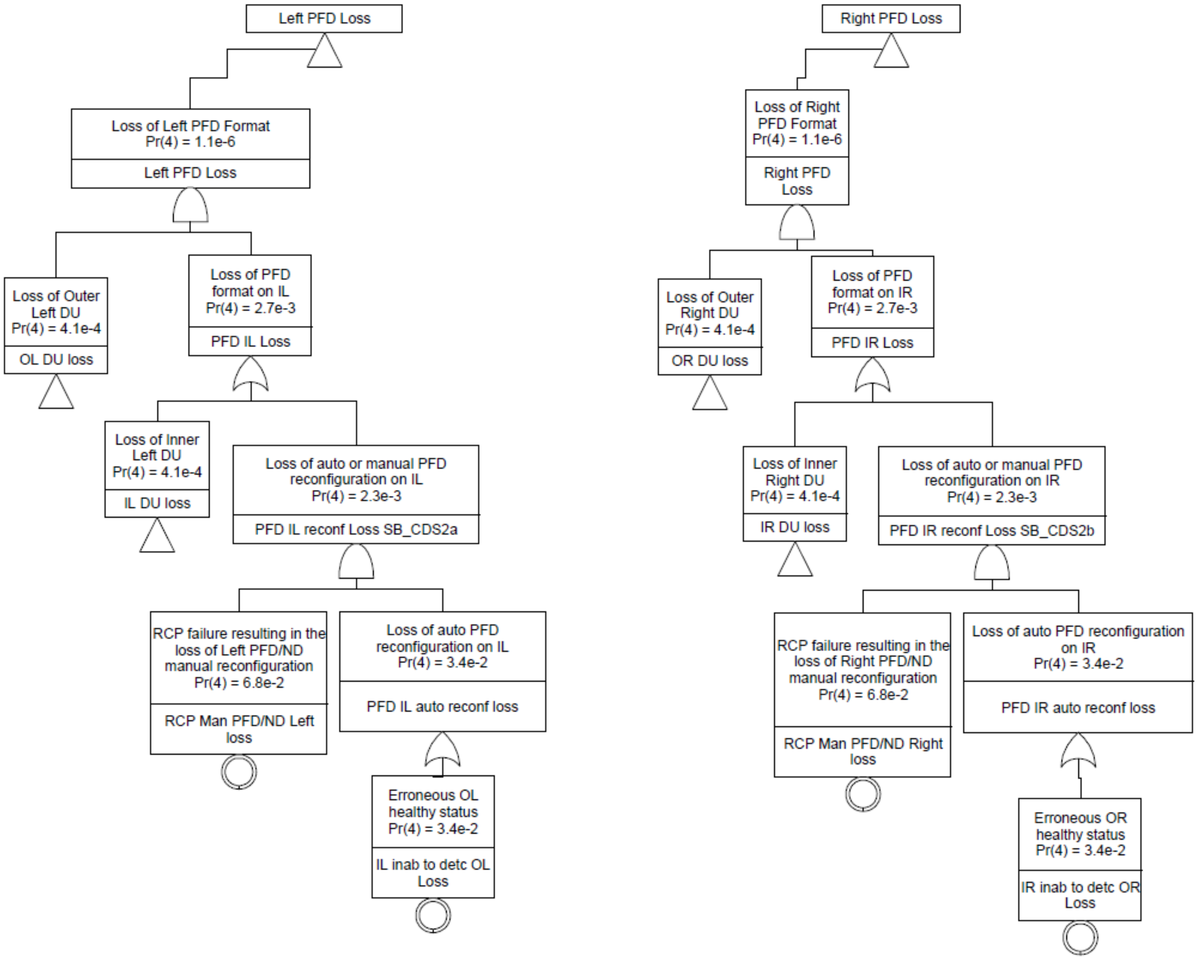


Figure D-21. Detailed FTA for loss of PFD

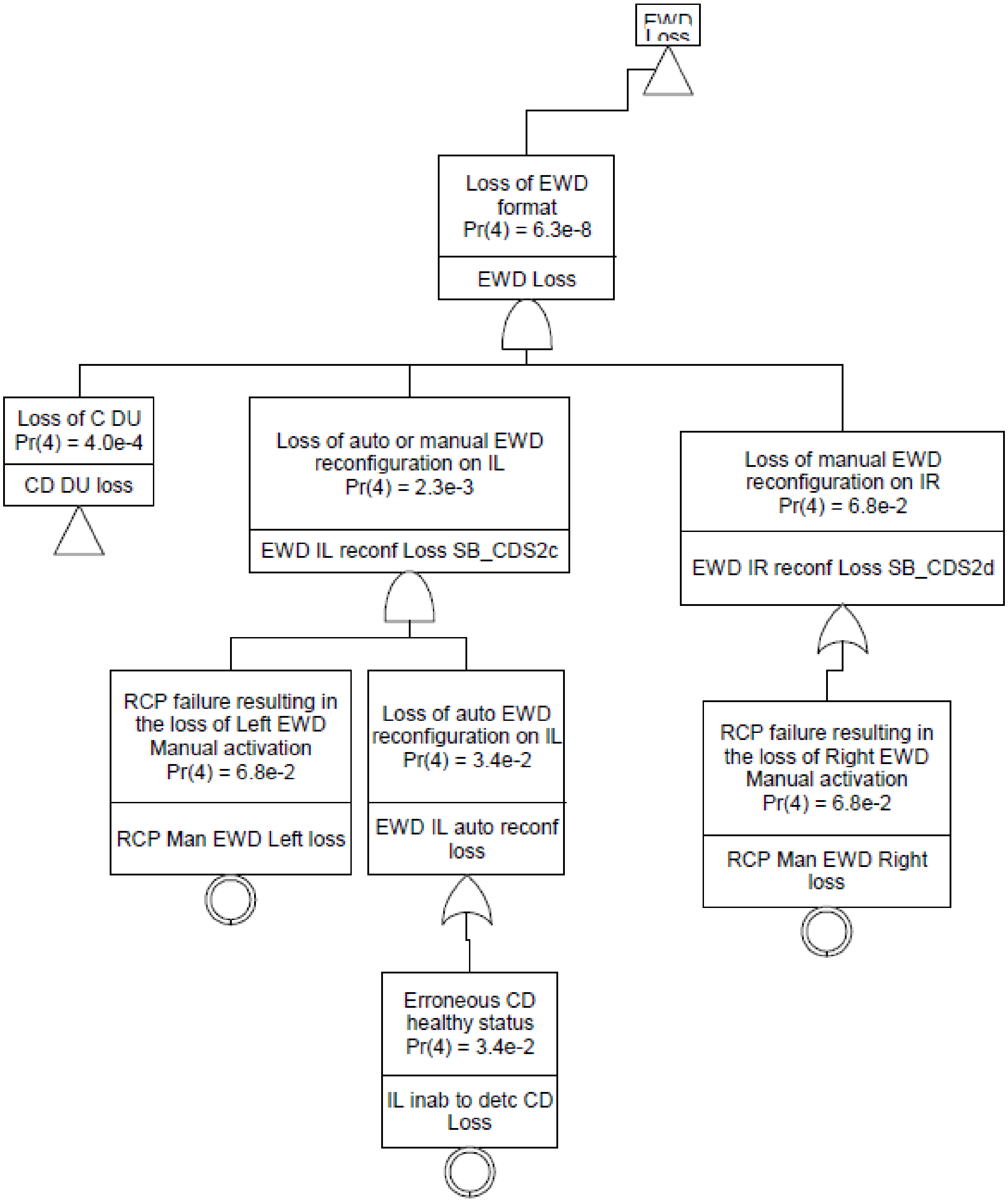

EWD Loss
Loss of EWD format
Pr(4) = 6.3e-8
EWD Loss
Loss of C DU
Pr(4) = 4.0e-4
CD DU loss
Loss of auto or manual EWD reconfiguration on IL
Pr(4) = 2.3e-3
EWD IL reconf Loss SB_CDS2c
Loss of manual EWD reconfiguration on IR
Pr(4) = 6.8e-2
EWD IR reconf Loss SB_CDS2d
RCP failure resulting in the loss of Left EWD Manual activation
Pr(4) = 6.8e-2
RCP Man EWD Left loss
Loss of auto EWD reconfiguration on IL
Pr(4) = 3.4e-2
EWD IL auto reconf loss
RCP failure resulting in the loss of Right EWD Manual activation
Pr(4) = 6.8e-2
RCP Man EWD Right loss
Erroneous CD healthy status
Pr(4) = 3.4e-2
IL inab to detc CD Loss

Figure D-22. Detailed FTA for loss of the engine and warning display

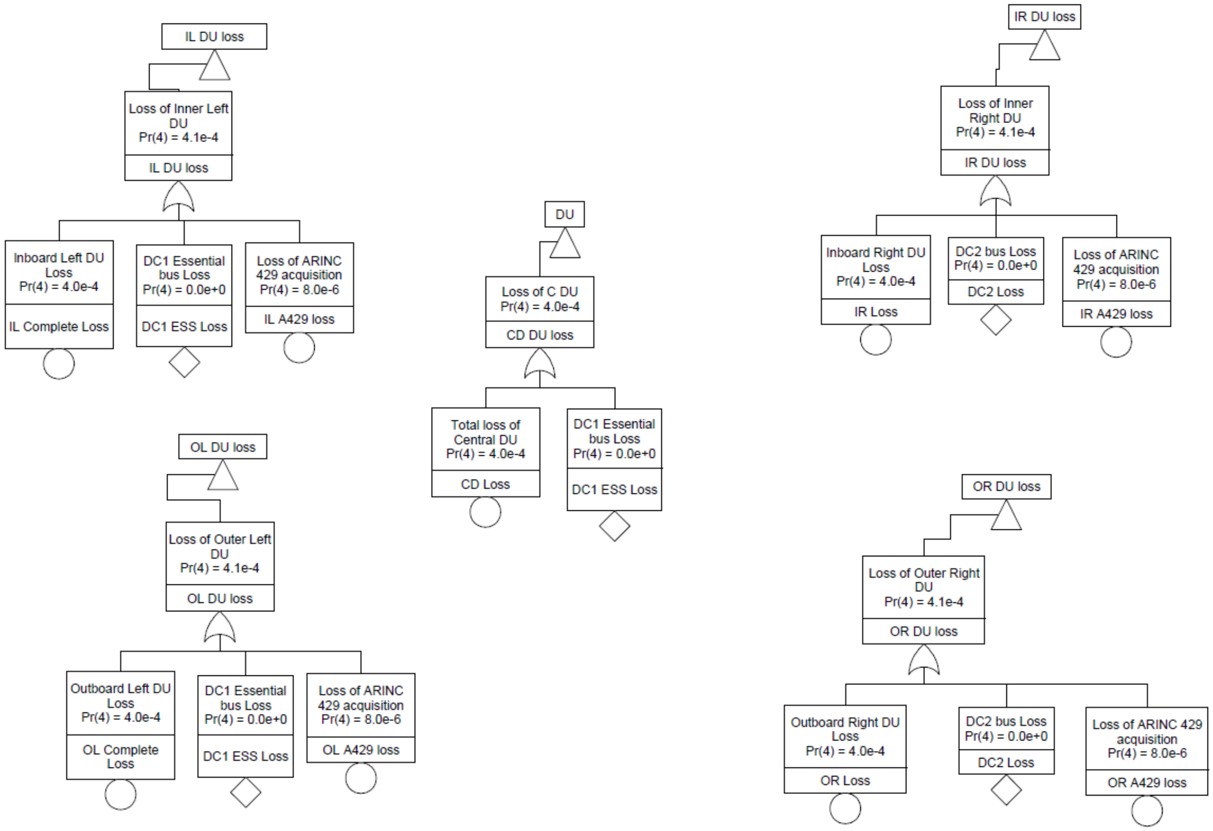

IL DU loss
Loss of Inner Left DU Pr(4) = 4.1e-4
IL DU loss
Inboard Left DU Loss Pr(4) = 4.0e-4
IL Complete Loss
DC1 Essential bus Loss Pr(4) = 0.0e+0
DC1 ESS Loss
Loss of ARINC 429 acquisition Pr(4) = 8.0e-6
IL A429 loss
DU
Loss of C DU Pr(4) = 4.0e-4
CD DU loss
Total loss of Central DU Pr(4) = 4.0e-4
CD Loss
DC1 Essential bus Loss Pr(4) = 0.0e+0
DC1 ESS Loss
IR DU loss
Loss of Inner Right DU Pr(4) = 4.1e-4
IR DU loss
Inboard Right DU Loss Pr(4) = 4.0e-4
IR Loss
DC2 bus Loss Pr(4) = 0.0e+0
DC2 Loss
Loss of ARINC 429 acquisition Pr(4) = 8.0e-6
IR A429 loss
OL DU loss
Loss of Outer Left DU Pr(4) = 4.1e-4
OL DU loss
Outboard Left DU Loss Pr(4) = 4.0e-4
OL Complete Loss
DC1 Essential bus Loss Pr(4) = 0.0e+0
DC1 ESS Loss
Loss of ARINC 429 acquisition Pr(4) = 8.0e-6
OL A429 loss
OR DU loss
Loss of Outer Right DU Pr(4) = 4.1e-4
OR DU loss
Outboard Right DU Loss Pr(4) = 4.0e-4
OR Loss
DC2 bus Loss Pr(4) = 0.0e+0
DC2 Loss
Loss of ARINC 429 acquisition Pr(4) = 8.0e-6
OR A429 loss

Figure D-23. Detailed FTA for loss of inner display unit

APPENDIX E—SUMMARY OF RECOMMENDATIONS

SEE-Rec-001	Failure conditions requiring SEE analysis
SEE-Rec-002	Level of details of system description
SEE-Rec-003	Reporting failure conditions from functional hazard assessment
SEE-Rec-004	Inclusion of transitory functional failure in assessment
SEE-Rec-005	Inclusion of human in the loop/level of automation considerations
SEE-Rec-006	Consideration of interrupted operations
SEE-Rec-007	Minimum mission profile information
SEE-Rec-008	Usage of a single value for neutron flux
SEE-Rec-009	Usage of scaling and/or adjustment(s) to neutron flux value
SEE-Rec-010	Consideration of solar flares
SEE-Rec-011	Types of SEE to be considered for analysis
SEE-Rec-012	Types of SEE error rates to be considered for analysis
SEE-Rec-013	Description of SEE impact
SEE-Rec-014	Coherence between SEE types, technology, and environmental conditions
SEE-Rec-015	Minimum design elements to be collected for SEE analysis
SEE-Rec-016	Claiming attenuation factors based on design
SEE-Rec-017	Additional design information for SET analysis
SEE-Rec-018	Computation of a conservative “raw” SEE rate
SEE-Rec-019	Acceptable units for SEE rate
SEE-Rec-020	Acceptable test data for the quantitative SEE analysis
SEE-Rec-021	Estimating SEE rate at equipment level from component rates
SEE-Rec-022	Substantiation of SEE immunity
SEE-Rec-023	Claiming SEE immunity based on service experience data
SEE-Rec-024	Indirect claims of SEE immunity
SEE-Rec-025	Elements to justify selection of mitigation technique(s)
SEE-Rec-026	Arguments to justify tradeoffs in selecting mitigation technique(s)
SEE-Rec-027	Impact of redundancy on verification method
SEE-Rec-028	Additional information when using built in ECCs with user-selectable feature
SEE-Rec-029	Testing evidence as a function of development assurance level
SEE-Rec-030	Assessment of critical bits
SEE-Rec-031	Additional justification when using heavy ion testing
SEE-Rec-032	Limitation of laser beam testing
SEE-Rec-033	Using margins on static SEE rate
SEE-Rec-034	Additional information when using service experience data
SEE-Rec-035	Information on scope of testing and limitations

APPENDIX F— SUMMARY OF RECOMMENDATIONS PER SINGLE EVENT EFFECT ANALYSIS PHASE

The descriptions of the various phases are extracted from the ongoing work within the Society of Automotive Engineers (SAE) to develop an Aerospace Information Report on Single Event Effect (SEE) Analysis.

Preparation Phase

Requirement Definition	
Safety requirements	SEE-Rec-001, SEE-Rec-003, SEE-Rec-004
Operational mission	SEE-Rec-005, SEE-Rec-006, SEE-Rec-007
Neutron flux definition	SEE-Rec-008, SEE-Rec-009, SEE-Rec-010
Bill of material	SEE-Rec-002, SEE-Rec-011, SEE-Rec-015
Inputs to analysis	
Architecture and design information	SEE-Rec-016, SEE-Rec-017
Components datasheet	SEE-Rec-012, SEE-Rec-013
Available or conservative component SEE rates	SEE-Rec-014, SEE-Rec-018, SEE-Rec-019, SEE-Rec-020, SEE-Rec-021
SEE-immune list/SEE-sensitive list	SEE-Rec-022, SEE-Rec-023, SEE-Rec-024

Qualitative Phase

Identify mitigation through analysis	
Component level mitigations	SEE-Rec-025, SEE-Rec-026
Component without safety impact	N/A
Equipment architecture	SEE-Rec-016, SEE-Rec-017
Assessment of mitigation level	
Mitigated component list	SEE-Rec-026
Input to quantitative analysis	SEE-Rec-025

Quantitative Phase

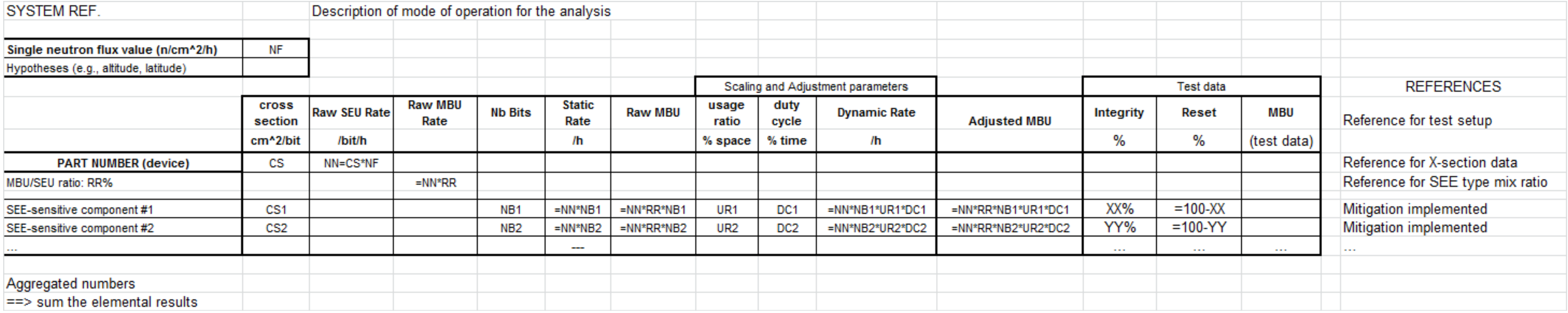
Identify mitigation through analysis	
Component effect rates per SEE type	SEE-Rec-026
SEE rate precision assessment	SEE-Rec-027, SEE-Rec-028, SEE-Rec-029, SEE-Rec-030, SEE-Rec-034
Testing	SEE-Rec-029, SEE-Rec-031, SEE-Rec-032, SEE-Rec-035
Determination of rates at equipment level	
Input information to SSA	SEE-Rec-0034, SEE-Rec-035

Design Process

Component mitigation	None
Component selection	None

APPENDIX G— EXAMPLE WORKSHEET FOR SEE RATE DETERMINATION

The following is provided as an example of how the minimum recommended information used to compute SEE rate per SEE type per device can be organized and used.



SYSTEM REF.		Description of mode of operation for the analysis												
Single neutron flux value (n/cm^2/h)	NF													
Hypotheses (e.g., altitude, latitude)														
							Scaling and Adjustment parameters				Test data			REFERENCES
	cross section	**Raw SEU Rate**	**Raw MBU Rate**	**Nb Bits**	**Static Rate**	**Raw MBU**	**usage ratio**	**duty cycle**	**Dynamic Rate**	**Adjusted MBU**	**Integrity**	**Reset**	**MBU**	Reference for test setup
	cm^2/bit	**/bit/h**			**/h**		**% space**	**% time**	**/h**		%	%	(test data)	
PART NUMBER (device)	CS	NN=CS*NF												Reference for X-section data
MBU/SEU ratio: RR%			=NN*RR											Reference for SEE type mix ratio
SEE-sensitive component #1	CS1			NB1	=NN*NB1	=NN*RR*NB1	UR1	DC1	=NN*NB1*UR1*DC1	=NN*RR*NB1*UR1*DC1	XX%	=100-XX		Mitigation implemented
SEE-sensitive component #2	CS2			NB2	=NN*NB2	=NN*RR*NB2	UR2	DC2	=NN*NB2*UR2*DC2	=NN*RR*NB2*UR2*DC2	YY%	=100-YY		Mitigation implemented
...					---						...	...	...	...
Aggregated numbers														
==> sum the elemental results														

Figure G-1. Example worksheet for computation of SEE rate

APPENDIX H—GLOSSARY FOR IMPACTED ELECTRONIC COMPONENTS

Amplifier
An amplifier is an electronic device that increases the power of a signal by taking energy from a power supply and controlling the output to match the input signal shape, while providing a larger amplitude. In avionics components, power amplifiers are found in servo-motor controllers, transistor amplifiers in radio transmitters contain bipolar junction transistors (BJTs), and metal-oxide semiconductor field effect transistors (MOSFETs) and operational amplifiers (OpAmps) are commonly found in any type of integrated circuit.

Analog-to-Digital Converter (ADC) and Digital-to-Analog Converter (DAC)
An analog-to-digital converter (ADC) is a device that converts a continuous voltage to a digital number representing the voltage’s amplitude. The reverse operation is performed by a digital-to-analog converter (DAC). All types of converters are implemented using at least one comparator; they can add register(s) and clocked gate element(s).

Application-Specific Integrated Circuit (ASIC)
An application-specific integrated circuit (ASIC) is an integrated circuit customized for a particular use. ASICs typically contain microprocessor(s) and memory blocks (read-only memory [ROM], random access memory [RAM], electrically erasable programmable read-only memory, and flash memory).

Bipolar Junction Transistor (BJT)
A bipolar junction transistor (BJT) is a type of transistor based on the contact of two types of semi-conductors characterized by two kinds of charge carriers (electrons and holes). The charge flow in an NJT is due to bidirectional diffusion of the charge carriers across the junction between two regions (emitter, collector, or base) of different charge concentrations. BJTs come in two types: PNP (junction share a p-doped anode region) and NPN (junction share an n-doped cathode region). BJT are present in discrete circuit design, analog circuits, amplifiers, and temperature sensors.

Complementary Metal-Oxide Semiconductor (CMOS)
A complementary metal-oxide semiconductor (CMOS) is a technology for constructing integrated circuits. It is used in microprocessors, micro-controllers, static RAM (SRAM), and other digital logic circuits. CMOS circuits use a combination of p-channel and n-channel MOSFETs to implement logic gates.

Comparator
A comparator is a device that compares two voltages or currents and outputs a digital signal indicating which is larger. An OpAmp can replace a comparator when performance requirements are low.

Content Addressable Memory (CAM)
Content addressable memory (CAM) is a special type of memory used in high-speed searching applications: the user supplies a data word and the CAM searches the entire memory to see if the

data word is stored somewhere in it. If the data word is in memory, the CAM returns a list of one or more storage addresses from which the word was found. Unlike a RAM chip with simple storage cells, each individual memory bit in a fully parallel CAM must have its own comparison circuit to detect a search match. To limit the increased complexity, size, and cost, some implementations emulate CAM functionality by using hardware-coded tree searches (e.g., replication, pipelining). Such implementations can be found in routers. Other uses of CAM include database engines, data compression hardware, and artificial neural networks.

Direct Current (DC)-to-DC Converter

A direct current (DC)-to-DC converter is an electronic circuit which converts a source of DC from one voltage level to another. Switching converters employ MOSFET or bipolar switches.

Diode

A diode is a two-terminal electronic component with asymmetric conductance (low resistance to current flow in one direction and high resistance in the other). Diodes are used to regulate voltage, steer current, protect circuits from high voltage surges, electronically tune radio frequency, and participate in the construction of AND and OR logic gates.

A semiconductor diode is a crystalline piece of semiconductor material with a p-n junction connected to two electrical terminals (N-type side or cathode and P-type side or anode). They are found in CMOS integrated circuits (two diodes per pin in addition to internal diodes). A PIN diode has a p-type/un-doped layer/n-type structure used as radio-frequency switches and attenuators but also in power electronics. The PIN structure can be found in IGBTs, power MOSFETs, and thyristors. Transient voltage suppression diodes have a larger p-n junction to conduct large current to ground and therefore protect other semiconductor devices from high-voltage transients.

Error Detection and Correction

Error detection and correction techniques are techniques that enable reliable delivery of digital data over unreliable communication channels. Error detection identifies errors caused by noise or other impairments during the transmission, and error correction includes the reconstruction of the original error-free data.

Error-detection schemes include checksums (e.g., CRC, parity bit), random-error-correcting codes, and repetition codes.

An error correction code (ECC) or forward error correction (FEC) adds redundant data (or parity data) to a message and is often used in RAM. An error-correcting memory or EDAC-protected memory (DRAM) is used for high fault-tolerant applications, such as servers, or for increased protection against radiation; they may combine ECC with TMR or use interleaving.

Field Programmable Gate Array (FPGA)

A field programmable gate array is an integrated circuit designed to be configured after manufacturing. FPGAs intensively use logic gates and memory elements (e.g., FF and RAM blocks), but they can also embed analog features such as differential comparators on input pins and peripheral ADCs and DACs.

Flash Memory
Flash Memory is an electronic, non-volatile computer-storage medium that can be electrically erased and reprogrammed. Flash memories are of two different types based on the implemented logic gates: NAND Flash memory and NOT OR (NOR). NAND flash memory is used in main memory, memory cards, USB, and solid-state drives, whereas NOR type is used to replace the obsolete ROM.

Flash memory stores information in an array of memory cells made from floating-gate transistors (resembling a MOSFET with two gates).

Flip-Flop (FF) or Latch
A flip-flop or latch is a circuit with two stable states that can be used to store state information. The circuit can change state using signals applied to one or more control inputs and will produce one of two outputs. FFs are the basic storage elements in sequential logic, but can also be used to count pulses or synchronize variably timed input signals to some reference timing signal.

Latch is the term mainly used to refer to a level-sensitive storage element, whereas FF describes edge-sensitive clocked devices.

FF or latches can be implemented using bipolar transistors, inverters, and inverting logic gates (NOR, NAND).

Globally Asynchronous Locally Synchronous (GALS)
A globally asynchronous locally synchronous device implements a model of computation in which the synchrony assumption in a computer is relaxed by designing synchronous “islands” interacting with each other over asynchronous communication (e.g., first-in, first-out).

Guard Ring
A guard ring surrounds an area in which surface current may be an issue and thus provides the circuit with isolation from any substrate noise caused by a digital or high-frequency switching circuit. The noise spike can turn on a latch, which generates parasitic NPN-PNP transistors from the N and P structure in CMOS.

Hamming Codes
Hamming codes are a family of linear error-correction codes that detect up to two-bit errors or correct one-bit errors without detection of uncorrected errors. Because of the limited redundancy added by these codes to the data, they can only detect and correct errors in cases for which the error rate is low. This makes them particularly attractive for implementation in computer memory (the bit errors are extremely rare). Hamming codes can be paired with parity to increase the detection-correction performance.

Insulated-Gate Bipolar Transistor (IGBT)
An insulated-gate bipolar transistor is a three-terminal power semiconductor device used as an electronic, highly-efficient, and fast switch. Amplifiers implementing pulse-width modulation or low-pass filters typically may use IGBT.

The IGBT cell forms a vertical PNP BJT with a cascade connection to a surface n-channel MOSFET.

Inverter

An inverter is a logic gate implementing logical negation (NOT). It can be implemented using a single N-metal-oxide semiconductor transistor (or PMOS) coupled with a resistor using two complementary transistors in a CMOS configuration or with BJTs in resistor-transistor or transistor-transistor logic configurations.

Inverters are the building blocks of digital electronics: a memory cell (1-bit register) is implemented by feeding the output of two inverters to each other's input.

Metal-Oxide-Semiconductor Field-Effect Transistor (MOSFET)

A metal-oxide-semiconductor field-effect transistor **(MOSFET)** is a silicon-based transistor used for amplifying or switching electronic signals. A power MOSFET has a vertical structure instead of a planar one, so that the transistor can sustain both high blocking voltage and high current.

The RHBD MOSFET is designed using an enclosed-layout-transistor approach, whereas the MOSFET drain is in the center, surrounded by the gate and then the source; another RHBD MOSFET is called an H-Gate. Both transistors have very low-leakage current with respect to a radiation environment, but they carry a large area penalty.

NAND Gate

A NAND gate is a logic gate that produces an output that is false only if all of its inputs are true. The attractiveness of a NAND gate is its functional completeness (any other logic function can be implemented solely using NANDs). The CMOS integrated circuit and transistor-transistor logic make use of NAND gates.

Parasitic Structure

A parasitic structure is a portion of the device that resembles in structure some other, simpler semiconductor device and causes the device to enter an unintended mode of operation. For example, the internal structure of an NPN bipolar transistor resembles two PN junction diodes connected by a common anode. Although the base-emitter junction does indeed form a diode, it is most of the time not desired for the junction to behave as a diode. If a sufficient forward bias is applied on the junction, it will form a parasitic diode structure.

Parity Bit

A parity bit is a bit added to the end of a string of binary code that indicates whether the number of bits in the string with a unit value is even or odd. Parity bits are the simplest form of error-detecting code. There are two types of parity bits: odd and even. Even parity is a special case of CRC in which the 1-bit parity CRC is generated by the polynomial x+1. A parity bit requires only XOR gates to be generated.

Random Access Memory (RAM)

Random Access Memory (RAM) is a form of computer data storage allowing stored data to be accessed directly in any random order. There are three main forms of RAM: SRAM, DRAM, and phase-changed random access memory (PRAM).

In SRAM, a bit of data is stored using the state of an FF; this type is often used for cache memory. DRAM stores a bit of data using a transistor-capacitor pair forming a memory cell; it is less expensive to produce than RAM and dominates the implementation of computer memory. Both DRAM and SRAM can include ECC for enhanced reliability.

Switch
A switch is an electrical component that can break an electrical circuit by interrupting the current or diverting it from one conductor to another.

Electronic switches (relay) control power circuits by using a semiconductor device to perform the switching. An analog switch uses two MOSFET transistors in a transmission gate arrangement. A power supply unit uses power transistors in its switching voltage regulator.

Transistor
A transistor is a semiconductor device used to amplify and switch electronic signals and electrical power. It is composed of semiconductor material with at least three terminals for connection to an external circuit.

There are two types of transistors: bipolar transistors with base-collector-emitter terminals (e.g., BJT and IGBT) and field-effect transistors with gate-source-drain terminals (e.g., MOSFET). Transistors are commonly used as switches or amplifiers, with BJT remaining the choice for analog circuits and MOSFET for digital circuits.

Voltage Regulator
A voltage regulator is designed to automatically maintain one constant or several alternating current or DC voltage(s). Electronic voltage regulators are found in computer voltage supplies, in power plants to control the plant output, and within power distribution lines. Voltage regulators can be implemented with resistor(s) and diode(s) as well as transistors, and can be complemented by OpAmps to stabilize the output voltage.