CROME System
Fault Resilient Design for 28nm ZYNQ SoC based Radiation Protection Monitoring System Fulfilling Safety Integrity Level 2

Dr. Hamza BOUKABACHE, CROME Team
12/06/2019 - System-on-Chip Workshop - CERN

Daniel Perrin, Gael Ducos, Saskia Hurst, Katharina Ceesay-Seitz, Markus Widorski, Michel Pangallo, Doris Forkel-Wirth, Stefan Roesler
Why do we need a radiation instrumentation system

When Accelerators are in operation

The interaction beam-matter generates stray radiation

Spallation
Why do we need a radiation instrumentation system

**When Accelerators are in operation**

The interaction beam-matter generates stray radiation.

**When Accelerators are stopped**

The interaction beam-matter has made the matter radioactive (activation).

Areas with risks due to ionizing radiation are classified and continually monitored.

When the ambient dose rate is below the safety threshold and the survey is Ok: Accesses are re-opened.
Why do we need a radiation instrumentation system

When Accelerators are stopped
The interaction beam-matter has made the matter radioactive (activation)

Areas with risks due to ionizing radiation are classified and continually monitored

When the ambient dose rate is bellow the safety threshold and the survey is Ok: Accesses are re-opened
Radiation & Environmental Protection

- Area Radiation Monitoring
- Induced Activity Monitors
- Ventilation Monitors
- Water Monitors
- Stray Rad Monitors

Introduction
The Context
CROME System
Performances
Conclusion
**CROME (CERN Radiation Monitoring Electronics)**

- **Development of a new generation of monitoring system for Radiation Protection**

  This system provides:
  - Continuous real-time monitoring of ambient dose equivalent rates over 9 decades
  - Alarm and interlock functionality with a probability of failure down to $10^{-7}$
  - Long term permanent and reliable data logging by linking to a SCADA supervision
  - Edge computing: Powerful processing capabilities for embedded calculation
  - Versatile interface

- **Replacing ARCON system**
- **Preparing for future, RAMSES**: 10 years of operation and over 14 years design
CROME Bulk System

Radiation Monitor

Uninterruptible Power supply
In this config. 8 hours of autonomy

Ionization Chamber
Interlocks
Alarm Bus
Alarm Unit
Access System / Machines
Worker
supervision

Introduction
The Context
CROME System
Performances
Conclusion

12/06/2019
SoC Workshop
CROME Buck System

Radiation Monitor

High Reliability components – Military, Automotive or Industrial qualification
CROME Buck System

CROME SoM

High Reliability components – Military, Automotive or Industrial qualification

CROME System

Introduction

The Context

CROME System

Performances

Conclusion

12/06/2019

SoC Workshop
Instantaneous dose rate
Environmental conditions
Avg Dose rate
Integrated dose 1
Integrated dose 2
Min Max Values ....

CUPS
Uninterruptible
Power supply

Interlock signal 1
Interlock signal 2

Access status
Beam Status
Zone Status
Interlocking system
SIL2 Smart Interlock

CROME Junction box
Introduction

The Context

CROME System

Performances

Conclusion

Front view

- Redundant power supply
- Redundant rooting matrix (CPLD)

Rear view

- SoM

CROME Junction box

- Interlocking system
- Access system

- Access status
- Beam Status
- Zone Status
- Interlock signal 1
- Interlock signal 2

SIL2 Smart Interlock

CJB

SoM

Introduction

The Context

CROME System

Performances

Conclusion

12/06/2019

SoC Workshop
Introduction

The Context

CROME System

Performances

Conclusion

CROME Rackable System

PS Facility

Air filled ionization chamber

Electron Unit

Supervision

High Radiation Area

Low Radiation Area

Alarm units

SPA6 cable
CROME Rackable System

- Rackable Modules
- Ethernet
- USB

SoM

Front End

Carrier Board

Interface Board

High rel components
Same Architecture shown previously

Powered either by the backplane or by the CUPS rack directly
CROME Products
CROME System Reliability
Safety Integrity Level Verification according to IEC 61508
CROME System Reliability
SIL Verification according to IEC 61508

• How to meet the requirements (Reliability, Life cycle, Performance … )
• How to master the complexity

Performance
• 9 decade of dynamic range
• Measurement down to $10^{-15}$ A
• Autonomous embedded system

Reliability
• Failure rate probability for measurement $< 10^{-7}$
• Failure rate probability of interlock triggering $< 10^{-6}$
• Failure rate probability of alarm triggering $< 10^{-6}$

Modularity
Totally reconfigurable
Scalable, maintainable and versatile

Scalability
• >200 calculation parameters per device
• 38,000,000,000 decision combinations per device (without CJB)

Prototype A

1- Systematic Safety Integrity (Process Quality Assurance)
CROME System Reliability
SIL Verification according to IEC 61508

2- Hardware Safety Integrity

System analysis  Functional analysis  MTTF calculation
FMEA  FTA

Probability of Dangerous Failure per Hour

\[ PFH = 8.24 \cdot 10^{-8} fpmh \]

<table>
<thead>
<tr>
<th>SIL</th>
<th>High demand/Continuous demand mode: Probability of dangerous failure per hour (PFH)</th>
<th>Risk reduction factor (RRF)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>( \geq 10^{-6} ) to (&lt;10^{-5})</td>
<td>100.000 - 1.000.000</td>
</tr>
<tr>
<td>2</td>
<td>( \geq 10^{-7} ) to (&lt;10^{-6})</td>
<td>1.000.000 - 10.000.000</td>
</tr>
<tr>
<td>3</td>
<td>( \geq 10^{-8} ) to (&lt;10^{-7})</td>
<td>10.000.000 - 100.000.000</td>
</tr>
<tr>
<td>4</td>
<td>( \geq 10^{-9} ) to (&lt;10^{-8})</td>
<td>100.000.000 - 1.000.000.000</td>
</tr>
</tbody>
</table>

Spurious Trip Rate (Availability)

The probability of a spurious trip after 10 years is 34%, after 50 years 87.5%.

Unexpected interlock/wrong interlock

- Unavailability: \( 7.66 \cdot 10^{-5} \)
- Frequency: \( 4.74576 \) fpmh
- CFI: \( 4.74612 \) fpmh
- Number expected failures: 4.15728
- Unreliability: 0.984355
- MTTF: 0.210626 Mhrs

*CFI: Conditional Failure Intensity
CROME System Reliability
SIL Firmware Verification according to IEC 61508

At CERN:

- No internal standards for verification of safety-critical FPGAs
- Universal Verification Methodology (UVM) used for non-safety-related designs
- Formal specification & directed tests for PLCs

Safety Standards and Methodologies:

- Standards “recommend” architecture based approach for FPGAs:
  - TMR, Isolation, ECC RAM, Fail safe FSM, Hamming 3

- Methods for Verification and Validation of Safety are vague:
  - Random simulation: not required by safety standards [But15, ESC10]
    - Discovers more faults than directed tests [next]

Development of an automated verification software framework:

- Reusable on system-level
- Flexible and extendible
CROME System Reliability
SIL Firmware (Prototype A) Architectural Constraint

Introduction

The Context

CROME System

Performances

Conclusion

Performances

CROME System

Reliability

SIL Firmware (Prototype A) Architectural Constraint

∫

HV Generator 0 to -2000V DC

Pulse counter

1Msps

DAC

ADC

PWRs

cBIT

1fA to 5uA

Detect

>1fA to 5uA

12/06/2019

Joel Gerber, CERN THESIS, EPFL

IEEE 754-2008 compliant – Verified using OSVVM

*
CROME System Reliability
SIL Firmware Verification according to IEC 61508

Introduction
The Context
CROME System
Performances
Conclusion

UVM Verification

<table>
<thead>
<tr>
<th>Cause</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Faults in DUV implementation</td>
<td>9</td>
</tr>
<tr>
<td>- Alarm output rose only for one clock cycle.</td>
<td></td>
</tr>
<tr>
<td>- Alarm switched unexpectedly.</td>
<td></td>
</tr>
<tr>
<td>- Rounding was wrong for negative offset values.</td>
<td></td>
</tr>
<tr>
<td>Unspecified or ambiguous requirements</td>
<td>3</td>
</tr>
<tr>
<td>Unspecified design decisions</td>
<td>2</td>
</tr>
<tr>
<td>Faults in reference model</td>
<td>2</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>15</strong></td>
</tr>
</tbody>
</table>

Table: Functional Coverage of the Integration Block

<table>
<thead>
<tr>
<th>Cover type</th>
<th>Covered</th>
<th>Number of test runs needed(^{1})</th>
<th>Number of stimuli applied(^{1})</th>
<th>Time needed (CPU time)(^{1})</th>
</tr>
</thead>
<tbody>
<tr>
<td>52 cover properties</td>
<td>100.00%</td>
<td>6</td>
<td>16355</td>
<td>5.72h</td>
</tr>
<tr>
<td>cglIntConditions</td>
<td>100.00%</td>
<td>19</td>
<td>324647</td>
<td>39.00h</td>
</tr>
<tr>
<td>cglIntRegression</td>
<td>100.00%</td>
<td>1</td>
<td>250</td>
<td>13.79min</td>
</tr>
<tr>
<td>cglIntValueRanges</td>
<td>91.95%</td>
<td>18</td>
<td>249327</td>
<td>37.23h</td>
</tr>
<tr>
<td>cglIntRobustness</td>
<td>7.15%</td>
<td>6</td>
<td>280977</td>
<td>28.94h</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>79.82%</strong></td>
<td><strong>21</strong></td>
<td><strong>454200</strong></td>
<td><strong>39.89h</strong></td>
</tr>
</tbody>
</table>

\(^{1}\) to reach the listed coverage with constrained input stimuli.
**CROME System Reliability**

**SIL Firmware (Prototype Q) – PL Architectural Constraint**

### Configuration Memory

Protected by Soft Error Mitigation Core (SEM IP):

- **Repair** – Corrects single bit errors with ECC
  (100MHz: boot time 110ms, 8ms max time for detection, 610μs correction time)
- **Enhanced Repair** – Corrects single or double bit errors using ECC and CRC
  (100MHz: boot time 110ms, 8ms max time for detection, 18ms correction time)
- **Replace** – Uses external flash to replace corrupted bits
  (100MHz, 8ms max time for detection, 830μs correction time)

### Block Memories

BRAMs have built-in ECC protection.

- Each 32-bit write is appended with 8 protection bits
- On read operation the protection bits correct single bit errors and detect double bit errors

Configuration from the PS is analysed and validated by a checksum

### Flip Flops

Control functionality is triplicated and outputs are voted on.
CROME System Reliability

SIL Firmware (Prototype Q) – PS Architectural Constraint

- CROMiX 18 (Kernel 4.14.0) - SMP
  (Petalinux Yocto framework Based)

- PL <-> PS BRAMs are managed using UIO device driver instead of /dev/mem
  driver:
  √ IRQ handling
  √ No Kernel code at all
  √ UIO Driver errors usually not fatal

&amba {
  uio.SendMessage: uio.SendMessage {
    compatible = "generic-uio";
    reg = <0xF8007000 0x1000 0x40002000 0x1000 0x40003000 0x1000>;
    interrupts = <0 57 0>;
    interrupt-parent = <&intc>;
  };
}

/* PL2PS */
REG_RESULTS: REG_RESULTS@40001000
{
  compatible = "generic-uio";
  reg = <0xF8001000 0x1000>;
  interrupts = <0 29 1>;
  interrupt-parent = <&intc>;
}

/* PS2PL */
Bram_DOWNSTREAM: Bram_DOWNSTREAM@40000000
{
  compatible = "generic-uio";
  reg = <0xF8000000 0x1000 0xF8002000 0x1000 0xF8003000 0x1000>;
  /* CONFIGURATION_BRAM DBG_REG RESETS+TIME_REG */
  interrupts = <0 30 1>;
  interrupt-parent = <&intc>;
}
CROME System Reliability
SIL Firmware (Prototype Q) – Architectural Constraint

- CROMiX 18 (Kernel 4.14.0) - SMP
  (Petalinux Yocto framework Based)

- PL <-> PS BRAMs are managed using UIO device driver instead of /dev/mem driver:
  ✓ IRQ handling
  ✓ No Kernel code at all
  ✓ UIO Driver errors usually not fatal

- User App : 3 processes

- Downstream data from : Supervision - > PS -> PL is end to end “protected” by an ECC and a checksum. Data is evaluated every 100ms

&amba {
  amba_pl: amba_pl {
    #address-cells = <1>;
    #size-cells = <1>;
    compatible = "simple-bus";
    ranges ;
    /delete-node/ axi_bram_ctrl@40000000;
    /delete-node/ axi_bram_ctrl@40001000;
    /delete-node/ axi_bram_ctrl@40002000;
    /delete-node/ axi_bram_ctrl@40003000;
  }
}

/* PL2PS */
REG_RESULTS: REG_RESULTS@40001000
{
  compatible = "generic-ui0";
  reg = <0x40001000 0x1000>;
  interrupts = < 0 29 1 >;
  interrupt-parent = <&intc>;
};
CROME System Reliability
SIL Firmware – BOOT Sequence & Automatic Recovery - Architectural Constraint

The Boot sequence and the automatic recovery in case of undefined behavior are both managed by an auxiliary CPLD connected to the PL and to PS.
CROME System Reliability
SIL Verification according to IEC 61508

1- Systematic Safety Integrity (Process Quality Assurance)

2- Hardware Safety Integrity

Probability of Dangerous Failure per Hour

\[ PFH = 8.24 \cdot 10^{-8} \text{ fpmh} \]

<table>
<thead>
<tr>
<th>SIL</th>
<th>High demand/Continuous demand mode: Probability of dangerous failure per hour (PFH)</th>
<th>Risk reduction factor (RRF)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>( \geq 10^{-6} \text{ to } &lt;10^{-5} )</td>
<td>100.000 - 1.000.000</td>
</tr>
<tr>
<td>2</td>
<td>( \geq 10^{-7} \text{ to } &lt;10^{-6} )</td>
<td>1.000.000 - 10.000.000</td>
</tr>
<tr>
<td>3</td>
<td>( \geq 10^{-8} \text{ to } &lt;10^{-7} )</td>
<td>10.000.000 - 100.000.000</td>
</tr>
<tr>
<td>4</td>
<td>( \geq 10^{-9} \text{ to } &lt;10^{-8} )</td>
<td>100.000.000 - 1.000.000.000</td>
</tr>
</tbody>
</table>

3- Software Safety Integrity – On going
CROME System Reliability
SIL Firmware Verification according to IEC 61508: Faults injection

There are two methods and metrics for the evaluation of APSoCs faults tolerance:

**Accelerated radiation tests**

- Mixed field

**Fault injection by emulation**

- Concerns only the PL
- Will not be presented here
CROME System Reliability
SIL Firmware Verification according to IEC 61508 : Faults injection

Introduction

The Context

CROME System

Performances

Conclusion

Accelerated radiation tests

What do we know :

- SEU, SDC and SEFI cross-sections of both Zynq PL and PS memories, registers and buses characterized [1][2] under various configurations

- ZYNQ PS has «relatively» higher SEFI cross section in neutrons compared to other processors (>2 order of magnitude compared to Hercules) [3]

- Compared to bare metal, the use of Linux OS barely affects the SDC rate but it greatly increases the SEFI rate (up to 748%) [4]

- The PS has access through the PCAP to the FPGA configuration primitive

What we don't know :

- Does OS (PS, AXI … ) crashes influence the PL (safety critical part) functionalities ?

References:
[2] On the Characterization of Embedded Memories of Zynq-7000 All Programmable SoC under SEU Induced by Heavy Ions and Protons, RADECS 2015
CROME System Reliability
SIL Firmware Verification according to IEC 61508: Faults injection

Introduction

The Context

CROME System

Performances

Conclusion

Test Setup

Mixed field

Radiation Safe Area

Tests at CHARM

The HEH fluence normalised per day inside the test area at beam height (1.5E15 protons per day)

CHARM dose rate distribution with copper target and no shielding

- Upset Position
- Upset Essential Yes/No?
- Double upsets
- Upset Corrected?
- Time

Serial Link Alive/Dead?

PS Alive/Dead?

PL internal status
- PS Heart Bit
- TMR
- BRAM 1 to 3 upsets or double upsets
CROME System Reliability
SIL Firmware Verification according to IEC 61508

Preliminary Results

Continuous Test Run with Automatic PS Restart

- Start: 23/08/2018
- End: 19/09/2018
- Duration: 26 Days, 16.5 Hours

<table>
<thead>
<tr>
<th>Resource</th>
<th>Estimation</th>
<th>Available</th>
<th>Utilization %</th>
</tr>
</thead>
<tbody>
<tr>
<td>LUT</td>
<td>40450</td>
<td>52000</td>
<td>76.03</td>
</tr>
<tr>
<td>LUTRAM</td>
<td>1075</td>
<td>17400</td>
<td>6.18</td>
</tr>
<tr>
<td>FS</td>
<td>3560</td>
<td>10640</td>
<td>33.79</td>
</tr>
<tr>
<td>DSP</td>
<td>121</td>
<td>220</td>
<td>55.00</td>
</tr>
<tr>
<td>IO</td>
<td>79</td>
<td>125</td>
<td>63.20</td>
</tr>
</tbody>
</table>

- Number of Corrected Upsets in CRAM: 1846
- Number of essential upsets in CRAM: 240
- Percentage of non-correctable upsets in the CRAM: 0.8%
- Number of PS crashes: 2344
- Number of PL Deaths – Non defined behaviour: 20

Tests at CHARM

- Proven PL 117 times more reliable than the PS, validating our general architecture
- Proven that PS crashes do not influence the PL
- Validated the architecture of the auto-reboot recovery sys.
Conclusion
Conclusion

- CROME HW has entirely been studied, tested and verified (not subject of this presentation)

- Measurement performances have been validated in operational conditions (not subject of this presentation)

- Serie production of 200 devices has been lunched at CERN

- On side infrastructure is being installed (Cabling, Network … ) at SM18, PSB, nTOF, North Area
Conclusion

- 5 Devices are currently in operation at CERN for more than 1 year
- 2 Devices are currently used at ESS (European Spallation Source)

- CROME FW consolidation and verification are still on going
  → An external company from Aerospace has been contracted to review our HDL
  → Discussion are on-going with a certification body concerning the FW assessment
- FW stability and Scalability tests are on going
- IT Security tests are foreseen