Safety Critical Applications
Rufino Olay
Microsemi Industrial Business Manager
June 26, 2012
Agenda

- Introduction to functional safety
- Different safety standards
- Design techniques
- Deployment examples
- Further resources
History of Microsemi FPGAs in safety critical applications

- Commercial Avionics
- Military Avionics
- Tactical Missiles
- Medical Equipment
- Military Ground Vehicles
- Space Systems
Increasing safety critical design focus

Market Drivers:
Industrial manufacturers upgrading products to include more electronics for higher dependability involving reliability, safety, availability, and security

- Safety-Critical Systems
  - Avionics
  - Medical
  - Industrial automation
  - Power plants
  - Railmotive
  - Gas/Oil industry
  - More...

- S-C System Characteristics:
  - Reliability
  - Availability
  - Secure operation
  - System integrity
  - Data integrity
  - System recovery
  - Maintainability

- Device selection considerations
  - Prior deployment in safety critical application
  - Length of time device has been in the market
  - Number of devices shipped over current product lifetime
  - Accessibility to reliability data
Industrial Application Examples

Other Examples from IEC website:
- Emergency shut-down systems
- Fire and gas systems
- Turbine control
- Gas burner management
- Crane automatic safe-load indicators
- Guard interlocking and emergency stopping systems for machinery
- Medical devices
- Dynamic positioning
  - Control of a ship's movement when in proximity to an offshore installation
- Railway signaling systems (including moving block train signaling)
- Variable speed motor drives used to restrict speed as a means of protection
- Remote monitoring, operation or programming of a network-enabled process plant

Images copyright of owners
Numerous Functional Safety Standards

Functional Safety Standards for Different Markets

- IEC 61508: Functional safety in industrial equipment
- DO-178B/DO-254: Functional safety in avionics
- IEC 6060: Functional safety in medical equipment
- EN 50128/9: Railway application - software for railway control & protection
- ISO 26262: Functional safety in road vehicles
All systems will have a possibility of failure in time
  • It is impossible for a system with absolute zero failure rate

Each application has a failure rate level
  • Goal is to significantly increase the time between any failures
  • Example in a US Nuclear power plant goal is failure in 110,000 years*
    – Many exceed this to 1 failure in 1M years with target of 1 failure in 10M years

Tolerable failure rates/levels vary per application
  • Depends on potential for direct or indirect physical injury

Safety Integrity Levels (SILs) are categories to quantify levels of risks

*Source: http://www.world-nuclear.org/info/inf06.html

© 2012 Microsemi Corporation.
IEC 61508: Industrial functional safety standard

- Developed by International Electrotechnical Commission (IEC)
  - Certification through TUV

- Functional safety in industrial equipment
  - Originally applied at system level but has been also applied to product & components

- Addresses Electrical, Electronic, Programmable Electronics including hardware and software

### Safety Integrity Level (SIL) - IEC 61508

<table>
<thead>
<tr>
<th>SIL Level</th>
<th>Availability</th>
<th>Probability of Failure</th>
<th>Consequence</th>
<th>Application Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>&gt;99.99%</td>
<td>1 failure in 110,000 yrs</td>
<td>Potential for fatalities in the community</td>
<td>Nuclear Power Plant Control</td>
</tr>
<tr>
<td>3</td>
<td>99.9%</td>
<td>1 failure in 11,100 yrs</td>
<td>Potential for multiple on-site fatalities</td>
<td>Hazardous area laser curtain sensors</td>
</tr>
<tr>
<td>2</td>
<td>99%</td>
<td>1 failure in 1,100 yrs</td>
<td>Potential for major on-site injuries or fatalities</td>
<td>Hazardous liquid flow meter</td>
</tr>
<tr>
<td>1</td>
<td>90%</td>
<td>1 failure in 110 yrs</td>
<td>Potential for minor on-site injuries</td>
<td>Thermal Meter</td>
</tr>
</tbody>
</table>
Safety standards for different markets

- **Medical**
  - IEC 62304: Software for medical devices
  - ISO 13849
    - IEC 62061: Safety of machines
  - EN 50271, EN 50402: Functional safety of gas warning systems

- **Process industry**
  - IEC 61511: Safety instrumented systems for the process industry sector
  - EN 50128: Railway applications - Software

- **Avionics**
  - DO-178B: Software considerations in airborne systems

- **Railway**
  - EN 50128: Railway applications - Software

- **Nuclear Power**
  - IEC 60880: Nuclear power–control technology, software aspects
  - IEC 61513

Source: TUV
Our Devices Deployed at the Highest Reliability Levels

Safety Integrity Level (SIL) - IEC 61508

<table>
<thead>
<tr>
<th>SIL Level</th>
<th>Availability</th>
<th>Probability of Failure</th>
<th>Consequence</th>
<th>Application Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>&gt;99.99%</td>
<td>1 failure in 110,000 yrs</td>
<td>Potential for fatalities in the community</td>
<td>Nuclear Power Plant Control</td>
</tr>
<tr>
<td>3</td>
<td>99.9%</td>
<td>1 failure in 11,100 yrs</td>
<td>Potential for multiple on-site fatalities</td>
<td>Hazardous area laser curtain sensors</td>
</tr>
<tr>
<td>2</td>
<td>99%</td>
<td>1 failure in 1,100 yrs</td>
<td>Potential for major on-site injuries or fatalities</td>
<td>Hazardous liquid flow meter</td>
</tr>
<tr>
<td>1</td>
<td>90%</td>
<td>1 failure in 110 yrs</td>
<td>Potential for minor on-site injuries</td>
<td>Thermal Meter</td>
</tr>
</tbody>
</table>

Microsemi FPGA Inherent Strengths

**Immunity to Firmware Errors**
- Ensures Data & System Integrity & Control
- Fully functional to 100KRad

**Fault Tolerance through Redundancy**
- Hardware redundancy through parallel, dissimilar processes
- Cortex-M3 & FPGA running in lockstep

**Extreme Temperature Operation**
- Fully operational in harshest conditions
- Up to 200°C
Neutron Induced Single Event Upset Background

- Single Event Upset issue was first discovered in 1979 by Intel and Bell Labs as failures in DRAM’s.

- In 1999 Sun Microsystems noticed errors in cache SRAM’s for mission critical servers.

- 2000’s saw an increasing concern over SEU in logic devices like FPGAs.

- Historically neutron interactions have been associated with electronics used in Aircrafts due to the high neutron flux at these altitudes.

- As more electronics is incorporated in everyday applications, likelihood of interference has increased.
Flash FPGAs immune to Single Event Upset

- As nodes shrink, the amount of charge on each node is smaller, but charge in Cosmic rays remain same thus causes a bigger “disturb”

- As nodes shrink, circuits require less charge per switch to operate

- In FLASH FPGAs when neutron or alpha particles strike Configuration Cells in:
  - Routing Matrix $\rightarrow$ No change
  - Logic Block $\rightarrow$ No change
SRAM FPGAs are effected by stray particles

- In SRAM FPGAs when neutron or alpha particles strike the CM’s in
  - Logic Block → results in a misconnected signal which in turn results in functional failure
  - Routing Matrix → results in a misrouted or missing signal

- In both cases it’s a CM upset leading to severe consequences!
  - These errors persist until detected
  - Need rebooting OR power cycling of the FPGA
# No SEU Configuration Failures in Microsemi FPGAs

<table>
<thead>
<tr>
<th>FPGA</th>
<th>Technology</th>
<th>Equivalent Functional Failure – FIT Rates per Device</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Ground-Level Applications</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Sea Level</td>
</tr>
<tr>
<td>Microsemi Antifuse FPGA</td>
<td>150nm Antifuse</td>
<td>No Failures Detected</td>
</tr>
<tr>
<td>1M-Gate</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsemi Flash FPGA</td>
<td>130nm Flash</td>
<td>No Failures Detected</td>
</tr>
<tr>
<td>1.5M-Gate</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Microsemi Upcoming Next Gen</td>
<td>65nm Flash</td>
<td>No Failures Detected</td>
</tr>
<tr>
<td>Flash FPGA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SRAM FPGA Vendor 1</td>
<td>90nm SRAM</td>
<td>320 FITs</td>
</tr>
<tr>
<td>1M-Gate</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SRAM FPGA Vendor 2</td>
<td>90nm SRAM</td>
<td>730 FITs</td>
</tr>
<tr>
<td>1M-Gate</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Neutron Testing Results: iRoC Technologies: [www.irochtech.com](http://www.irochtech.com)
Regular testing at Los Alamos National Labs neutron test facility
**Fewer Requirements for Flash Based FPGAs**

**Due to Non Volatility & SEU Immunity**

- **IEC61508 Annex E04**
  - 7.4.5.4 *Especially for application of FPGAs and PLDs in E/E/PE safety related systems the following systemic faults shall be controlled*

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Applicability to Microsemi</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss of information in Configuration RAM (RAM Based FPGAs)</td>
<td>na: SEU immune</td>
</tr>
<tr>
<td>Malfunction of erase feature (EEProm based FPGAs/PLDs)</td>
<td>na: Flash is non-volatile</td>
</tr>
<tr>
<td>Power supply drops, EMC (RAM based)</td>
<td>na: Flash is non-volatile</td>
</tr>
<tr>
<td>Incorrect initialization during power-on (RAM based)</td>
<td>na: Live at power-up</td>
</tr>
<tr>
<td>Faults in individual programming / configuration bits (all technologies)</td>
<td>Yes</td>
</tr>
<tr>
<td>Modification of coarse functionality (macro cells, FPGA &amp; CPLD)</td>
<td>Yes</td>
</tr>
<tr>
<td>Coupling between “independent” channel (temperature, supply voltage, EMC, cross-talk) if implemented on a single chip (all technologies)</td>
<td>Yes</td>
</tr>
<tr>
<td>Single point of failure (e.g. compare logic, efficient self testing even if system uses long time static data during normal operation)</td>
<td>Yes</td>
</tr>
<tr>
<td>Malfunction in design and implementation tools</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Meeting Security Requirements

From IEC 61508, Part 1, P. 8

- this standard demands that any malicious and unauthorized actions are to be examined during the hazard and risk analysis. The application scope of this analysis includes all relevant phases of the security life cycle;

- Protection against
  - Reverse engineering
  - Tampering
  - Overbuilding
  - Cloning
Microsemi Security Features

- **Secured IP**
  - FlashLock® controls access to security settings of the device
  - No bitstream communicated from external configuration device
  - Flash cells more secure against micro-probing than other FPGA technologies

- **Secured manufacturing flow**
  - AES-encrypted programming file sent to manufacturer
  - Devices pre-programmed with matching AES key sold direct to manufacturer
  - Protects against overbuilding and cloning
Redundancy Techniques

- Redundancy is mandatory for safety critical systems
  - Provides fault-tolerant systems
  - Operate properly in the event of a failure

- Dual Modular Redundancy
  - Duplicated designs work in parallel
    - The same inputs are provided to each processing element
    - Fail safe certification engine checks for consistency

- Triple Modular Redundancy
  - Three control systems
  - Error in one component can be out-voted by the other two
Diversity Concept

- What is it – “Diversity”?
  - Fundamental differences or dissimilarity between two devices
    - usually to implement the same functions
  - In case of FPGAs: Silicon (technology & architecture), Software, Hardware development tools

- Without Diversity:
  - In a system is designed with TMR or DMR redundancy,
  - if ALL FPGA’s behave similar, then if 1 type of failure causes 1 FPGA to fail,
  - then ALL the redundant (backups in case of failures) could possibly also FAIL, and the system would shut down.
  - Redundancy in this case did not keep the system running.

- With Diversity:
  - If a system is designed with redundancy, and all FPGA’s are DIVERSE, then 1 type of failure mode is DIFFERENT between 2 DIFFERENT devices
  - If 1 type of failure causes 1 FPGA to fail, the redundant FPGA behaves DIFFERENTLY.
  - The system would still RUN.
Diversity through two different Microsemi FPGA technologies

- Microsemi manufactures Antifuse & Flash FPGAs

- Antifuse technology and flash technology are completely different in terms of the manufacturing process, how the devices store the design, and how the devices are programmed with the design.

- Antifuse devices are 1-time-programmable (OTP) and the device design is stored by permanently creating a conductive path.

- Flash devices are re-programmable and the device design is stored by storing a charge on a floating gate of a flash transistor.
Evolution of Programmable Logic
Increasing Levels of Integration

1st Generation
Low Power FPGA

2nd Generation
First Mixed Signal FPGA

3rd Generation
Customizable System-On-Chip (cSoC)

Flash FPGA Fabric
- Hardware Acceleration
- Customized Pulse Width Modulation
- I/O Expansion

Programmable Analog
- Voltage & Current Monitoring
- Temperature Monitoring

Embedded ARM® Cortex-M3
- Complex Algorithms
- System Management

Flash FPGA Fabric
- Hardware Acceleration
- Customized Pulse Width Modulation
- I/O Expansion

Programmable Analog
- Voltage & Current Monitoring
- Temperature Monitoring

Flash FPGA Fabric
- Hardware Acceleration
- Customized Pulse Width Modulation
- I/O Expansion

Power Matters.
SmartFusion
Ideal platform to partition software & hardware architecture requirements

Software Platform
- System layer
- Application Layer

Hardware Platform
- Co-Processing
- Customized Drivers

Power Matters.
© 2012 Microsemi Corporation.
Safety Implementation Comparison

**Microcontrollers**
- Two core implementation
  - Redundant *Similar* Processes

- Same code / Algorithm
  - Potential duplication of code error

- Multiple different code / algorithms
  - Requires higher speed processors
  - Increases Power Consumption

**cSoC (FPGA & MCU)**
- MCU & FPGA implementation
  - Redundant *Dissimilar* Processes

- Same algorithm designed twice
  - H/W & S/W implemented on same die

- Multiple different code / algorithms
  - Build parallel processing elements
  - Lowers power consumption
Safety Critical Application Example #1

Safety Critical System Requirement
- Firm Error Immunity
- Non-Volatile & Live at Power-up

Solution
- Flight Control Actuator
  - Aircraft flaps & spoiler control
  - Trim for speed brakes and horizontal stabilizer
  - Yaw & roll trim

Deployed Example in Fusion

Flight Control Actuator Example
Safety Critical Application Example #2

Safety Critical System Requirement
- Firm Error Immunity
- Non-Volatile & Live at Power-up
- Dissimilar processing elements

Solution
- Two processing elements
  - MCU: IR Interface & laser beam surveillance
  - FPGA: Signal processing and pulse detection

Deployed Example in SmartFusion
- Laser Safety Curtain: SIL3
- Second Highest Safety Integrity Level
Quality Management Systems & Certification

- Quality management system
  - TS 16949
  - SAE / AS9100
  - QML

- Qualification and certification
  - MIL-STD-883 Class B
  - PURE:
    - European packaging Standard
    - Commercial components in rugged environments
  - QML Class Q
    - Cert for components in high reliability / military
  - AEC-Q100
    - Automotive certification for ProASIC3 devices
Resources: For more information

- **Web pages**

- **Numerous documentation**
  - White Paper
    - Basics on single event effects
    - Understanding SEE impact in avionics, networking applications (ground level apps)
    - Increasing Fault Tolerance by Using Diverse Design Programmable Logic Technologies
  - Frequently Asked Questions
    - Neutron FAQ
3rd Party Articles, Publications

- Military & Aerospace
  - Radiation Article
- Medical
  - FDA articles on radiation emitting products
- EE Times
  - Automotive
    - Cosmic Rays Damage Electronics
    - Alpha particles, DRAMs, SEU, Toyota Acceleration
  - General
    - Neutron Storm Swirls Around FPGA Reliability
    - Soft Errors become hard truth for logic
    - Space Particles hit logic chips
    - Reliability and Redundancy
- Others
  - Electronic Products: Battling Single Event Upsets in Programmable logic
  - Tech Focus Media: Gearing up for rain, new soft error tolerant circuits
  - EDN: Cosmic Radiation comes to ASIC and SOC Designs
Summary

- Flash Based FPGAs are an excellent high reliability platform

- History of deployments in Safety Critical Applications
  - Industrial & Medical
  - Avionics
  - Military
  - Space

- Dedication to Quality Systems
  - Quality management systems & certification

- Next Steps
  - Microsemi exploring IEC 61508 certification for FPGAs & dev S/W
    - Leveraging knowledge and techniques from other certifications for Industrial
  - Developing safety documentation package