

GE

smiths

Aviation

(formerly Smiths Aerospace)

SPAESRANE - SEEDER SEMINAR

Bristol, 9th May 2007

System Mitigation Techniques

Presentation by: Roger Bargh



Introduction

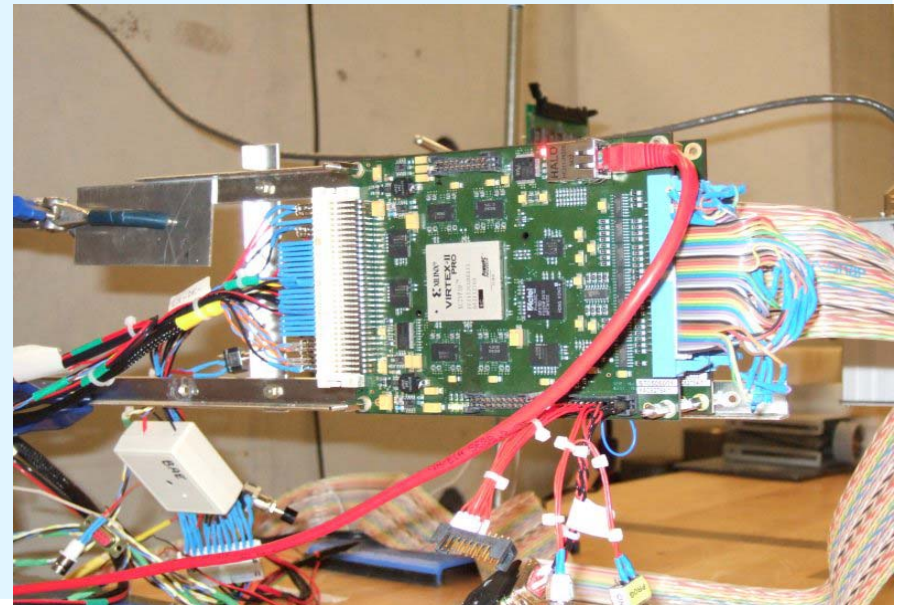
smiths



Project SPAESRANE

- Solutions for the Preservation of Aerospace Electronic Systems Reliability in the Atmospheric Neutron Environment.
- Part DTI funded project.
- Consortium - MBDA, BAe Systems, Smiths, Goodrich, UCLAS, Lancaster University, Surrey Space Centre, Qinetiq.
- Website: www.spaesrane.com

- **Memory, FPGA & Microprocessor Testing**
- **System SEE Tolerance Techniques**
- Neutron testing into performance of an existing Standby Flight Display Unit at LANSCE
- H/W and example system (SEEM1) developed as a platform to investigate SEE mitigation techniques
- Neutron testing of SEEM1 at TSL, LANSCE, ISIS



SEU - Single Event Upset (a bit flip).

- all digital electronics (registers, memory)

MBU - Multiple Bit Upset (multiple bit flips from one event).

- as SEU

SEFI - Single Event Functional Interrupt (incorrect operational mode) .

- devices with state machines (processors, programmable logic, EPROM)

SET - Single Event Transient (signal glitch, spurious clocking).

- combinatorial logic, op amps

SEL - Single Event Latchup (parasitic circuits - leaves large current path).

- CMOS devices

SHE - Single Hard Error (persistent change - a stuck bit).

- all digital electronics (registers, memory)

SEB - Single Event Burnout (transient current - feedback - breakdown).

- power MOSFETs, BJTs, GTO thyristors, power diodes, IGBTs

SEGR - Single Event Gate Rupture (dielectric breakdown).

- power MOSFETs

TID - Total Ionizing Dose (cumulative, gradual device degradation).

- all devices to some extent

Displacement Damage (atom displacement - gain degradation, current leakage).

- bipolar, optocouplers, photodiodes

Single Event Effects are caused predominantly by neutrons.

High energy neutrons > 10MeV.

Thermal neutrons < 1eV.

Particle flux increases with height (max @ 60,000ft).

Particle flux increases with latitude.

6000 n/cm²-hr (100 per minute) @ 40,000ft 40°Lat.

- This is a conservative estimate for “normal” conditions
- Can be 300 times higher in worst case solar flare
- Calculate device event rate by cross section (cm²) * neutron flux (n/cm²hour)

Do we need to respond to SEE?

Results of no action - SEE can have knock-on effects:

- **Glitch - operation recovers and continues**
- **Lock-up/crash - user hits reset**
- **Component or circuit damage**
- **System damage**
- **Mission failure**
- **Damage to other systems**
- **Injury/loss of life**

Of particular importance for aerospace:

- **Safety**
- **Reliability (MTBF)**

SEE Mitigation strategy will be influenced by:

- **Environment (relates to aircraft type, routes)**
- **Availability and Integrity requirements**
- **Criticality and Reliability levels**
- **System complexity**
- **System type**
 - **High state content (e.g. CPU, memory)**
 - **Cyclic fixed function**
- **Cost**

Standards

- **IEC 62396 - IEC Standard for the Accommodation of Atmospheric Radiation Effects via SEE within Avionics Electronic Equipment**
- **NATO AEP50**
- **ECSS-E-20-02**

Fault avoidance

- **Not feasible to shield against neutrons (concrete cockpit scenario!)**
- **Select hard or hardy devices. Look at:**
 - **SEE test result databases**
 - **Manufacturers claims and test data**
 - **In-house (historic) data**
 - **Estimates from similar device types (use conservative margins)**
 - **Device simulation (calibration required, usually by accelerated testing)**
 - **Environment testing (probably only feasible for device manufacturers due to number of devices required)**
 - **Accelerated testing (neutron, proton, ion or laser beam)**
- **Device de-rating (reducing power, voltage)**
- **Design simple systems (reduces likelihood of SEE)**

Fault tolerance

- **Error Detection and Correction (EDAC)**
- **Architecture - circuit and system level (dual or triple mode redundant)**
- **Temporal redundancy (recalculation)**
- **Robust design techniques**
 - **Remove/detect invalid states**
 - **Recalculation of state**
 - **Recovery mechanisms**
- **Monitoring and reset**
 - **Built In Test**
 - **Abnormal current, temperature**
 - **Incorrect data**
 - **Data loops**
 - **Test data / calculation**

Error correction (Hamming) codes useful in:

- Memory (DRAM, SRAM, possibly ROM)
- Cache (although parity with replace from memory can be used)
- Registers
- Data communication paths
- State machines

Scrubbing may be required to avoid error accumulation.

- Depends on operational up-time and event rate

SEDED for SEUs.

DECTED for double bit MBUs.

Higher orders of MBUs require excessive amounts of memory for codes.

Reed-Solomon codes more complex but more capable where data words are long.

Config in SRAM susceptible to SEU/MBU.

- Upsets can change users logic design

Detect by readback and correct by bitstream repair or reset.

FPGA Config data contains many “don’t care bits” (so functional fail rate \leftrightarrow SEU rate).

High availability systems will also require redundancy (DMR or TMR).

TMR can be added by automated tools.

TMR uses approx. 3.2 times resources and can half the clock speed.

- (Depending on design - number of feedback paths)

New devices are embedding bitstream repair and EDAC within the device.

Keep design simple if possible - added logic can reduce reliability.

State (in FSM, registers, memory) has potential to latch errors.

Remove/protect invalid states.

- Provide a recovery path
- EDAC, Companion states
- Binary vs one-hot FSM

Consider repetitive/combinatorial methods vs state machines.

Include read back capability to allow correction.

SEB sensitivity is related to operating voltage.

- increased voltage lowers the fluence required to cause failure

400-500V MOSFETs - neutron induced SEB can occur at >300V

Lower voltage devices are less susceptible unless near max operating voltage (e.g. 200V rated can fail @ 190V op.).

p-channel MOSFETS (rather than n-channel) are immune to SEB but still suffer SEGR.

Power diodes can be more susceptible to SEB than IGBTs.

When applied voltage is >200V, use a 50% voltage de-rating to protect against SEB/SEGR.

- Higher operating voltage can be used without burnout but increased current spikes

Circuit times out on no update to protect against SEFI / SEL and reduce chance of damage to system.

Link watchdog to system reset or a safe mode.

Needs to be simple and radiation hardened.

Enable/disable by hardware switch and/or software interlock.

Pulse the watchdog from a critical task.

**Abnormal current consumption can indicate SEFI / SAL.
For device protection and recovery, link current trip to reset.
Monitor unit health (gradual current drift).**

Event and BIT errors should be logged.

Event time stamps are useful for analysis (phase of flight).

Helps understand SEE on real systems in the environment.

- **Device qualification/selection**
- **Error detection/correction codes**
- **Self checking and fail safe designs**
- **Software detection/correction (BIT)**
- **Checkpoint and rollback**
- **Redundancy and voting (DMR, TMR)**
- **Voltage, temperature and current checks/limits**
- **Radiation level detection**
- **Device derating**
- **Watchdog / Timeout**
- **Robust / simple design**