Safety design on FPGA’s using soft Lockstep Processors

Roger May
Industrial System Architect
Example of a Motor Control System

Control algorithm implemented on Nios II Softcore processor

Low level motor control implemented in FPGA logic

Industrial Ethernet communication implemented on Nios II Softcore processor
Example of a Motor Control System with Safety

Safety processing implemented on Nios II Lockstep softcore processor

Safety encoder considered black channel communication

Industrial Ethernet considered black channel communication

Safety critical software
Non-safety critical FPGA IP
Non-safety critical software

Safety Processing
- Safety Communication Layer(s)
- Safety Encoder Processing

Emergency Shut off

Encoder I/face

Power Stage

FoC or DTC

PWM

ADC Interface

High level drive control

IE Stack
- Industrial Ethernet MAC

© 2016 Altera—Public

now part of Intel
Background: Lockstep Safety Processors

Safety designs require diagnostics to be run periodically to ensure safety function is functioning correctly.

For a processor this generally requires Software Test Libraries (STL’s):
- STL’s used to test processor functionality in addition to rest of system.

Disadvantages of STL’s:
- Running STL’s consume essential processing MIPS.
- STL’s are often destructive and require system context to be
  - Saved before running
  - Restored after running

Alternative to provide hardware realtime diagnostics via Lockstep processor implementation.
What is a lockstep processor ....

- It is **not** a 1oo2 system

- It is a processor with hardware diagnostics
  - Diagnostics provided by 2\textsuperscript{nd} slave processor and comparator
Why use a lockstep processor: DC requirements

<table>
<thead>
<tr>
<th>Safe Failure Fraction</th>
<th>Hardware Fault Tolerance</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0</td>
</tr>
<tr>
<td>&lt;60%</td>
<td>Not Allowed</td>
</tr>
<tr>
<td>60% - &lt;90%</td>
<td>SIL1</td>
</tr>
<tr>
<td>90% - &lt;99%</td>
<td>SIL2</td>
</tr>
<tr>
<td>≥99%</td>
<td>SIL3</td>
</tr>
</tbody>
</table>

STL may achieve 70% DC
- Limits safety capability to SIL1/2

Lockstep capable of achieving >99%
- Enables SIL3/4 capability
Why use a lockstep processor: Safety over IE

- Safety over Industrial Ethernet
  - IEC 61784-3

- Early solutions mapped logical SCL’s to separate processors
  - 1x standard MCU
  - 2x “safe” MCU’s

- High diagnostic coverage of lockstep solution allows both SCL’s to be mapped to single lockstep core
Nios II Lockstep

Verilog RTL IP implementing a smart comparator, integrated in a Dual Core Lock Step safety architectures using Nios II and Qsys
- IEC 61508 compliant: SIL3 (DC > 99%)
Nios II LockStep: Features

- Self-checking Comparator
  - Logic for self-diagnostic
  - Scalable fine grain comparator
  - Programmable blind window
  - HW Fault injector

- Timers
  - Programmable Reset events counter
  - Programmable Timeout on reset exit (timeout)
  - HW fault injector

- Error Controller
  - Robust OKNOK signal to flag errors detection to an external supervisor
  - Programmable alarms severity

- Configuration & Status interface
  - Logs and alarm context information dedicated for each safety mechanism
  - Protected configuration registers for safety relevant information
What additional tools/concepts do you need to realise this concept
(ASIC) V-Flow in IEC61508, is a cornerstone of safety development
Altera Safety Data Package

Qualified methods
- Altera have analysed IEC61508
- Part of this is FPGA specific V Flow

Altera FPGA specific V Flow
- FPGA Tuned
- Relates V Flow steps to FPGA tasks and tools
Safety FPGA Toolflows

Application Function

Safe Function

Altera FPGA/SoC

Modified Application Function

Safe Function

Need to re-certify my design!!
Safety Design Partitioning Overview

- Minimize impact analysis and re-certification efforts

- Tools to verify non-safe partition changes do not impact safe partitions
  - Significantly reduces risk and time-to-market

- Methodology and verification tools is qualified by TUV-Rheinland

- Available for use with Cyclone IV, Cyclone V & Cyclone V SoC
Failure Modes Effects and Diagnostic Analysis Tools

FMEDA tools calculates device specific failure rates

- **Inputs**
  - Details of users design (resource used)
  - Diagnostic features used and coverage
  - Mission profile (for IEC 62380 calculations)

- **Outputs**
  - Calculation of functional safety standard specific metrics
  - Device specific failure rates for permanent and transient faults
  - Detailed module / sub-module level failure rates
Example of a Motor Control System with Safety
Safe Processor Architecture

Safe processor & peripherals is safety critical

- Implement using
  - LockStep processor
    - >99% DC
    - Reduces need for STL -> more performance for safety application

- ECC for program/data RAM
  - 90% DC

- STL (limited) for
  - Timers
  - Interrupts
  - Bus infrastructure

- CRC Calculation
  - Accelerate CRC calculations for Safe IE

- Clock Checker
  - Check clock network/PLL
Use of FMEDA

<table>
<thead>
<tr>
<th>Module</th>
<th>Safety Related Module?</th>
<th>Number of I/Os used</th>
<th>Number of Transceiver used</th>
<th>Number of ALM Blocks</th>
<th>Number of Memory used for Memory</th>
<th>Number of M16K Blocks</th>
<th>Number of DSP Blocks</th>
<th>Routing Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>No</td>
<td>140</td>
<td>6</td>
<td>300</td>
<td>0</td>
<td>70</td>
<td>79</td>
<td>84.213%</td>
</tr>
</tbody>
</table>

**Remaining FPGA Fabric Resources**
- Logic
  - Memory: Yes
  - CRAM: No
  - I/O: Yes
- Transceiver

**Jser Module 1**
- Logic: Yes
- Memory: No
- CRAM: 5
- I/O: 0
- Transceiver: 8000

**Proportion of safe faults**
- Diagnostic 1: 99.00%
- Diagnostic 1 Coverage: 99.00%

**Total Diagnostic Coverage DC**:
- Diagnostic 1: 99.00%

**FPFGA**
- Permanent FIT (Die): 15.1
- Transient FIT (Die): 1209.0

**Safe Failure Fraction (SFF)**
- Combined permanent and transient: 98.38%

**Diagnostic Coverage (DC)**
- Combined permanent and transient: 96.77%

**Review Summary page**
- SFF > 98%

Enter Design Resource used for Safety design
Enter Diagnostics Used
FPGA Implementation

- Use Certified FPGA Toolflow to map design into FPGA

- Separation of safe/non-safe blocks
  - To allow updates of non-safe portion

Example Floorplan in FPGA
Altera’s TÜV-Qualified Functional Safety Data Package

First and only Comprehensive FPGA Safety Solution!

Altera Tools and IP are sufficiently free of systematic errors. Production Devices Qualified for SIL3.
Save man-years of development time to certify a safe application

Development Without “TÜV-Qualified Safety Package”

Development with “TÜV-Qualified Safety Package”

Safe Requirement Specification  Qualification of Used Devices and Tools  Implementation of Safe Functionality

Implementation of Safe Diagnostic Functions  Certification by TÜV

© 2016 Altera—Public
now part of Intel
### Qualified Tools
- Quartus II Software Version 14.1
  - QSys
- Altera Simulation Libraries
  - Synthesis
  - Place and Route
  - TimeQuest
- Signal Tap II
- NIOS® II debugger
- In-System memory editor
- PowerPlay power analyzer
- Safety Design Partitioning Flow
- SoC FMEDA

### Qualified IP
- Nios® II Embedded Processor
  - CRC Compiler
  - DDRx Memory Controller
  - 8B10B Encoder/Decoder
  - Qsys IP Suite
  - Diagnostic IP: CRC, SEU, Clock

### Qualified Devices
- Cyclone® V SoC, Cyclone® V, Cyclone® IV, Arria® V SoC, Arria® V
- Arria® V GZ, Arria® II GX/GZ
- Stratix® V, Stratix® IV
- Stratix® IV GX,
- MAX® V, MAX® II, MAX® II Z
SafeFlex – Functional Safety Development Kit

- 2 Cyclone V FPGAs and associated logic
- 1oo2 architecture (IEC61508: HFT=1)
- DDR3 RAM
- monitored power supply
- 6 DSIs / 4 DSOs
- supports Industrial Ethernet
- connectors for expansion boards
Thank You