UNDERSTANDING THE IMPACT OF SINGLE EVENT EFFECTS (SEE) ON SYSTEM SAFETY

MANJU MAHEVE

PRINCIPAL RMS ENGINEER

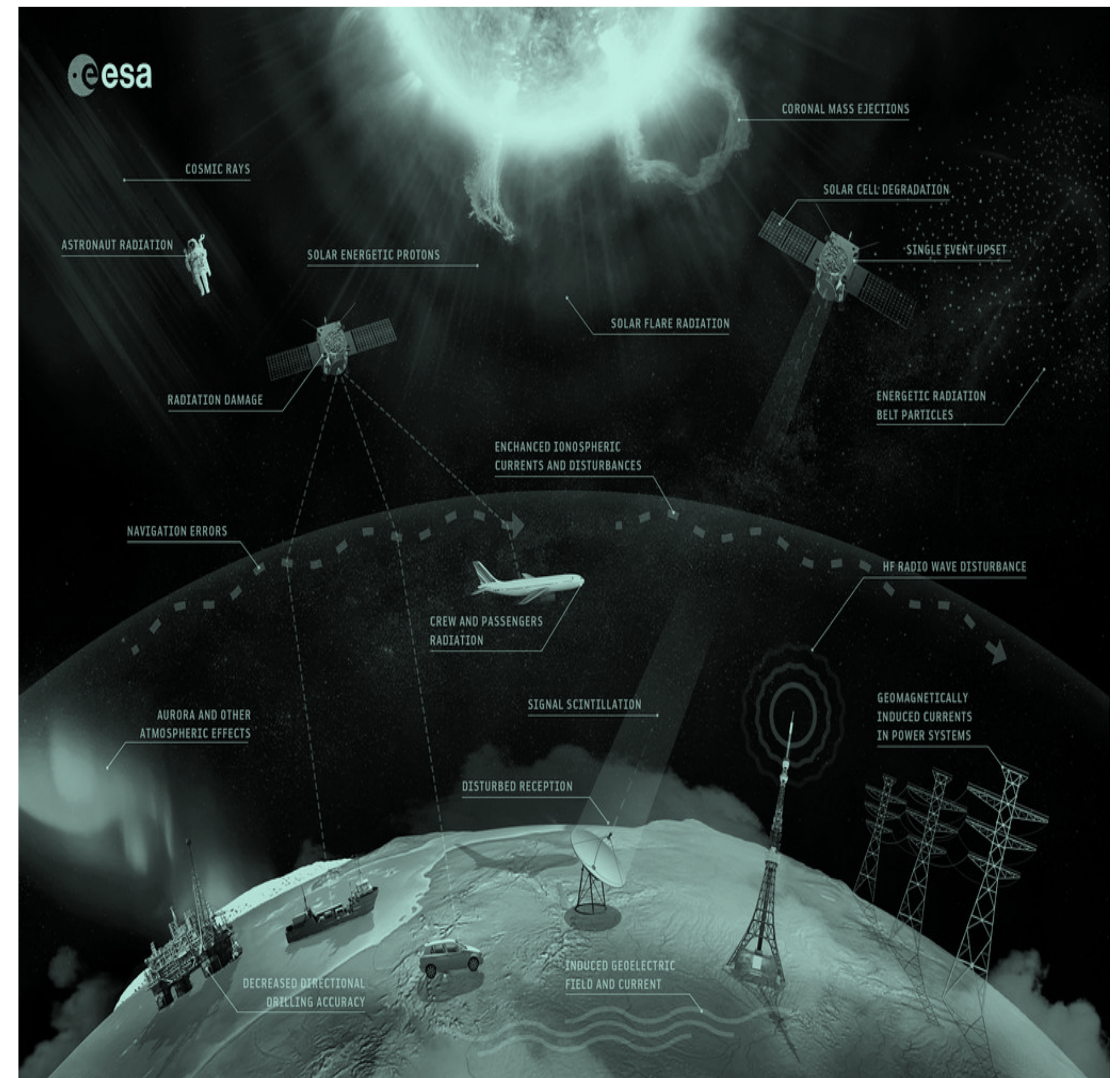
OUTLINE

- Definition of SEE
- Types of SEE
- Why concerned about Neutron Single Event Upsets (NSEUs)?
- SEE Analysis Process
- How to account SEE failures in SSA?
- How to address the impact of SEE ?

This document does not include any export controlled technical data.

DEFINITION OF SEE

- A Single Event Effect (SEE) is an electrical disturbance that <u>disrupts the normal operation of a circuit</u>
- It is caused by the passage of a single ion through or near a sensitive node in a circuit
- Single Event Effects can be either destructive or non- destructive



This document does not include any export controlled technical data.

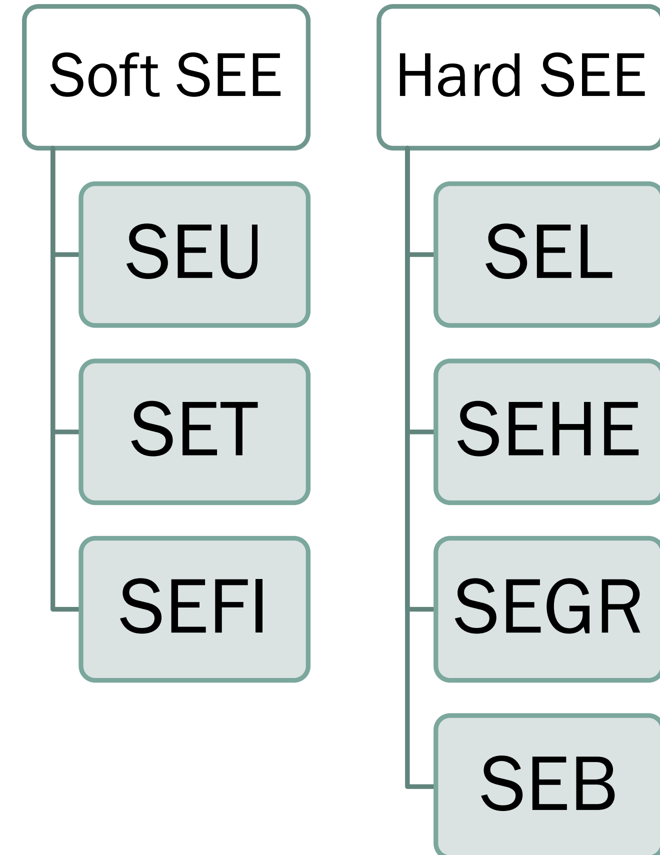
WHY SEE

- 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 a SEE to a device/Memory
- Flights at higher altitudes and/or on polar routes increase likelihood of a SEE due to increased radiation

This document does not include any export controlled technical data.

TYPES OF SEE

- Single Event Effects (SEE) are electronic events caused by one highly energetic particle
- Soft SEE errors such as Single Event Upset (SEU), Single Event Transient (SET) & Single Event Functional Interrupt (SEFI)
- Hard SEE errors such as Single Event Latch-up (SEL), Single Event Hard Errors (SEHE), Single Event Gate Rupture (SEGR) and Single Event Burnout (SEB)
- The severity of SEEs depends on the type of the effect and how critical the system is



This document does not include any export controlled technical data.

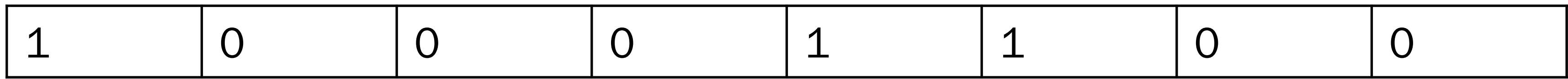
SOFT SEE- SEU

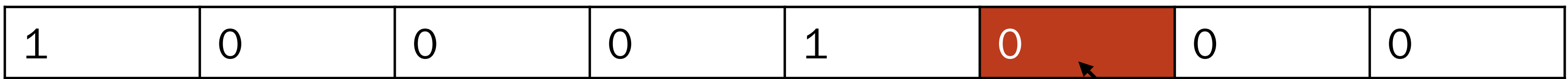
SEU - Single Event Upset

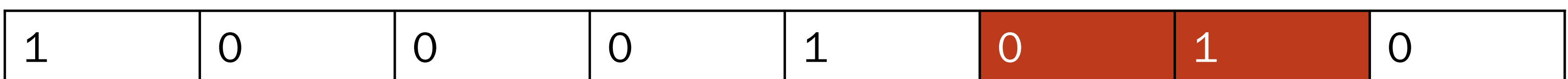
SEU is a change of state of an electronic device storage element caused by a single ionizing particle. These events usually do not affect the reliability and function of a system over time and are easier to fix than hard errors.

- One Bit upset are called Single Bit Upsets (SBU)
- Multiple upsets are named Multiple Cell Upsets (MCU)
- Several upset cells that are part of the same logic word are Multiple Bit Upsets (MBU)
    - MBU results in multiple bit errors from a single particle event

The SEUs usually affect latches, memory devices, and sequential logic







This document does not include any export controlled technical data.

SOFT SEE

SET - Single Event Transient

- Occurs when the motion of charges by a single particle, causes a temporary (transient) voltage glitch
- Transient can recover quickly without any power reset
- Erroneous data may be passed to downstream memories where the effect is not transient
- Faster devices have a higher chance of being SET instead of SBU or MBU
  - SETs affect mostly analog and mixed-signal circuits

SEFI - Single Event Functional Interrupt

- Device stops normal functions
- Requires a cycling the power, resetting, or reloading a configuration register to resume normal operations
  - Special case of SEU changing an internal control signal

This document does not include any export controlled technical data.

HARD SEE

SEL - Single Event Latch-up

- Hard fault
- Latch-up is caused by a charged particle creating a short across the device
- Potential loss of device functionality
- Destructive condition
  - The device is not permanently damaged, but power cycling is required to resume normal device operation

SEHE - Single-Event Hard Errors

- Stuck bits
  - Memory bits that are unable to be changed by a write process, therefore rendered non-functional
  - Memory cell gets "pinned" to either a "1" or "0" state

This document does not include any export controlled technical data.

HARD SEE

SEGR - Single Event Gate Rupture

- Affects mainly the power MOSFET
- Also observed in MOS-based digital and linear ICs resulting in destructive consequences
- Observed simultaneously with Single Event Burnout (SEB) in power MOSFETs

SEB - Single Event Burnout

- Hard error often results in catastrophic failure of the memory or device.
- SEB affects primarily bipolar transistors and N-channel power MOSFET in space
- Observed in high voltage diodes in terrestrial applications

For any device that is not immune to SEL or other potentially destructive conditions, protective circuitry must be added to eliminate the possibility of damage and verified by analysis and test

Latent damage must be addressed

This document does not include any export controlled technical data.

SEE TYPES, EFFECT AND IMPACT ON THE COMPONENTS

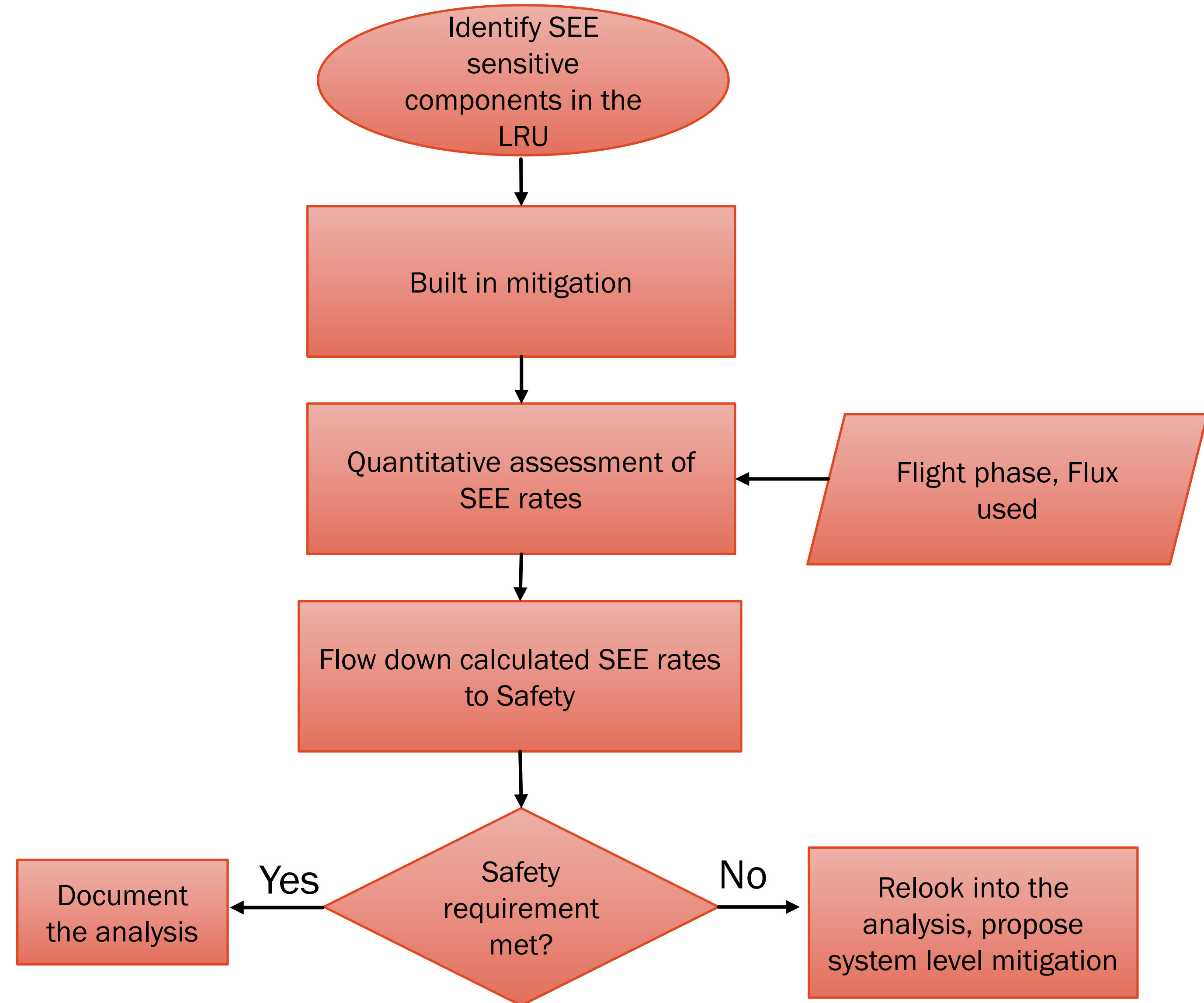
SEE Type	Effect	Affected components
SEU	Corruption of the information stored in a memory element	Memories, latches in logic devices
MBU	Corruption of several memory elements in a single hit	Memories, latches in logic devices
SEFI	Loss of normal operation	Complex devices with built-in state/control sections
SET	Impulse response of certain amplitude and duration	Analog and mixed-signal circuits, photonics
SEL	High-current conditions, flipped bits uncorrectable by a logic reset	CMOS devices
SEB	Destructive burnout	Bipolar junction transistors, N-channel power MOSFET
SEGR	Rupture of gate dielectric	Power MOSFET

This document does not include any export controlled technical data.

SEE ANALYSIS PROCESS

An analysis should be performed for each equipment, which contributes to a Catastrophic or Hazardous or Major failure condition.

Resulting from this, a parts list should be produced to identify the electronic devices contributing to Catastrophic or Hazardous or Major failure conditions.



This document does not include any export controlled technical data.

SEU RATE CALCULATIONS

In order to determine if a system's safety and reliability requirements can be met, it is necessary to first quantify the system SEE rate.

- System SEE rate - combined SEE rates of all susceptible components that are used in the system
- Impacts of mitigation
- Incorporated in overall system failure rate & measured against the safety and reliability requirements

1. For each device which has been determined to likely be SEE sensitive, request the Component group to contact the device supplier to obtain SEE data
2. If no data is available, use the alternate estimation techniques
3. SEU Rate is calculated as
   SEU rate= σ x Φ (at desired altitude & latitude)
   σ – cross section
   Φ – Flux (particles/cm^2 – sec (or -h).
4. Cross section area is a figure of merit that establishes how sensitive the component is to the effects of atmospheric radiation
   - Different types of effects, such as SEU or SEL, will have different cross sections

Average neutron flux rate at cruise flight environment - 6,000 n/cm^2/hr (>150nm), 9200 n/cm^2/hr (<150nm) [Ref IEC TS 62396-1]

Flux value - 40,000 feet and 45 degrees latitude [Ref IEC TS 62396-1]

This document does not include any export controlled technical data.

EXAMPLE: SEU RATE CALCULATIONS

PART DESCRIPTION	λ_{SER} (SEU/FH)	ERROR DETECTION	SYSTEM EFFECT
FPGA3, MICROPROCESSOR	2.4×10^{-5}	ECC	NO EFFECT ON System
RECEIVE DPRAM, MICROPROCESSOR	8.16×10^{-4}	PARITY	IMPACT ON THE AVAILABILITY OF THE SYSTEM
TRANSMIT DPRAM, MICROPROCESSOR	8.16×10^{-4}	PARITY	IMPACT ON THE AVAILABILITY OF THE SYSTEM
DISCRETE I/O	4.08×10^{-5}	CHECKSUM	FUNCTION OF A CHANNEL EXPERIENCES A TRANSIENT UPSET

Details on calculating SEE rates in avionics are provided in the IEC Technical Specification IEC TS 62396-1.

- Where actual test or manufacturer data is not available, a full neutron energy spectrum upset cross section of 1E-13 cm^2/bit can be used for SEU events in SRAM or Flip flops.
- Where actual test or manufacturer data is not available, a full neutron energy spectrum cross section of 3E-14 cm2/bit can be used for MBU events.
- These cross section values are conservative relative to typical measured SEU cross sections (<150nm)

This document does not include any export controlled technical data.

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 (HAZ) or major (MAJ) 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.
- 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 SSA is completed when compliance with the safety objectives is shown for the design. System-level Safety Barrier are adjusted until the compliance is demonstrated.

This document does not include any export controlled technical data.

SEE IMPACT ON SYSTEM

- ❑ 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

This document does not include any export controlled technical data.

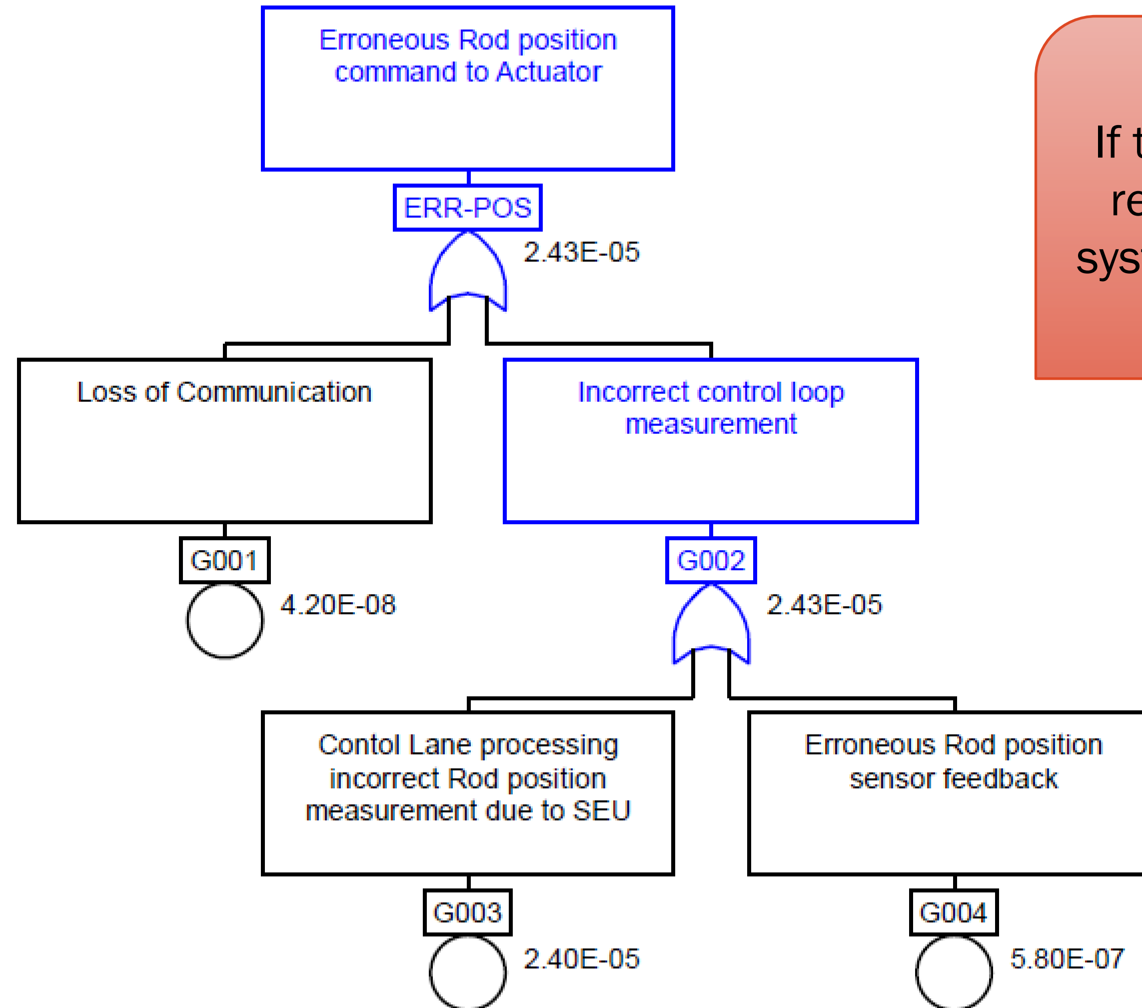
EQUIPMENT LEVEL SEE ANALYSIS

- Component-level FMEA is performed to verify the compliance of the equipment design with the derived safety objectives allocated to the equipment
- SEE safety assessment is performed—taking into account built-in mitigations
- Compare SEE rates to the failure rates derived from the FMEA for a verified design
  - SEE rates are negligible → Design complaint
  - SEE rates are not negligible → Verify Compliance with top level Safety objectives

Types of component technology used & previous “in-service” history can be used to show system effect due to SEE

This document does not include any export controlled technical data.

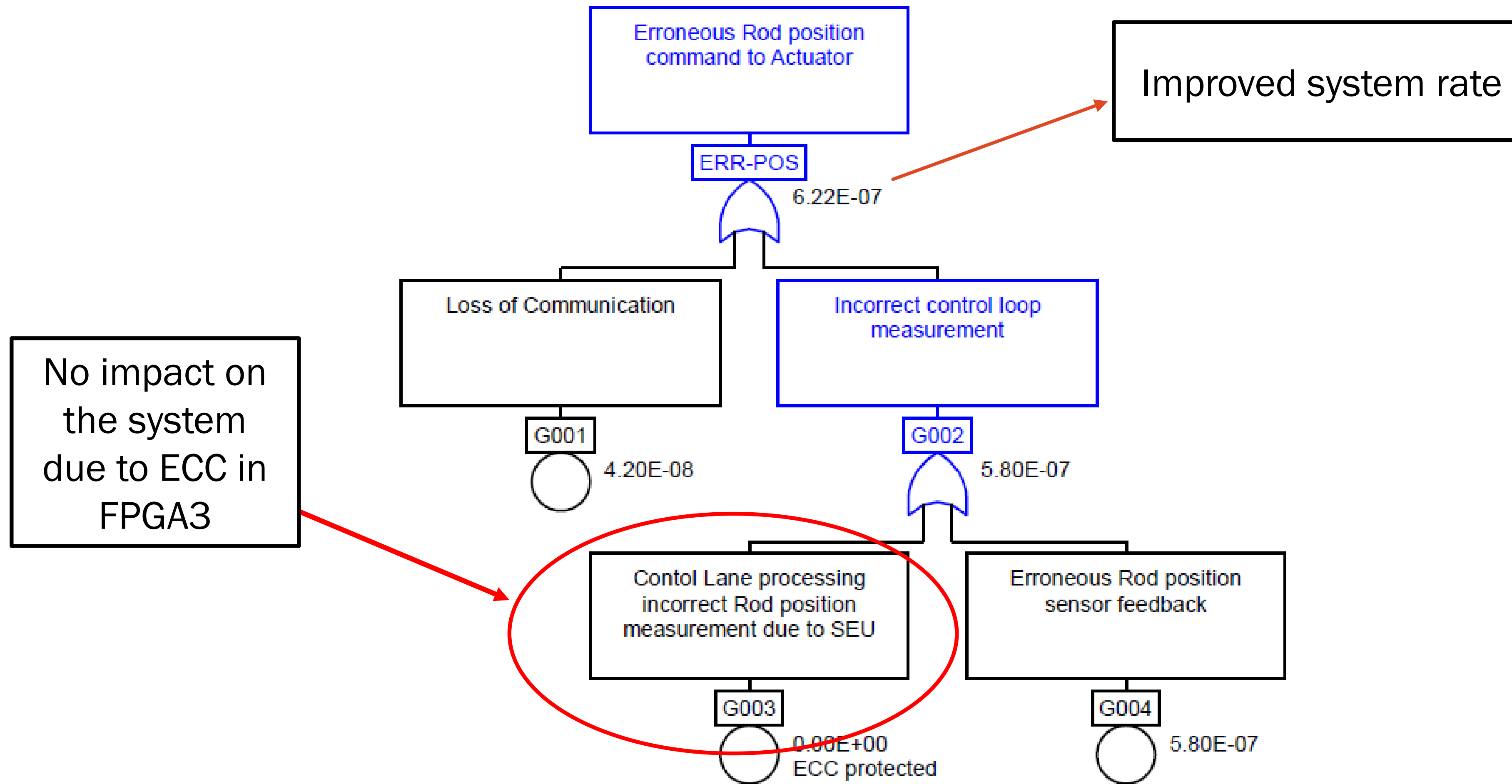
EXAMPLE: SEE IMPACT ON SYSTEM



If the design is non-compliant, redesign to be considered at system level or component level

This document does not include any export controlled technical data.

EXAMPLE: SEE IMPACT ON SYSTEM



This document does not include any export controlled technical data.

EXAMPLE: DERIVED SAFETY REQUIREMENTS

Identify the derived safety requirements from the Safety assessment if any

Example:

- The processor card shall use a Watchdog timer to monitor the health of the processor.
- The watchdog timer shall Reset the processor if the processor fails to strobe the watchdog timer within 60ms +/- 2ms
- The processor's memory controller shall be configured to correct single bit errors and detect at least double bit errors in the external SDRAM
- The processor (FPGA3) shall have ECC on the L1 Instruction cache, L1 Data cache and L2 cache

This document does not include any export controlled technical data.

MITIGATION TECHNIQUE

- The development of highly reliable and available systems requires
  - Identify the occurrence of single event effects
  - Impact they on system performance.
- SEE mitigation solutions at the chip, subsystem and system design levels can address the radiation effects issue.
- Mitigation against the impact of SEE, on a device, within a system or piece of equipment could be addressed
  - Architectural system design (e.g. dual systems, dual channels, error detection and correction, etc.)
  - Equipment design and/or electronic device selection.
- These architectural or design features, and any supporting assumptions, should be documented in a PSSA, SSA, or similar document (e.g. Safety Analysis Report) following standard practices.

This document does not include any export controlled technical data.

SEE SYSTEM-LEVEL MITIGATION

Various Mitigation techniques:

- Reasonableness testing
- Filters
- Exposure window
- Data range-checking
- Continuous monitoring and exception handling

Additional options

- Redundancy
- Watchdog supervisory logic
- Error correction
- Partitioning

Cover impacts on system integrity (comparison with two pieces of equipment) and availability (vote with at least three pieces of equipment)

System level mitigation techniques can be utilized to reduce the impact of these errors to the overall system performance.

System Redesign:

- Refers to additional mitigation means not built-in at lower levels (the mitigations at equipment level are addressed in the equipment-level redesign).
- Primarily architecture-based or based on redundancy if the penalties are acceptable
- External protection, or containment for destructive SEEs.

This document does not include any export controlled technical data.

SEE EQUIPMENT-HARDWARE MITIGATION

- Mitigation techniques for microprocessors:
  - Parity checking
  - Refreshing cache
  - Implementing a dual processor configuration
  - ECC
- All of these solutions require additional logic & have significant impacts on performance.

Note: When selecting a microprocessor, verify upset protection of internal registers and cache memory functionality.

This document does not include any export controlled technical data.

SEE EQUIPMENT-HARDWARE MITIGATION

Examples of on-chip mitigation techniques for FPGA design include:

- Triple modular Redundancy
- Scrubbing
- Selective Modular redundancy
- Soft error resilient flip-flop design
- EDAC - Incorporating EDAC into the device design is the most common solution for dealing with SEUs in memory devices.

Additional, more complex solutions include:

- Hamming codes
- Double or triple redundancy
- Interleaving - the bits in each word comprising cell addresses are physically separate or interleaved on memory device

This document does not include any export controlled technical data.

SEE EQUIPMENT-HARDWARE MITIGATION

Other Common Mitigation:

- ❑ Parity checks, cyclic redundancy checks on memory to protect integrity of critical data: allow detection of SEU, reset 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 interleaving: arrangement of bits of memory to ensure that all MBU produce only "logical" SEU

This document does not include any export controlled technical data.

SOFTWARE SOLUTIONS

- ❑ Instruction Monitoring and Resets
- ❑ SEE Event Recording (enables targeting of future mitigation)
- ❑ Periodic refreshing of component registers/configuration – Limits exposure to SEE to refresh rate
  - – Configuration, Control, and Status Register (CCSR) Space
  - – May be Partial Mitigation through Periodic Refreshing of Static Register Values
- ❑ Data Transmit/Receive – Integrity checks (CRC's, Checksums)
- ❑ Storing triple versions of critical values for voting
- ❑ Minimizing the use of vulnerable variables (such as pointers) where bit flips are unacceptable

This document does not include any export controlled technical data.

SOFTWARE SOLUTIONS

- ❑ Perform a register analysis – Determine the intended state of all bits
  - Determine impact if the bit were to be in the incorrect state
  - Determine the amount of time the incorrect state could be tolerated safely
  - Implement mitigation for any cases where bit flips are unacceptable
- ❑ Periodic checksum calculations for critical memory
- ❑ Repeat calculations
- ❑ Define constants in ROM rather than RAM
- ❑ Minimize stack and heap usage

This document does not include any export controlled technical data.

- 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, HAZ or MAJ FCs.

- 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 selection and effectiveness of mitigation techniques are dependent on the type of SEE to be mitigated and the function of the component to be protected.

CONCLUSION

This document does not include any export controlled technical data.

REFERENCE

- IEC Technical specification IEC TS 62396 part 1– Process management for avionics-Atmospheric radiation effects - Standard for the accommodation of Atmospheric Radiation Effects via Single Event Effects within Avionics Electronic Equipment," International Electrotechnical Commission, 2006
- SAE, ARP4761, "Guidelines and Methods for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment," December 1996
- SAE, ARP4754A, "Guidelines for Development of Civil Aircraft and Systems," December 2010
- EASA CM No.: CM-AS-004 Issue 01
- DOT/FAA/TC-15/62 - Single Event Effects Mitigation Techniques Report
- https://www.google.com/url?sa=i&url=https%3A%2F%2Fcommons.wikimedia.org%2Fwiki%2FFile%3ASpace_weather_effects_ESA386787.jpg&psig=AOvVaw2sqKBgAEz51QLJIGjdNp44&ust=1641907802700000&source=images&cd=vfe&ved=2ahUKEwistfirpaf1AhUSzqwKHTW2AbUQr4kDegQIARBF

This document does not include any export controlled technical data.

Manju Maheve
Principal Safety Engineer, Collins Aerospace
Email: manju.maheve3@collins.com

This document does not include any export controlled technical data.

Q&A