Safety design on FPGA's using soft Lockstep Processors

Roger May
Industrial System Architect

now part of Intel

© 2016 Altera—Public

Example of a Motor Control System

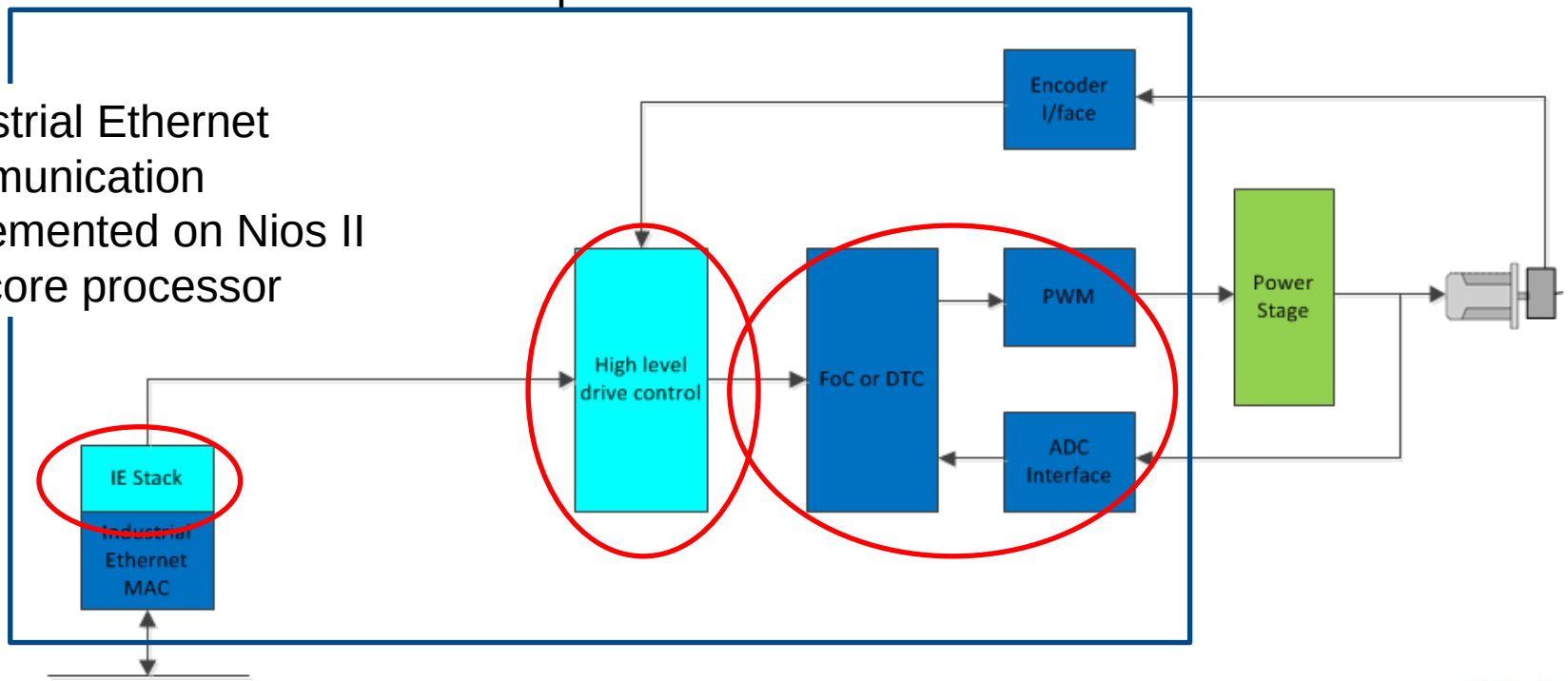
Non-safety critical FPGA IP

Non-safety critical software

Control algorithm implemented on Nios II Softcore processor

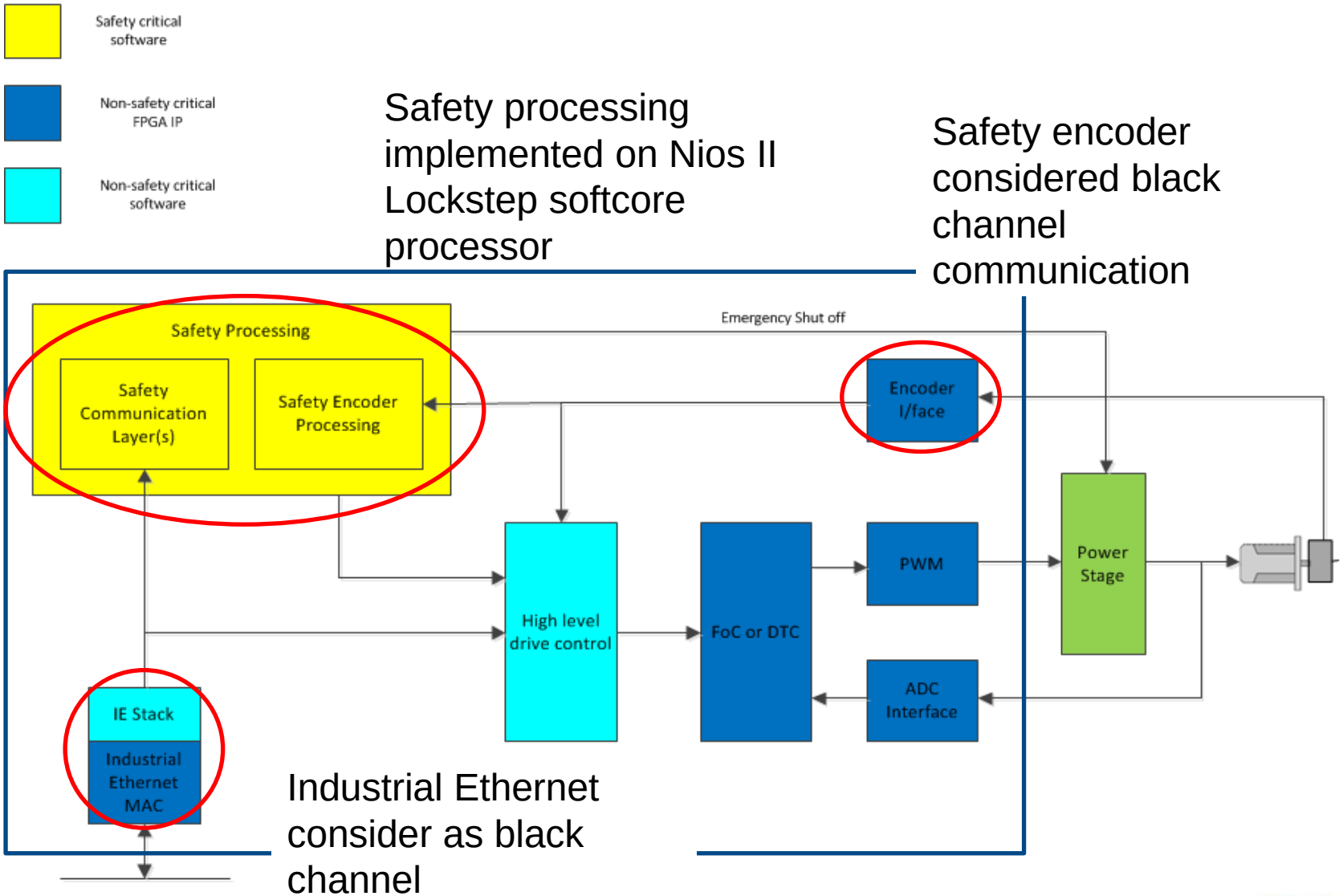
Low level motor control implemented in FPGA logic

Industrial Ethernet communication implemented on Nios II Softcore processor



© 2016 Altera—Public
ALTERA now part of Intel

Example of a Motor Control System with Safety



© 2016 Altera—Public
ALTERA 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

© 2016 Altera—Public
ALTERA now part of Intel

What is a lockstep processor ….

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

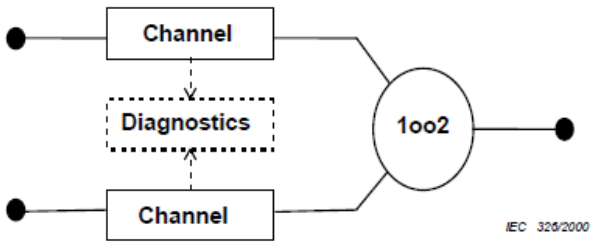
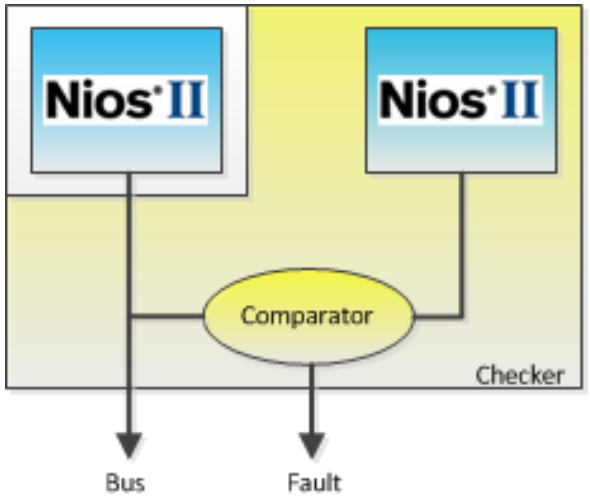


Figure B.6 – 1oo2 physical block diagram

- It is a processor with hardware diagnostics
  - Diagnostics provided by 2nd slave processor and comparator



© 2016 Altera—Public
ALTERA
now part of Intel

Why use a lockstep processor: DC requirements

Safe Failure Fraction	Hardware Fault Tolerance		
	0	1	2
<60%	Not Allowed	SIL1	SIL2
60% - <90%	SIL1	SIL2	SIL3
90% - <99%	SIL2	SIL3	SIL4
≥99%	SIL3	SIL4	SIL4

- STL may achieve 70% DC
  - Limits safety capability to SIL1/2
- Lockstep capable of achieving >99%
  - Enables SIL3/4 capability

© 2016 Altera—Public
ALTERA. now part of Intel

Why use a lockstep processor: Safety over IE

- Safety over Industrial Ethernet
  - IEC 61784-3

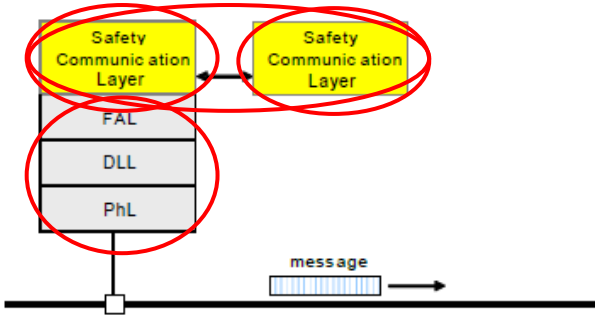
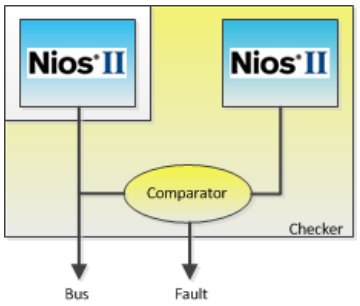


Figure A.1 - Model A

- Early solutions mapped logical SCL's to separate processors
  - 1x standard MCU
  - 2x "safe" MCU's

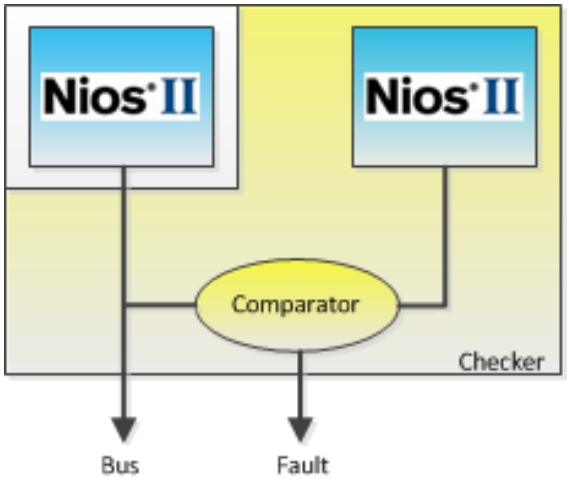
- High diagnostic coverage of lockstep solution allows both SCL's to be mapped to single lockstep core



© 2016 Altera—Public
ALTERA now part of Intel

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%)



Certificate

TÜVRheinland CERTIFIED — Functional Safety — www.tuv.com ID 0600000000

No.: 968/FSP 1260.00/16

Product tested	Diagnostic Intellectual Property (IP) for ALTERA NIOS II processor cores	**Certificate holder**	Yogitech SPA Via Lenin 132/p 56017 San Martino Ulmiano (Pisa) Italy
Type designation	fRSmartComp_nios2, details on the certified version can be found in the associated Revision Release List		
Codes and standards	IEC 61508 Parts 1-7:2010		
Intended application	The diagnostic IP is intended to be used together with the NIOS II/s or NIOS II/f processor cores. It is suitable to reach a diagnostic coverage (DC) of 99% for the processor core. The diagnostic IP meets the requirements IEC 61508-2 chapter 7.4.6 and Annex F for fault avoidance up to the Systematic Capability (SC) 3.		
Specific requirements	The instructions of the associated User Guide and Safety Manual shall be considered.		

Valid until 2021-04-22

The issue of this certificate is based upon an examination, whose results are documented in Report No. 968/FSP 1260.00/16 dated 2016-04-22.
This certificate is valid only for products which are identical with the product tested. It becomes invalid at any change of the codes and standards forming the basis of testing for the intended application.

Köln, 2016-04-22

TÜV Rheinland Industrie Service GmbH
Bereich Automation
Funktionale Sicherheit
Am Grauen Stein, 51105 Köln
Certification Body Safety & Security for Automation & Grid

Dipl.-Ing. Heinz Gall

TÜV Rheinland Industrie Service GmbH, Am Grauen Stein, 51105 Köln / Germany
Tel.: +49 221 806-1790, Fax: +49 221 806-1539, E-Mail: industrie-service@de.tuv.com

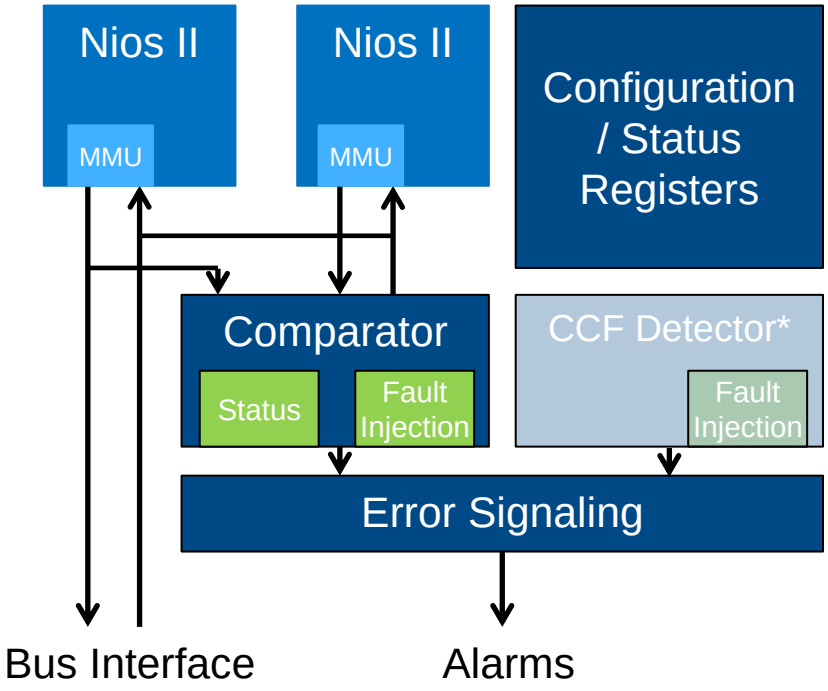
www.fs-products.com
www.tuv.com

TÜVRheinland®
Precisely Right.

© 2016 Altera—Public

ALTERA
now part of Intel

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

YOGITECH

© 2016 Altera—Public
ALTERA now part of Intel

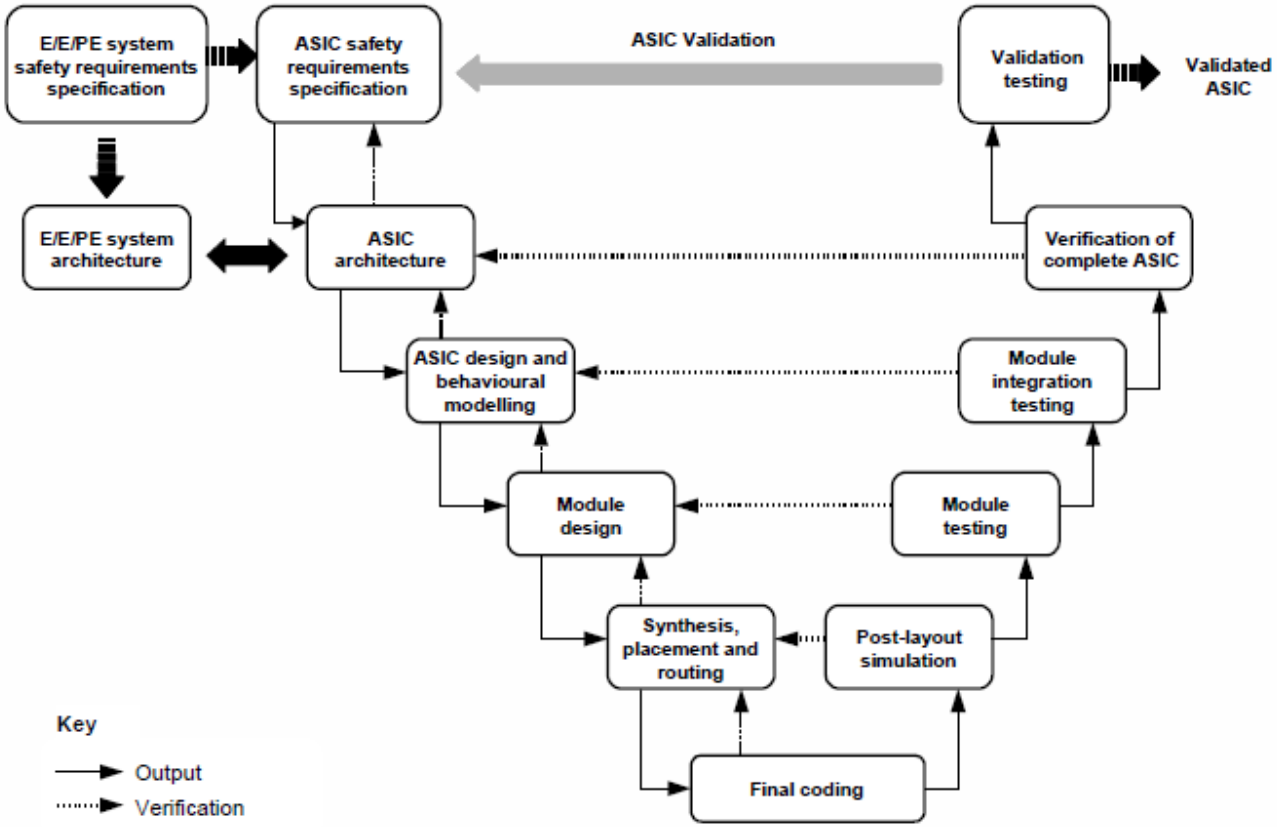
What additional tools/concepts do you need to realise this concept

now part of Intel

© 2016 Altera—Public

IEC61508 ASIC V Flow

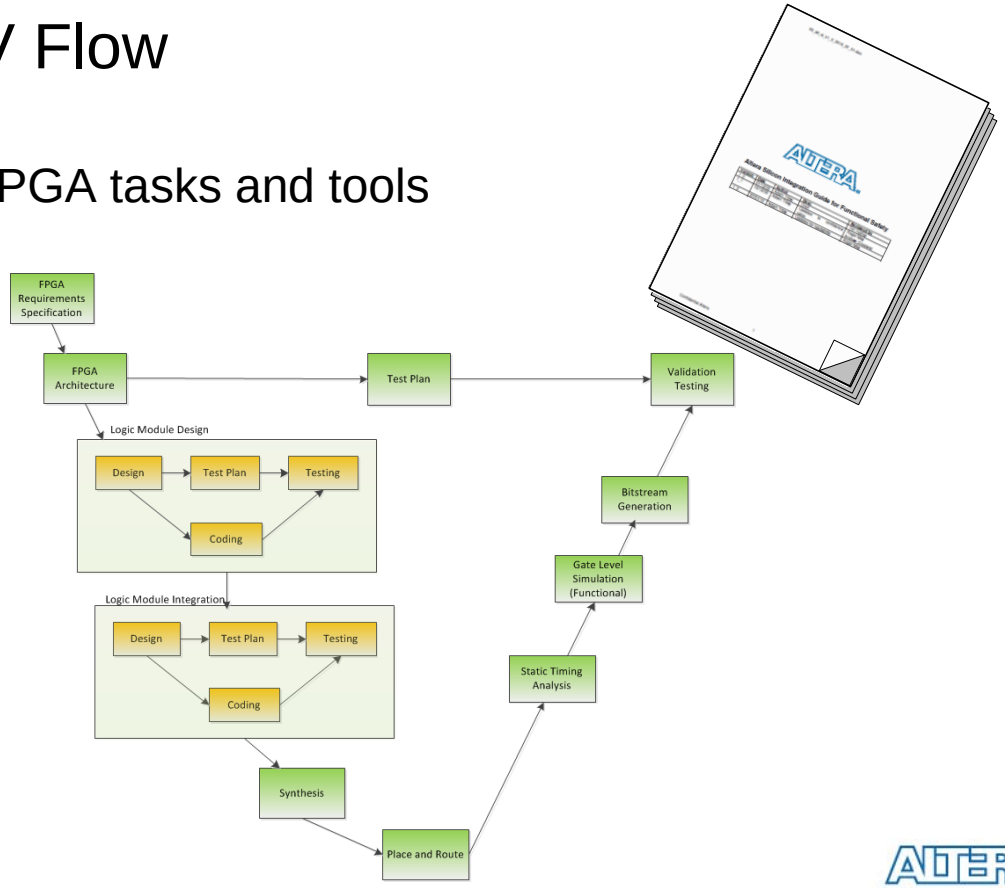
- (ASIC) V-Flow in IEC61508, is a cornerstone of safety development



© 2016 Altera—Public
ALTERA now part of Intel

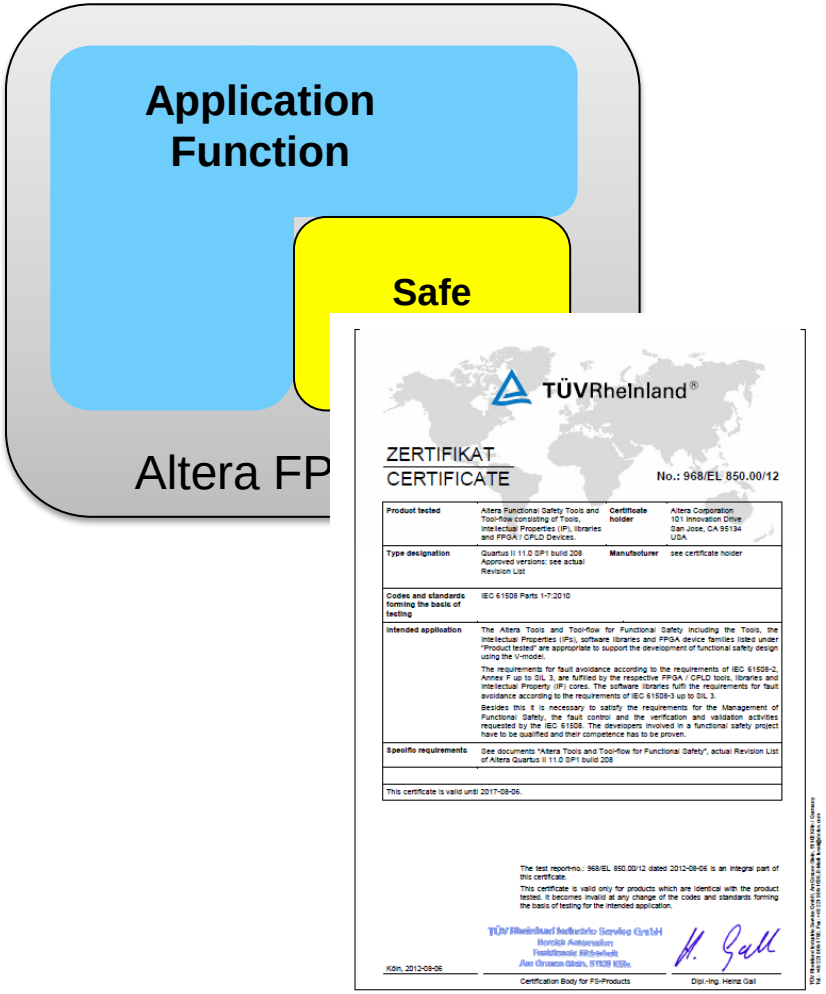
Altera Safety Data Package

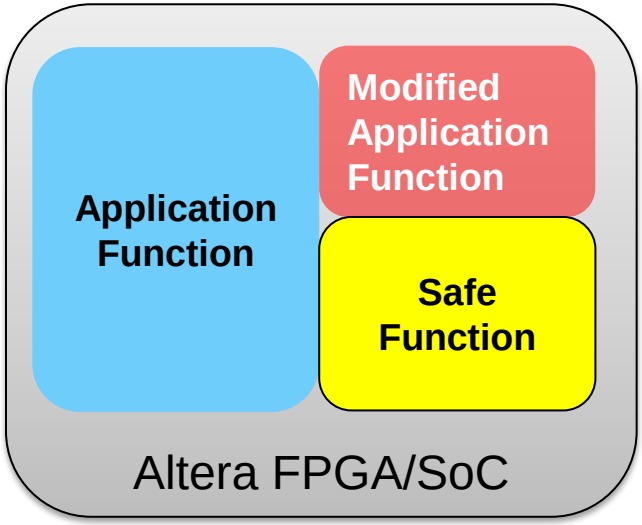
- Qualified methods
  - Altera have analysed IEC61508
  - Part of this is FPGA specific V Flow
- Altera FPGA specific V Flow
  - FPGA Tuned
  - Relates V Flow steps to FPGA tasks and tools



© 2016 Altera—Public
now part of Intel

Safety FPGA Toolflows





- Need to re-certify my design!!

© 2016 Altera—Public

ALTERA now part of Intel

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

TÜVRheinland®

ZERTIFIKAT
CERTIFICATE

No.: 968/EL 850.00/12

Product tested	Altera Functional Safety Tools and Tool-flow consisting of Tools, Intellectual Properties (IP), libraries and FPGA / CPLD Devices.	**Certificate holder**	Altera Corporation 101 Innovation Drive San Jose, CA 95134 USA
Type designation	Quartus II 11.0 SP1 build 208 Approved versions: see actual Revision List	**Manufacturer**	see certificate holder
Codes and standards forming the basis of testing	IEC 61508 Parts 1-7:2010		
Intended application	The Altera Tools and Tool-flow for Functional Safety including the Tools, the Intellectual Properties (IPs), software libraries and FPGA device families listed under "Product tested" are appropriate to support the development of functional safety design using the V-model. The requirements for fault avoidance according to the requirements of IEC 61508-2, Annex F up to SIL 3, are fulfilled by the respective FPGA / CPLD tools, libraries and Intellectual Property (IP) cores. The software libraries fulfil the requirements for fault avoidance according to the requirements of IEC 61508-3 up to SIL 3. Besides this it is necessary to satisfy the requirements for the Management of Functional Safety, the fault control and the verification and validation activities requested by the IEC 61508. The developers involved in a functional safety project have to be qualified and their competence has to be proven.		
Specific requirements	See documents "Altera Tools and Tool-flow for Functional Safety", actual Revision List of Altera Quartus II 11.0 SP1 build 208		
This certificate is valid until 2017-08-06.			

Köln, 2012-08-06

© 2016 Altera—Public

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

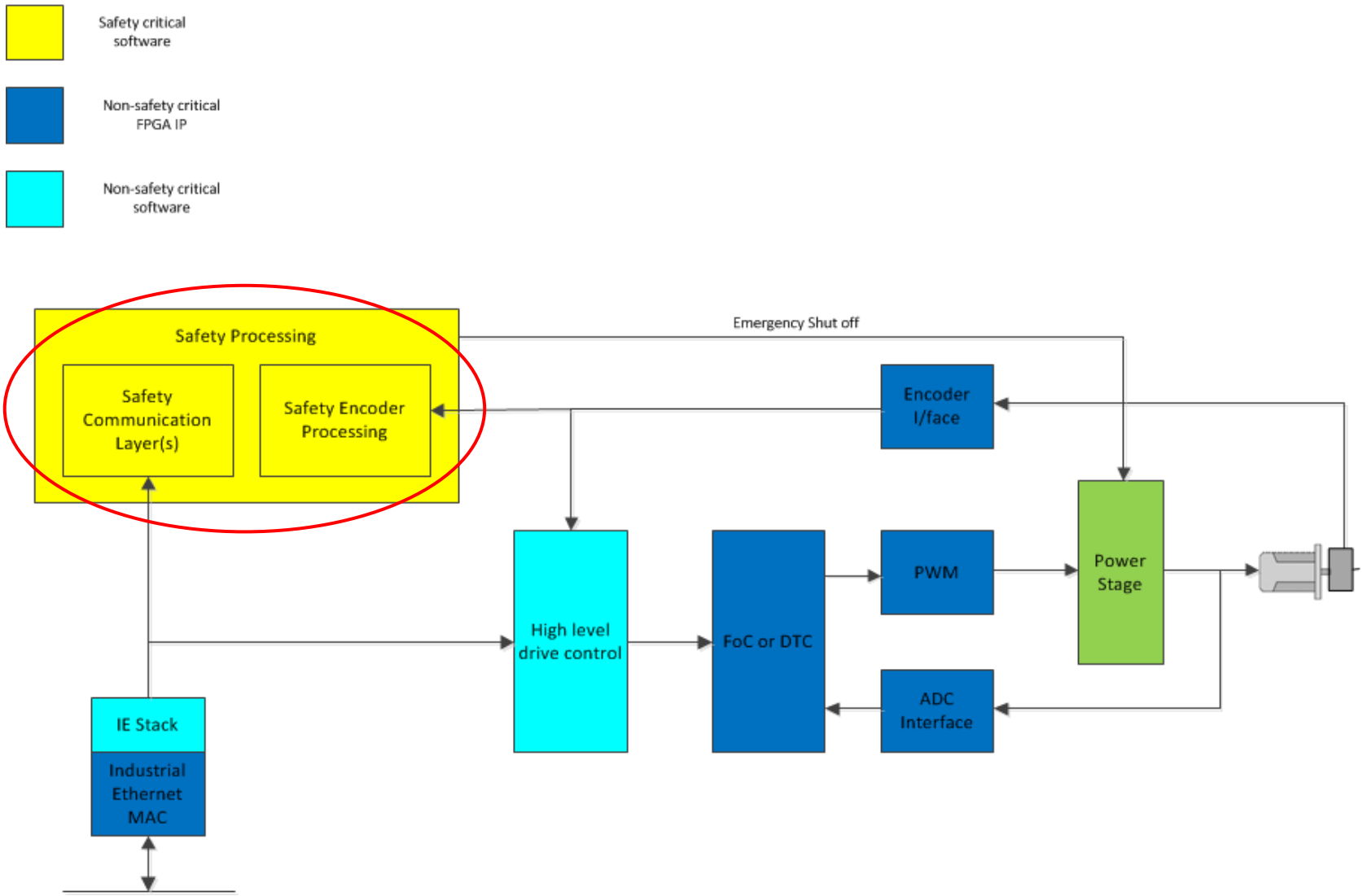
ALTERA

Average Interconnect Usage:	0%	Total FIT	11.4715346	9.74704816	1.72448639

Module		Safety Related Module?	Number of I/Os used	Number of Transceiver used	Number of ALM Blocks	Number of ALM used for Memory	Number of M10K Blocks	Number of DSP Blocks	Routing Percentage	Intrinsic FIT (λ)	Proportion of safe faults (F_{safe})	Safe Fault (λ_{Sa})	Dangerous Fault (λ_{Da})	Diagnostic 1	Diagnostic 1 Coverage	Diagnostic 1 used in application?
Safety Module #1	Logic	Yes	20	0	3000	20	300	20	0.000%	1.06198126	50.00%	0.53099063	0.53099063	Self test	90.00%	Yes
	Memory									0.86666496	50.00%	0.43333248	0.43333248	Galpat test power on test	100.00%	Yes
	CRAM									0.10260119	50.00%	0.05130059	0.05130059	EDCRC	99.00%	Yes
	I/O									0.03127875	50.00%	0.01563938	0.01563938	Redundant IO	99.00%	Yes
	Transceiver									0	50.00%	0	0		0.00%	No

© 2016 Altera—Public
ALTERA now part of Intel

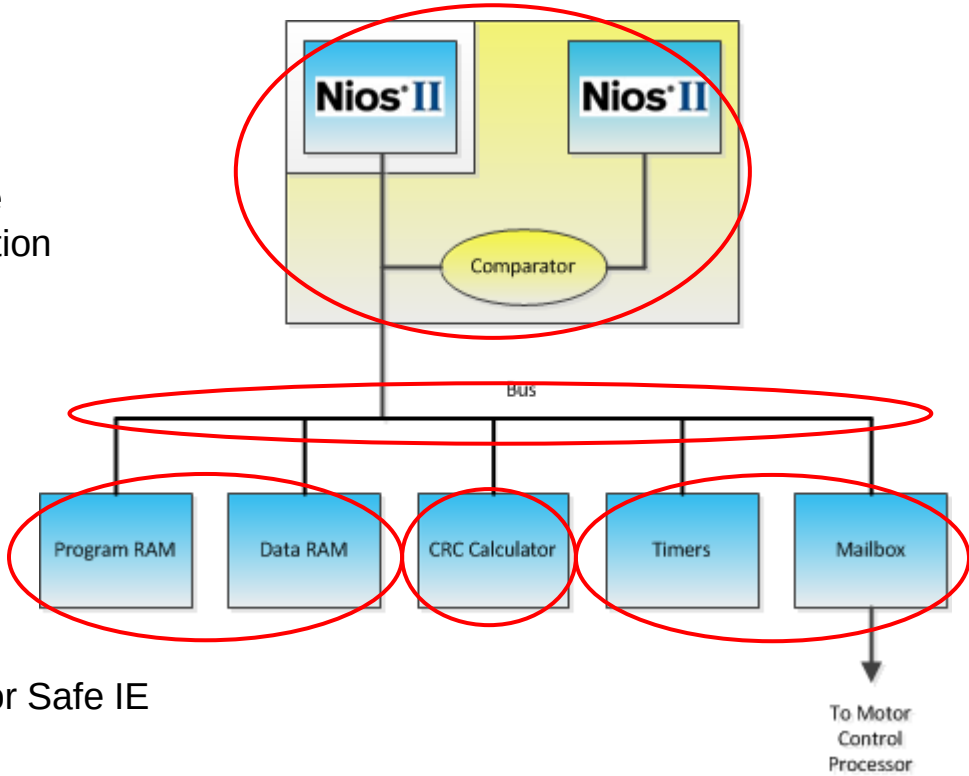
Example of a Motor Control System with Safety



© 2016 Altera—Public
now part of Intel

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



© 2016 Altera—Public
ALTERA now part of Intel

Use of FMEDA

ALTERA

Average Interconnect Usage:	30%	Total FIT

Module		Safety Related Module?	Number of I/Os used	Number of Transceiver used	Number of ALM Blocks	Number of ALM used for Memory	Number of M10K Blocks	Number of DSP Blocks	Routing Percentage
Remaining FPGA Fabric Resources	Logic	No	140	6	7094	0	70	79	84.211%
	Memory								
	CRAM								
	I/O								
	Transceiver								
User Module 1	Logic	Yes	5	0	8000	0	200	5	15.789%
	Memory								
	CRAM								
	I/O								
	Transceiver								

Module		Permanent Faults: Proportion of safe faults (F_{safe})	Permanent Faults: Diagnostic 1	Permanent Faults: Diagnostic 1 Coverage	Transient Faults: Proportion of safe faults (F_{safe})	Transient Faults: Diagnostic 1	Transient Faults: Diagnostic 1 Coverage	Transient Faults: Total Diagnostic Coverage DC
Remaining FPGA Fabric Resources	Logic	50.00%		0.00%	50.00%		0.00%	0.00%
	Memory	50.00%		0.00%	50.00%		0.00%	0.00%
	CRAM	50.00%		0.00%	50.00%		0.00%	0.00%
	I/O	50.00%		0.00%	50.00%		0.00%	0.00%
	Transceiver	50.00%		0.00%	50.00%		0.00%	0.00%
User Module 1	Logic	50.00%	STL	60.00%	50.00%	STL	60.00%	60.00%
	Memory	50.00%	ECC	90.00%	50.00%	ECC	90.00%	90.00%
	CRAM	50.00%	EDCRC	99.00%	50.00%	EDCRC	99.00%	99.00%
	I/O	50.00%	STL	60.00%	50.00%	STL	60.00%	60.00%
	Transceiver	50.00%		0.00%	50.00%		0.00%	0.00%

Enter Design Resource used for Safety design

Enter Diagnostics Used

	FPGA Permanent FIT (Die)	FPGA Transient FIT (Die)
Intrinsic FIT	15.1	1209.0
Safe fault (λ_S)	2.2	156.5
Dangerous fault (λ_D)	2.2	156.5
Dangerous Detected fault (λ_{DD})	2.1	151.5
Dangerous Undetected fault (λ_{DU})	0.1	5.0

Safe Failure Fraction (SFF) - combined permanent and transient	98.38%
Diagnostic Coverage (DC) - combined permanent and transient	96.77%

Review Summary page

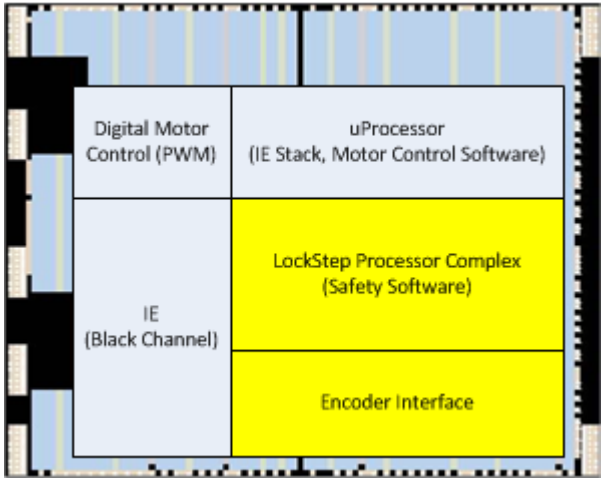
- SFF > 98%

© 2016 Altera—Public

ALTERA now part of Intel

FPGA Implementation

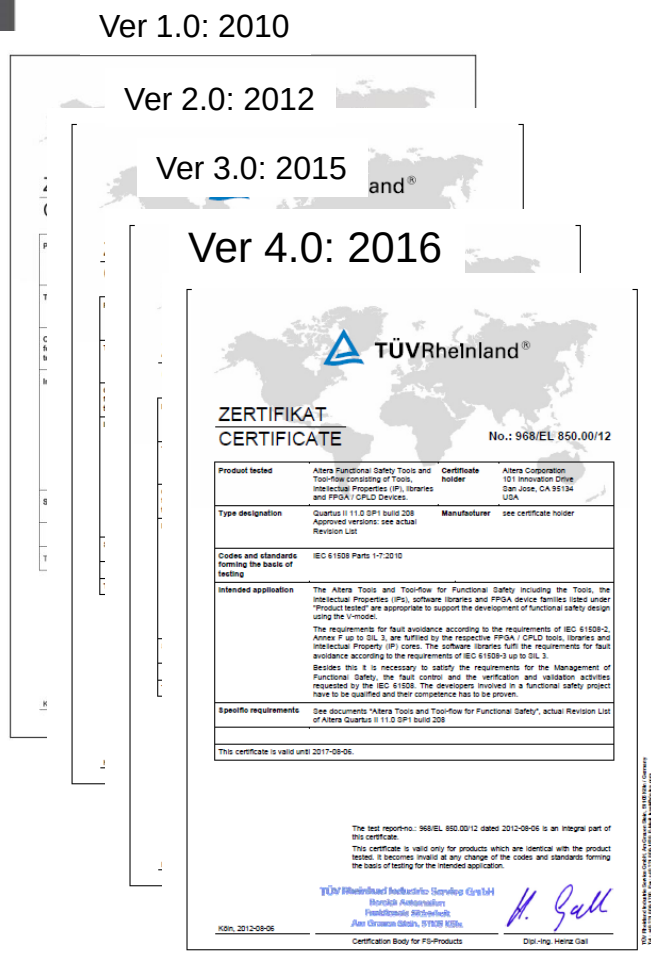
- Use Certified FPGA Toolflow to map design into FPGA
- Separation of safe/non-safe blocks
  - To allow updates of non-safe portion



Example Floorplan in FPGA

© 2016 Altera—Public

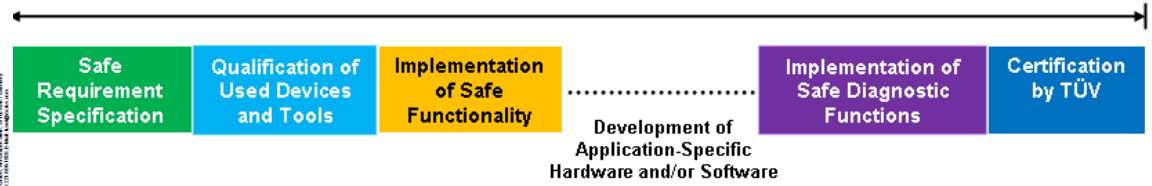
Altera's TÜV-Qualified Functional Safety Data Package



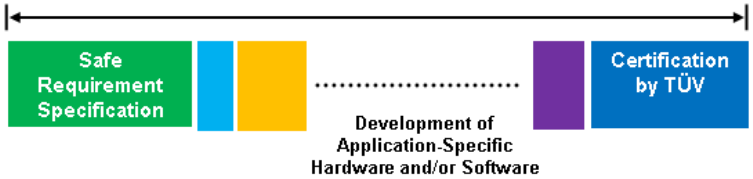
First and only Comprehensive FPGA Safety Solution!

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 "TUV-Qualified Safety Package"



Development with "TUV-Qualified Safety Package"



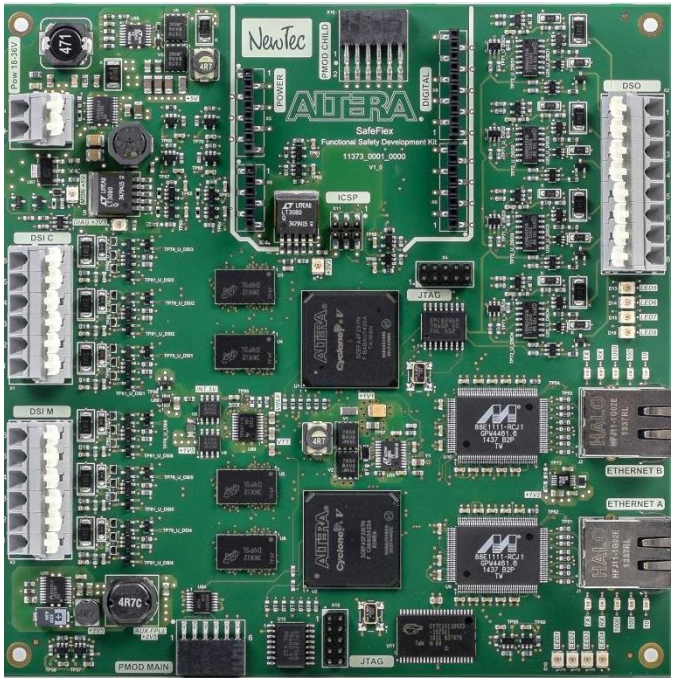
© 2016 Altera—Public
ALTERA now part of Intel

Functional Safety Data Package Rev 4

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

© 2016 Altera—Public
now part of Intel

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

© 2016 Altera—Public

Thank You

© 2015 Altera Corporation—**Confidential**

All rights reserved. ALTERA, ARRIA, CYCLONE, ENPIRION, MAX, MEGACORE, NIOS, QUARTUS and STRATIX words and logos are trademarks of Altera Corporation and registered in the U.S. Patent and Trademark Office and in other countries. All other words and logos identified as trademarks or service marks are the property of their respective holders as described at www.altera.com/legal.