CROME
A Safety and Reliability Perspective of the CERN RadiatiOn Monitoring Electronics

Hamza Boukabache, Saskia Hurst, Katharina Ceesay-Seitz

EP-ESE Seminar

(CROME Website: https://crome.web.cern.ch)
Outline

• Context and Overview of CROME (CERN RadiatiOn Monitoring Electronics)

• Hardware Safety Integrity Verification according to IEC 61508
  Of the CROME system and the CROME Junction Box (CJB)

• Functional Verification Methodology
  Compliant to and enhancing IEC 61508
Why do we need a radiation monitoring system

When Accelerators are in operation

The interaction beam-matter generates stray radiation

Spallation

Super Proton Synchrotron (450 GeV/c)

Beryllium Targets

Target Attenuators eXperiments

Stable matter

Beam

Stray radiation

The Context
Why do we need a radiation monitoring system

When Accelerators are in operation

The interaction beam-matter generates stray radiation

Accesses to the beam tunnel and to experimental areas are closed

When Accelerators are stopped

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

Areas with risks due to ionizing radiation are classified and continuously 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 monitoring system

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

When Accelerators are stopped

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

When the ambient dose rate is below the safety threshold and the survey is Ok: Accesses are re-opened
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 dangerous failure down to 10e-7 (undetectable 10e-8)
- 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: 12 years of operation and over 16 years design
The Context

CERN - Radiation & Environmental Monitoring System

864 Radiation Protection channels & 523 Environmental channels

- CROME 2021
- CROME 2028
- GRAMS 2012
- LHC
- North Area
- Bldg. 867
- SPS
- AD
- HIE-ISOLDE
- East Area
- CTF3
- LHC injectors
- TTs
- n-TOF
- LINACs
- PS

The diagram illustrates the radiation and environmental monitoring system at CERN, with specific focus areas and locations such as the LHC, North Area, SPS, AD, HIE-ISOLDE, and East Area. The system includes 864 Radiation Protection channels and 523 Environmental channels.
CERN Radiation Monitoring Electronics (CROME)

Conceptual view of CROME at CERN

- Plastic Air filled ionization chamber
- SPA6 cable
- 1000V
- 100fA

High Radiation Area
Low Radiation Area

Two configurations:
- Rackable
- Bulk

The Context
CROME System
HW Safety Integrity Verification
FW Safety Integrity Verification
Conclusion
CROME Bulk System for low radiation areas

Simplest Configuration

Uninterruptible Power supply
In this config. 8 hours of autonomy

Alarm Bus

Alarm Unit

Interlocks

Access System / Machines

Worker

supervision
CROME Bulk System for low radiation areas

Simplest Configuration

- Ionization Chamber
- Interlocks
- Alarm Bus
- Alarm Unit
- Worker
- Access System / Machines
- Uninterruptible Power supply
  - In this config. 8 hours of autonomy
CROME System: Radiation Monitor

The Context

CROME System

HW Safety Integrity Verification

FW Safety Integrity Verification

Conclusion

RACK Version

BULK Version

SoM cooling

Measurement Circuit

1fA to 2uA

High Voltage

(0 – 2000V)

Calculated failure rate of 1.10 fpmh

Sealing for IP54

Front-end Board

Analog Board

Custom SoM

SoM

CROME System: Radiation Monitor

The Context

CROME System

HW Safety Integrity Verification

FW Safety Integrity Verification

Conclusion

RACK Version

BULK Version

SoM cooling

Measurement Circuit

1fA to 2uA

High Voltage

(0 – 2000V)

Calculated failure rate of 1.10 fpmh

Sealing for IP54

Front-end Board

Analog Board

Custom SoM

SoM
CROME Bulk System: Radiation Monitor (processing board)

Zynq System on Chip

CROME System

The Context

HW Safety Integrity Verification

FW Safety Integrity Verification

Conclusion

CROME Bulk System: Radiation Monitor (processing board)
CROME Bulk System: Radiation Monitor (processing board)
CROME Bulk System: Radiation Monitor (Zynq Programmable Logic)

* IEEE 754-2008 compliant – Verified using OSVVM
Contributions to the SIL 2 Radiation Monitoring System CROME, Nicola Joel Gerber, CERN THESIS, EPFL
Fault resilient FPGA design for 28 nm ZYNQ system-on-chip based radiation monitoring system at CERN

Microelectronics Reliability Journal
CROME Bulk System: Radiation Monitor (Zynq Processing System)

System On Chip

Hardware

- Radiation Monitor
- Zynq Processing System

Software

- ROMULUSLib 6.1
- Linux Kernel
- NTP Time Synchronization

Networking

- Ethernet
- Network Communication
- REMUS Supervision

Historical Data

- Min. 5 Days
- Collection
- Search
- Deletion
CROME Bulk System: Radiation Monitor (CPLD)

Different boot media are possible: managed by CPLD

ZSBL (BOOTROM)
entry / HW Configuration
do / Load FSBL

Bootbin
- FSBL (First Stage Boot Loader)
  entry / PS Init
  do / Load P7_Init.*
- FSBL (First Stage Boot Loader)
  entry / Program PL
  do / Load Bitstream
- U-boot
  entry / image.ub
  do / Load Device Tree
  do / Load Linux Kernel Image
  do / Load Root File System Image

SD Card
- Default
- Option 2: Image not found? Bad update?
- Option 1: Image not found? Bad update?

CROME CMPU Processing Board

Possible BootMedia: SD Card, eMMC

SD Corrupted?
Linux boot timeout

Bitstream redundancy
(QSPI / SD Card / eMMC)

CPLD
Zynq PS
Zynq PL

Timer
Watchdog
State of FSM
Power Rst
Soft Rst

Safety Critical HW
CPLD
SD Card
QSPI FM
eMMC
DDR3 RAM
SPI FM

Remote Server
QSPI Flash Memory

Conclusion
Redundancy can be extended at system level

CROME System On Field

Supervision

CUPS
Uninterruptible Power supply

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

Access system
Interlocking system

Smart Interlock router

Interlock signal 1
Interlock signal 2

Access status
Beam Status
Zone Status

Hardened Field Bus
(NESS + EB6-DPFR)

Alarm Unit 1
Alarm Unit 2
Alarm Unit N

Power Supply
Loop Detection
Unlimited number of Alarms Units is supported

Radiation Monitor 1
Radiation Monitor 2

The Context

CROME System

HW Safety Integrity Verification

FW Safety Integrity Verification

Conclusion

First operational installation of CROME
CROME Detection performances

Front-end Performances Linearity
LNE – Certified Lab in Paris (France)

CROME System Under Calibration

Calculation of the Calibration Factor

The Context

CROME System

HW Safety Integrity Verification

FW Safety Integrity Verification

Conclusion
CROME (environmental monitoring)
Uncontrolled cabins

Spikes due to the rain

32 fA

3nSv/h

4.8 fA
• Context and Overview of CROME (CERN RadiatiOn Monitoring Electronics)

• Hardware Safety Integrity Verification according to IEC 61508
  Of the CROME system and the CROME Junction Box (CJB)

• Functional Verification Methodology
  Compliant to and enhancing IEC 61508
Outline

• General IEC 61508 Requirements
• Hardware Safety Integrity Verification According to IEC 61508
  • Reliability Prediction
  • Failure Modes Effects and Diagnostic Analysis
  • Fault Tree Analysis
• Results
  • Improvements / Modifications on the CROME System
  • Final Results
Safety Integrity Requirements (IEC 61508-2)

- All requirements must be met, in order to achieve a certain SIL
- Systematic safety integrity aims at avoiding systematic faults during design, installation, operation and maintenance
- Software safety integrity relates to the safety integrity achieved by having adapted restrictions for application programming methods, tools and associated procedures
- Hardware safety integrity is related to random hardware failures
IEC 61508-2 Hardware Safety Integrity

Quantitative requirements

• Give quantified evidence, that the safety instrumented function is able to meet the reliability target

<table>
<thead>
<tr>
<th>SIL</th>
<th>Continuous mode: Probability of dangerous Failure per Hour (PFH)</th>
<th>Low demand mode (≤ 1 per year): Probability of Failure on Demand (PFD)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>$\geq 10^{-6}$ to $&lt; 10^{-5}$</td>
<td>$\geq 10^{-2}$ to $&lt; 10^{-1}$</td>
</tr>
<tr>
<td>2</td>
<td>$\geq 10^{-7}$ to $&lt; 10^{-6}$</td>
<td>$\geq 10^{-3}$ to $&lt; 10^{-2}$</td>
</tr>
<tr>
<td>3</td>
<td>$\geq 10^{-8}$ to $&lt; 10^{-7}$</td>
<td>$\geq 10^{-4}$ to $&lt; 10^{-3}$</td>
</tr>
<tr>
<td>4</td>
<td>$\geq 10^{-9}$ to $&lt; 10^{-8}$</td>
<td>$\geq 10^{-5}$ to $&lt; 10^{-4}$</td>
</tr>
</tbody>
</table>

• PFD is a probability with consideration of the dangerous failure rate
• PFH is a frequency with consideration of only the dangerous undetectable failure rate
IEC 61508-2 Hardware Safety Integrity

Qualitative requirements

- Give the necessary constraints on the system architecture

<table>
<thead>
<tr>
<th>Safe Failure Fraction</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>Hardware Fault Tolerance</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;60%</td>
<td>SIL 1</td>
<td>SIL 2</td>
<td>SIL 3</td>
<td></td>
</tr>
<tr>
<td>60% - &lt;90%</td>
<td>SIL 2</td>
<td>SIL 3</td>
<td>SIL 4</td>
<td></td>
</tr>
<tr>
<td>90% - &lt;99%</td>
<td>SIL 3</td>
<td>SIL 4</td>
<td>SIL 4</td>
<td></td>
</tr>
<tr>
<td>&gt;99%</td>
<td>SIL 3</td>
<td>SIL 4</td>
<td>SIL 4</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Safe Failure Fraction</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>Hardware Fault Tolerance</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;60%</td>
<td>Not allowed</td>
<td>SIL 1</td>
<td>SIL 2</td>
<td></td>
</tr>
<tr>
<td>60% - &lt;90%</td>
<td>SIL 1</td>
<td>SIL 2</td>
<td>SIL 3</td>
<td></td>
</tr>
<tr>
<td>90% - &lt;99%</td>
<td>SIL 2</td>
<td>SIL 3</td>
<td>SIL 4</td>
<td></td>
</tr>
<tr>
<td>&gt;99%</td>
<td>SIL 3</td>
<td>SIL 4</td>
<td>SIL 4</td>
<td></td>
</tr>
</tbody>
</table>

- Type A* Components: simple components, with well known failure modes
- Type B* Components: complex components (containing software)
IEC 61508-2 Hardware Safety Integrity

Qualitative requirements

- **Hardware Fault Tolerance (HFT):**
  Represents the ability of a functional unit to continue performing a required function in the presence of faults or errors

- **Safe Failure Fraction (SFF):**
  Ratio between the sum of the safe failure rate ($\lambda_{SD}$, $\lambda_{SU}$) and the detected dangerous failure rate ($\lambda_{DD}$) over the sum of the total failure rate ($\lambda_{T}$)

$$SFF = \frac{\sum \lambda_{SD} + \sum \lambda_{SU} + \sum \lambda_{DD}}{\sum \lambda_{T}}$$
Hardware Safety Integrity Verification

- **General Approach (performed with ©Isograph)**

  1. Reliability prediction
  2. Failure modes, effects and diagnostic analysis (FMEDA)
  3. Fault tree analysis
  4. PFD/PFH calculation
  5. Architectural constraints
  6. SiL evaluation according to IEC 61508

- Total component failure rate
- Division into $\lambda_{SD}$, $\lambda_{SU}$, $\lambda_{DD}$, $\lambda_{DU}$ by the diagnostic coverage
- Calculation of the PFH by Boolean logic
- Calculation of the Safe Failure Fraction (SFF) and estimation of the Hardware Fault Tolerance (HFT)
- Comparison against the requirement tables in IEC 61508
Reliability Prediction

• Serves as basis for all further calculations
• Component failure rates (specified as Mean Time To Failure (MTTF) or Failures In Time (FIT)) are calculated by:
  • FIDES standard (2009) for standard (passive) components
  • Manufacturer data for all other (active) components
    • Calculated by JESD85 (EIA/JEDEC Standard): Methods for calculating failure rates in units of FITs used in electronic industry
    • Based on high temperature operational life (HTOL) tests
• Study contains all ~3700 components of the CROME system and junction box
Reliability Prediction

Example:

<table>
<thead>
<tr>
<th>ID</th>
<th>Category</th>
<th>Parameters</th>
<th>Phase Parameters</th>
<th>Rate/PI Factors</th>
<th>Tasks</th>
<th>Notes</th>
<th>Hyperlink</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.4.1.2</td>
<td>Switch/Relay</td>
<td>Quantity: 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Adjustment Factor:</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Switch/Relay Type:</td>
<td>Electromechanical</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Contact Type:</td>
<td>Silver</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Breaking Capacity:</td>
<td>Less than 2 Amps</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Load Type:</td>
<td>Resistor</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Protection Level:</td>
<td>Sealed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Component quality:</td>
<td>Level 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Experience factor:</td>
<td>Recognised - not analysed</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Placement:</td>
<td>Digital interface</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Temperature Rise:</td>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>No of Manoeuvres Per Hour: 0.042</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Number of Contacts:</td>
<td>8</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Number of Single Throw Poles: 0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Number of Double Throw Poles: 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Electric Stress Calc Mode: Calculated</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Voltage Stress Ratio:</td>
<td>0.4</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Operating Voltage (V):</td>
<td>24</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Failure Rate [fpmh]</th>
<th>MTTF [mh]</th>
<th>N x Failure Rate [fpmh]</th>
</tr>
</thead>
<tbody>
<tr>
<td>PI_LPHY</td>
<td>1.48999</td>
<td>83.376</td>
<td>1.199e-2</td>
</tr>
<tr>
<td>PI_PM</td>
<td>2.01375</td>
<td>3.735e-2</td>
<td>1.199e-2</td>
</tr>
<tr>
<td>PI_HMPRO</td>
<td>4.00000</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Conclusion

09/02/2021

H. Boukabache, S. Hurst, K. Ceesay-Seitz – A safety and reliability perspective of the CERN Radiation Monitoring Electronics (CROME)
Failure Modes, Effects and Diagnostic Analysis

• Implementation of:
  • All component failure modes and failure mode probabilities (Military Handbook 338B, IEC 62380)
  • Immediate failure effects and end effects on system level and
  • Their diagnostic coverage / detectability

<table>
<thead>
<tr>
<th>Device type</th>
<th>Failure mode</th>
<th>Mode probability (α)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Capacitor, Ceramic</td>
<td>Short</td>
<td>0.49</td>
</tr>
<tr>
<td></td>
<td>Change in value</td>
<td>0.29</td>
</tr>
<tr>
<td></td>
<td>Open</td>
<td>0.22</td>
</tr>
</tbody>
</table>

• Division of the total component failure rate $\lambda_T$ into its safe detectable $\lambda_{SD}$, safe undetectable $\lambda_{SU}$, dangerous detectable $\lambda_{DD}$ and dangerous undetectable $\lambda_{DU}$ failure rate
### The Context

CROME System

HW Safety Integrity Verification

FW Safety Integrity Verification

Conclusion

## FMEDA

### Example:

<table>
<thead>
<tr>
<th>ID</th>
<th>Description</th>
<th>Failure modes</th>
<th>Higher effect</th>
<th>End effect</th>
<th>Dangerous failure %</th>
<th>Dangerous coverage %</th>
<th>Safe coverage %</th>
<th>Detected safe failure rate</th>
<th>Undetected safe failure rate</th>
<th>Detected dangerous failure rate</th>
<th>Undetected dangerous failure rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1.2.3.18.5</td>
<td>Resistor Thin Film Chip ±0.1% 0.1W ±10ppm</td>
<td>(CC) R91 - open</td>
<td>No -12VA</td>
<td>Unexpected interlock</td>
<td>0</td>
<td>0</td>
<td>100</td>
<td>0.0049059</td>
<td>2728255243</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(CC) R91 - parameter change</td>
<td>No -12VA</td>
<td>Unexpected interlock</td>
<td>0</td>
<td>0</td>
<td>100</td>
<td>0.0029834</td>
<td>4715545572</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>(CC) R91 - short</td>
<td>No effect CB</td>
<td>No effect CROME</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4.15756549</td>
<td>30885E-05</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2.1.2.3.18.6</td>
<td>Zener Diode Jumper 2A (200V DC max 7V)</td>
<td>(CC) R62 - short</td>
<td>No effect CB</td>
<td>No effect CROME</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>5.083217</td>
<td>9217E-06</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Fault Tree Analysis

- Based on the structure of the FMEDA and the functional analysis
- **Aim:** Calculate the PFD/PFH of the safety integrated function by Boolean logic
- **Assumption:** Exponential lifetime distribution for all electronic components (failure rate $\lambda = \text{const. over lifetime}$)
- System unavailability:

  $$PFD = \lambda_{DU} \cdot \frac{\tau}{2} \cdot \frac{PTC}{100} + \lambda_{DU} \cdot \frac{\sigma}{2} \cdot \left(1 - \frac{PTC}{100}\right) + \lambda_{DD} \cdot MTTR$$

- PFH is the mean over the unconditional failure intensity
- Failure frequency (unconditional failure intensity):

  $$PFH = \lambda_{DU} \cdot (1 - Q)$$
Fault Tree Analysis

Example:

Top gates:
Safety-critical end-effect on system level, contains overall PFH/PFD

Inter-gates:
Safety-critical failure effects on subsystem / board level, contains possible redundancies / voting channels

Events:
Component failure mode as entry, contains $\lambda_{SD}, \lambda_{SU}, \lambda_{DD}, \lambda_{DU}, \sigma, \tau$ and PTC
Architectural Constraints

Determination of architectural constraints by a four-step procedure:

1. Assessment and classification of the subsystem components
   • With respect to their complexity (Type A / Type B)

2. Calculation of the Safe Failure Fraction (SFF) of each component

3. Determination of the achievable SIL of the subsystem
   • Determination of the Hardware Fault Tolerance (HFT) by considering voting channels and redundancies in
     the subsystem architecture

4. Determination of the achievable SIL of the SIF
   • By using merging rules and considering the architecture of the system (subsystems installed in series or in
     parallel)
Results for the CROME system

- Iterative procedure from the second prototype A.2 to the last prototype Q
- Several modifications have been made on all boards, for example:
  - **On component level**
    - change of components to higher quality, e.g. capacitors to automotive grade
    - changing components to alternatives, e.g. hard-wired slide switch to reduce failure rate
  - **On board level**
    - adding redundancies on critical functions, e.g. additional power supply, interlock output/input signal
    - adding monitoring circuits to detect additional failures
    - adding a coprocessor as a redundancy to the FPGA on the Processing board
  - **Mechanical improvements**
    - heat sink on the Processing board, implementation of IP54 by complete sealing of the chassis

H. Boukabache, S. Hurst, K. Ceesay-Seitz – A safety and reliability perspective of the CERN Radiation Monitoring Electronics (CROME)
Final results

- **CROME system - Prototype Q (basic configuration)**
  - Probability of dangerous failure per hour: \( PFH = 9.28 \cdot 10^{-08} \ [fpmh] \)  
  - Architectural constraints (whole system):

  - **SIL 2 requirements are fulfilled**

- **CROME Junction Box (CJB) - simplified schematics (one device)**
  - Probability of dangerous failure per hour: \( PFH = 9.74 \cdot 10^{-09} \ [fpmh] \)  
  - Architectural constraints (whole system):

  - **SIL 2 requirements are fulfilled**

<table>
<thead>
<tr>
<th>SFF</th>
<th>HFT</th>
<th>SIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>97.4%</td>
<td>0</td>
<td>min SIL 2 compliant</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SFF</th>
<th>HFT</th>
<th>SIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>97.3%</td>
<td>0</td>
<td>min SIL 2 compliant</td>
</tr>
</tbody>
</table>
• Context and Overview of CROME (CERN RadiatiOn Monitoring Electronics)

• Hardware Safety Integrity Verification according to IEC 61508
  Of the CROME system and the CROME Junction Box (CJB)

• Functional Verification Methodology
  Compliant to and enhancing IEC 61508
Functional Verification of CROME

• Safety-critical FPGA:
  • Verification according to IEC 61508
    (Standard for Functional Safety of Programmable Electronics)

• Verification of functionality → find systematic faults

• Goal: Find corner case faults
  • Hard to find with directed testing
  • Could be a risk for safety
Outline

• Functional Verification Methodology
  • for highly parametrizable FPGA designs
  • compliant to and enhancing IEC 61508
• Constrained-random simulation
  • with Universal Verification Methodology (UVM)
• Formal Property Verification
• Summary
## Compliance and additions to IEC 61508 requirements for ASIC/FPGA

<table>
<thead>
<tr>
<th>Phase</th>
<th>Method</th>
<th>SIL 1</th>
<th>SIL 2</th>
<th>SIL 3</th>
<th>SIL 4</th>
<th>Chosen Technique</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verification planning</td>
<td>Semi-formal methods</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>Natural Language Properties (NLPs)</td>
</tr>
<tr>
<td></td>
<td>Requirements traceability</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>Tool based or manual</td>
</tr>
<tr>
<td>Verification of the system design</td>
<td>Inspection of specification</td>
<td>A</td>
<td>HR</td>
<td>HR</td>
<td>HR</td>
<td>Review</td>
</tr>
<tr>
<td></td>
<td>Semi-formal methods</td>
<td>R</td>
<td>R</td>
<td>HR</td>
<td>HR</td>
<td>Natural Language Properties (NLPs)</td>
</tr>
<tr>
<td>Verification of results documentation</td>
<td>Requirements traceability</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>Tool based or manual</td>
</tr>
<tr>
<td></td>
<td>Repeatability</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>A</td>
<td>Version control system &amp; automation</td>
</tr>
</tbody>
</table>

A: Addition  
R: Recommended  
HR: Highly Recommended
## Compliance and additions to IEC 61508 requirements for ASIC/FPGA

<table>
<thead>
<tr>
<th>Phase</th>
<th>Method</th>
<th>SIL 1</th>
<th>SIL 2</th>
<th>SIL 3</th>
<th>SIL 4</th>
<th>Chosen Technique</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verification of the system design and development</td>
<td>Simulation</td>
<td>A</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>Mixed-language simulation</td>
</tr>
<tr>
<td></td>
<td>Formal methods</td>
<td>A</td>
<td>A</td>
<td>R</td>
<td>R</td>
<td>Formal Property Verification</td>
</tr>
<tr>
<td></td>
<td>Functional testing on module level</td>
<td>HR</td>
<td>HR</td>
<td>HR</td>
<td>HR</td>
<td>Constrained-random simulation with functional coverage and reference model / coverage of NLPs</td>
</tr>
<tr>
<td></td>
<td>Expanded functional testing</td>
<td>A</td>
<td>HR</td>
<td>HR</td>
<td>HR</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Coverage of the verification scenarios</td>
<td>R</td>
<td>R</td>
<td>HR</td>
<td>HR</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Black-box testing</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>Independence</td>
</tr>
</tbody>
</table>

A: Addition  
R: Recommended  
HR: Highly Recommended
Functional Verification Methodology

Integration Block (radiation dose):
7 conditions at 2 real-time cycles
determine alarm state → $2^{14}$ possibilities
max. integration period: 10 years
large bit widths: 48-64 bit
DUV Design under Verification (VHDL)

UVM Test (SystemVerilog = SV)

UVM Sequences: generate constrained-random transactions

UVM Environment

UVM Active Agent

UVM Driver

UVM Sequencer

UVM Scoreboard

Reference Model Wrapper (SV)

DUV Design under Verification (VHDL)

Virtual Interface (SV)

Properties

Output comparison

Coverage Collector

TEST RESULTS

COVERAGE DATA

UVM Top module (SV)

DUV Instantiation

Interface (SV)

Test entry function

DPI Interface (SV)

Function calls

Reference Model (C)
Functional coverage

• Describes the **design functionalities that should be verified**

• **Safety-related designs:** Coverage based on requirements

• **Black-box verification:** Coverage model describes relationship between inputs and outputs

• **SystemVerilog support:**
  • Cover groups: Value ranges (equivalence classes), value transitions, condition outcomes, cross coverage, …
  • Cover properties
## Constrained-Random Simulation with UVM Radiation Dose

<table>
<thead>
<tr>
<th>Cover type</th>
<th>Covered - all tests</th>
<th>Covered - passed tests</th>
<th>Nr. of coverpoints</th>
<th>Nr. of bins</th>
<th>Nr. of stimuli applied</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cover properties</td>
<td>100.00%</td>
<td>100.00%</td>
<td>–</td>
<td>–</td>
<td>16355</td>
</tr>
<tr>
<td>cgIntConditions</td>
<td>100.00%</td>
<td>93.98%</td>
<td>28</td>
<td>466</td>
<td>324647</td>
</tr>
<tr>
<td>cgIntRegression</td>
<td>100.00%</td>
<td>100.00%</td>
<td>3</td>
<td>3</td>
<td>250</td>
</tr>
<tr>
<td>cgIntValueRanges</td>
<td>91.95%</td>
<td>73.02%</td>
<td>17</td>
<td>656</td>
<td>249327</td>
</tr>
<tr>
<td>cgIntRobustness</td>
<td>7.15%</td>
<td>6.02%</td>
<td>8</td>
<td>392</td>
<td>280977</td>
</tr>
<tr>
<td>Total</td>
<td>79.82%</td>
<td>74.60%</td>
<td>56</td>
<td>1517</td>
<td>454200</td>
</tr>
</tbody>
</table>

Long calculation periods not covered.
Code coverage: Only most significant bits of time counting registers were not covered.
Constrained-Random Simulation with UVM
Radiation Dose

<table>
<thead>
<tr>
<th>Cover type</th>
<th>Covered - all tests</th>
<th>Covered - passed tests</th>
<th>Nr. of coverpoints</th>
<th>Nr. of bins</th>
<th>Nr. of stimuli applied</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cover properties</td>
<td>100.00%</td>
<td>100.00%</td>
<td>–</td>
<td>–</td>
<td>16355</td>
</tr>
<tr>
<td>cgIntConditions</td>
<td>100.00%</td>
<td>93.98%</td>
<td>28</td>
<td>466</td>
<td>324647</td>
</tr>
<tr>
<td>cgIntRegression</td>
<td>100.00%</td>
<td>100.00%</td>
<td>3</td>
<td>3</td>
<td>250</td>
</tr>
<tr>
<td>cgIntValueRanges</td>
<td>91.95%</td>
<td>73.02%</td>
<td>17</td>
<td>656</td>
<td>249327</td>
</tr>
<tr>
<td>cgIntRobustness</td>
<td>7.15%</td>
<td>6.02%</td>
<td>8</td>
<td>392</td>
<td>280977</td>
</tr>
<tr>
<td>Total</td>
<td>79.82%</td>
<td>74.60%</td>
<td>56</td>
<td>1517</td>
<td>454200</td>
</tr>
</tbody>
</table>

Clock cycle based cover properties: 37h simulation, transition cover groups: 3h simulation
integral >= threshold: 0 => 0 => 0 => ... => ... => 0 => 0 => 1
periodEnd == 1: 0 => 0 => 0 => ... => ... => 0 => 0 => 1
alarmReset == 1: 0 => 0 => 1 => ... => ... => 0 => 0 => 0

transition coverage

**MT** = Measurement Time
**DT** = Device Time
Formal Property Verification

**Goal:** Model checkers mathematically prove properties of design
+ Exhaustive proofs for all verification scenarios (within constraints)
+ Quick generation of counter examples (usually corner cases)
- State space explosion (depending on size of data inputs and sequential depth)

**Language:** SystemVerilog Assertions
+ Very flexible
+ Same code usable in formal tool & simulation
- Expensive licenses for commercial tools necessary, so far only few open source options (e.g. SymbiYosys)
Natural Language Properties

• **Requirement:**
"It shall be possible to manually trigger a reset of an radiation dose alarm through the supervision software."

• **Natural language property:**
"(Cycle is no MC and (alarm was configured as latched at the previous MC) and alarm reset equals 1 and (dose value is less than (threshold at previous MC) or alarm function was deactivated at previous MC)) implies that: (in one clock cycle, alarm is off)"

Natural Language Properties

"(Cycle is no MC and (alarm was configured as latched at the previous MC) and alarm reset equals 1 and (dose value is less than (threshold at previous MC) or alarm function was deactivated at previous MC)) implies that:(in one clock cycle, alarm is off)"

• SystemVerilog property:
  property pIntAlarmResetBetweenMT1();
  (mtValidxDI == 0 && latchedLastMC == 1 && integralAlarmResetxDI == 1 &&
   (signed’(integralxDO) < signed’(thresholdLastMc) ||
   alarmActiveLastMc == 0)) ->
   ##1 (ALARMxDO == 0);
endproperty
Functional Coverage – Formal Verification

\[ \text{Functional coverage}[^\%] = \frac{\text{Nr. of proven properties}}{\text{Nr. of properties}} \times 100.00 \]

Or with weights, similar to SystemVerilog covergroup coverage:

\[ \text{Weighted functional coverage}[^\%] = \frac{\sum_i (w_i \times p_i)}{\sum_i w_i} \times 100.00 \]

\[ w_i = \text{weight per property, } p_i = 1 \text{ if property was proven, } 0 \text{ otherwise} \]
Formal Property Verification Approach

DUV (VHDL)

DUV input/output ports

Input ports

Formal Module Instantiation

Formal Module (SystemVerilog)

Internal signals, constants

Assume statements

Formal properties

Assertion statements

inputs

Formal tool

outputs

PROOF RESULTS

COVERAGE DATA

Verification engineer

Design engineer

Verification tool

The Context
CROME System
HW Safety Integrity Verification
FW Safety Integrity Verification
Conclusion

H. Boukabache, S. Hurst, K. Ceesay-Seitz – A safety and reliability perspective of the CERN RadiatiOn Monitoring Electronics (CROME)

09/02/2021
Formal Property Verification

Approach

• Apply only necessary constraints (i.e. assumptions)
  • Verify all expected input values plus as many as possible unexpected ones

• Use synthesizable code for reference modelling
  • Full/partial models
  • Cycle-accurate/higher abstraction layer
  • Keeps properties simpler → faster proof calculation
  • Use functional & structural coverage as additional assurance
Formal Property Verification Approach

• Abstract time
  • Find recurring patterns
    • Arbitrary (X) values in reset state
    • Bounded proofs that span over one occurrence
  • Use cut points on time counters
    • All possible values will be verified, so it includes the normal passing of time
    • Verify passing of time in separate properties

Formal Property Verification
Example of results – Radiation Dose

• **Exhaustively Proved** radiation dose **alarm generation**

• **Partially proved** radiation dose **calculation**
  • Reference model in SystemVerilog
  • Constraints (formal assumptions)
    • Configured calculation period 0 … 100 ms, 0 = special value = unlimited
    • Internal time counting register < 4288896000 * 100ms (13.6 years)
    • Version 1: Operands of calculation -4 … 3
    • Version 2: Calculation period < 2, offset = 0xF80000 (16252928)
• Undocumented design decision discovered
  • Fault in rounding mechanism only if internal result was negative
  • Scenario not covered by simulation (400000 stimuli applied)

• Fault that would happen after 7 years of continuous operation
  • Found after 1 second with formal
  • Would require > 7 years of simulation
## Results – Integration block

<table>
<thead>
<tr>
<th>Found by</th>
<th>Update of specification</th>
<th>Update of implementation</th>
<th>Update of verification code</th>
<th>Total found by method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Review of requirements</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>9</td>
</tr>
<tr>
<td>Natural Language Properties</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Review of design specification</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>Constrained-random simulation</td>
<td>5</td>
<td>9</td>
<td>2</td>
<td>15</td>
</tr>
<tr>
<td>Formal Property Verification</td>
<td>4</td>
<td>3</td>
<td>4</td>
<td>11</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>15</strong></td>
<td><strong>20</strong></td>
<td><strong>13</strong></td>
<td><strong>38</strong></td>
</tr>
</tbody>
</table>
CERN RadiatiOn Monitoring Electronics (CROME)

crome.web.cern.ch

Alarm/Interlock Matrix:

Huge configurable logical formula
451 input bits (= $2^{451}$ configuration options)

Drives safety-critical outputs

sequential depth: 4 clock cycles
Formal Property Verification
Results – Alarm/Interlock Matrix

• Reference model in SystemVerilog
• Only constraint: parameters do not change during 4 cycles of formula evaluation

→ 46 properties proven in 33 seconds
  • estimated simulation time: $8 \times 10^{137}$ years

• Faults:
  • In one particular configuration radiation dose alert was not triggered due to a wrong VHDL vector range
  • Outputs were not consistently in safe state when invalid inputs were applied (inputs are anyway checked at software level)
Summary – Functional Verification

• Presented functional verification methodology
  ➢ Suitable for highly-parametrizable, continuously operating safety-critical designs
    ➢ Proofed safety-critical alarm functions
    ➢ Detected safety-critical faults
  ➢ Compliant to and enhances IEC 61508 verification requirements
    ➢ Independent black-box verification
    ➢ Semi-formal methods used during verification planning
    ➢ Relation of results to requirements (via coverage model)
    ➢ Formal verification for all safety integrity levels
CROME Manufacturing

- CROME HW has entirely been studied, tested and verified in in house

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

- Series production of 500 devices has been performed at CERN

28 External suppliers (2018/2019)

(2) High-Tech Electronic Companies
(1) Heat sinks Manufacturing
(1) Plastics Manufacturing
(1) Mechanics Manufacturing
(3) Electronic PCB Manufacturing
(3) Electronic Assembly
(5) Sealings Manufacturing
(5) Connectors
(5) Electronic Board Assembly
(5) Electronic Board Assembly
(1) LabView
(1) Mechanics manufacturing
(5) Electronic Assembly

(Industries per country)

High-Tech Electronic Companies

- FR 13%
- CH 24%
- US 13%
- IT 12%
- DE 10%
- NL 4%
- NO 2%
- ES 2%
- SE 1%
- AU 1%
- BE 1%
- PT 1%
- GR 1%
CROME Manufacturing

Assembly and integration of CROME Bulk version

- HW integration automated tests
- Temperature stress validation
- Temperature compensation

Assembly and integration of CROME Rackable version

- Automated current calibration
- HW integration automated tests

CROME Team

Detector integration
Stability tests

Temperature tests of CROME Rackable versions
Long-term tests of CROME Rackable versions

Conclusion
CROME at ESS
Cryogenic test stand (TS2b)

Monitored Areas at ESS

→ A second collaboration agreement is being negotiated to provide ESS with ~30 devices

4 CROME devices are currently being used at ESS

Ionizing radiation monitoring using CROME at ESS

The Context  CROME System  HW Safety Integrity Verification  FW Safety Integrity Verification  Conclusion

A second collaboration agreement is being negotiated to provide ESS with ~30 devices
Outlooks

- Prepare for future with HW upgrade
Thank you very much for your attention
Backup slides
The time structure of a radiation field at a given location depends directly on the accelerator(s) or experiment(s) in question.
CROMÉ 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 Devices

RAMS analysis and functional safety assessment according to the IEC 61508

- All critical components have been replaced with qualified ones
- Fail-safe architecture evolution:
  - Extension CROME radiation monitors testability
  - Defined measurement redundancy management
  - Defined power supply tree
- Extended tests to define functional limits:
  - Cycling tests and high temperature tests
Final results for the CROME system – Prototype Q

- **Probability of dangerous failure per hour**: \( PFH = 9.28 \times 10^{-08} \text{ [fpmh]} \)
- **Architectural constraints**: - excerpt

<table>
<thead>
<tr>
<th>Board</th>
<th>Functional blocks</th>
<th>Component type</th>
<th>SSF</th>
<th>HFT</th>
<th>SIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connectic board</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Power supply low voltages</td>
<td>Type A</td>
<td>98%</td>
<td>0</td>
<td>SIL 3</td>
<td></td>
</tr>
<tr>
<td>Output interlock interface</td>
<td>Type A</td>
<td>83%</td>
<td>1</td>
<td>SIL 3</td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Frontend board</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>High voltage power supply</td>
<td>Type A</td>
<td>99%</td>
<td>0</td>
<td>SIL 3</td>
<td></td>
</tr>
<tr>
<td>Current measurement</td>
<td>Type B</td>
<td>91%</td>
<td>0</td>
<td>SIL 2</td>
<td></td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Overall: **SIL 2 requirements are fulfilled**
Final results for the CJB – CROME Junction Box, simplified schematics

- Probability of dangerous failure per hour: \(PFH = 9.74 \cdot 10^{-09}[f_{pmh}]\)
- Architectural constraints: - excerpt

<table>
<thead>
<tr>
<th>Board</th>
<th>Functional blocks</th>
<th>Component type</th>
<th>SSF</th>
<th>HFT</th>
<th>SIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power module</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AC power input</td>
<td>Type A</td>
<td>100%</td>
<td>1</td>
<td></td>
<td>SIL 3</td>
</tr>
<tr>
<td>Power input redundancy</td>
<td>Type A</td>
<td>100%</td>
<td>1</td>
<td></td>
<td>SIL 3</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Processing module</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CPLD 1/2</td>
<td>Type B</td>
<td>77%</td>
<td>1</td>
<td></td>
<td>SIL 2</td>
</tr>
<tr>
<td>Internal power supplies</td>
<td>Type A</td>
<td>97%</td>
<td>0</td>
<td></td>
<td>SIL 3</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Overall: **SIL 2** requirements are fulfilled
IEC 61508 Standard

• International Electro-technical Commission (IEC) is an international standards organisation that publishes international standards for all electronic, electrical and related technologies.

• IEC 61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES) is a generic standard, which is applicable to all kinds of industries and covers the general requirements for a Safety Instrumented System (SIS) in all phases of its safety lifecycle.

• Consists of seven parts, whereas IEC 61508 - part 2 covers specific requirements for safety-related hardware.