An overview of functional safety standards and easing certification

exida / Texas Instruments

Chris O’Brien – exida, CFSE
Hoiman Low – TI Safety MCU
June / 2014
Topics

• exida
  • Overview of functional safety standards for industrial and automotive systems
  • Steps to certification
  • Services provided by exida

• Texas Instruments
  • Hercules MCU family and safety features overview
  • Hercules MCU for IEC 61508, ISO 26262 and other functional safety standards
exida Capabilities

Assessment and Certification

Lifecycle Services

Knowledge Base

Library
Training
Tools
Experts

Copyright exida 2000-2014
The origins of IEC 61508: 1988

Piper Alpha 167 dead $3.4B
Industrial Accident Causes: 1995

- Specification: 44%
- Design & Implementation: 15%
- Installation & Commissioning: 6%
- Operation & Maintenance: 15%
- Changes after Commissioning: 21%

"Out of Control: Why Control Systems go Wrong and How to Prevent Failure," U.K.: Sheffield, Heath and Safety Executive

Copyright exida 2000-2014
The continuing need today . . .
Functional Safety

• Functional Safety Goal – The automatic safety function will perform the intended function correctly or the system will fail in a predictable (safe) manner.

• Perform the intended function correctly – Reliability Engineering
• Fail in a predictable manner – Safety Engineering
IEC 61508 Safety Lifecycle

ANALYSIS Phase
What should it do?

REALIZATION Phase
How will it do it?

OPERATION Phase
How do you keep it doing what it should?

Copyright exida 2000-2014
IEC 61508 – Fundamental Concepts

IEC61508 Safety Life Cycle – detailed engineering process

Systematic Faults – Design Mistakes

RELIABILITY

Probabilistic performance based system design

Random Failures

HARDWARE RELIABILITY
The Functional Safety Standards Can be Applied at Many Levels

- **Components**
  - Process assessment, failure analysis/data and documentation to help product development

- **Elements**
  - Process assessment, hardware failure analysis/data and documentation showing usage in system design

- **Systems**
  - Risk based framework for SIL level, process assessment and system failure analysis
Safety Functions (Safety Goals)

• Specific single set of actions and the corresponding equipment needed to identify a single hazardous event and act to bring the system to a safe state.

• Examples:
  – Open drain valve when tank level is too high
  – Sound an alarm when explosive gas concentration exceeds a certain level
**Element** - part of a subsystem comprising a single component or any group of components that performs one or more element safety functions.

[IEC 62061, definition 3.2.6, modified]

**NOTE 1**: An element may comprise hardware and/or software.

**NOTE 2**: A typical element is a sensor, programmable controller or final element.
The system architecture drawing(s) document the relevant sub-systems and their relationship. The function(s) of each sub-system is fully described.
Project Milestones

• Product and process review
• Product reliability and failure mode analysis
• Requirements fulfillment and traceability
• Final audit and assessment report
Certification Process

New product with no field history:

– The new design must have a full hardware failure analysis.

– The new design must follow the design process requirements of IEC 61508 for the target SIL level.

– A Safety Manual must be created to explain how to use the product at the system level.
Using a component database, failure rates and failure modes for a product (transmitter, I/O module, solenoid, actuator, valve) can be determined far more accurately than with only field warranty failure data.
Software Development V-model

- **E/E/PE system safety requirements specification**
- **Software architecture**
- **Software safety requirements specification**
- **Software system design**
- **Module design**
- **Module testing**
- **Integration testing (module)**
- **Integration testing (components, subsystems and programmable electronics)**
- **Validation testing**
- **Validated software**
- **Coding**
- **Output**

Copyright exida 2000-2014
Tool Justification

Why would the IEC 61508 committee care about tools?

During the final certification audit of a transmitter, the assessor asked to witness the RAM test. After injecting a bad bit, nothing happened.

The software engineer had “simply set the optimization up one level”. The optimizer concluded the diagnostic code (save a byte to a temporary location, set all bits, clear all bits, return the original value) could be eliminated. And it did exactly that. This had a major impact on cost and release schedule.

Those using a tool must know how the tool works. Sometimes tools can be dangerous.

Those using a tool must understand how all settings impact operation of the tool.
Offline Tool Qualification Requirements

• Documented selection criteria and justification
• Document tool version and release date
• Document results of any tool validation performed
• For T2 and T3 only:
  – Evidence that Tool Specification/Documentation is provided to users
  – Determine level of reliance on tools (T2 / T3)
  – Identify and mitigate tool failures that could affect executable software (e.g., Tool HAZOP)
Accreditation

Each Certification Body (CB) operates per a “scheme” and gets accredited by an Accreditation Body (AB). In the USA, ANSI is the AB.

Functional Cyber-Security
- Achilles Level 1-2
- ISA Secure Levels 1 – 3

Functional Safety Certification
- IEC 61508
- IEC 61511
- IEC 62061 / ISO 13849
- IEC / ISO 26262
- EN 50271
- Other Functional Safety

Copyright exida 2000-2014
exida Products and Services

Consulting
- Process Safety (IEC 61511, IEC 62061, ISO 26262)
- Alarm Management
- Control System Security (ISA S99)

Product Certification
- Functional Safety (IEC 61508)
- Control System Security
- Network Robustness (Achilles)

Professional Certification
- CFSE
- CFSP
- Control System Security Expert (CSSE)

Training
- Process Safety
- Control System Security
- Onsite
- Offsite
- Web
- Security Development

Engineering Tools
- exSILentia (PHA Import, SIL Selection, LOPA, SRS, SIL Verification)
- Safety Case
- FMEDA
- SCA

Reference Materials
- Databases
- Tutorials
- Textbooks
- Reference Books
- Market Studies

Copyright exida 2000-2014
excellence in Dependable Automation
Topics

• exida
  • Overview of functional safety standards for industrial and automotive systems
  • Steps to certification
  • Services provided by exida

• Texas Instruments
  • Hercules MCU family and safety features overview
  • Hercules MCU for IEC 61508, ISO 26262 and other functional safety standards
TI Hercules™ MCU Platform
ARM® Cortex™ Based Microcontrollers

Hercules™ MCU Platform

Industrial and Medical Safety MCUs
- 100MHz to 330MHz
- 384KB to 4MB Flash
- -40 to 105°C Operation
- ENET, USB, CAN & UART
- Developed to Safety Standards
  - IEC 61508 SIL-3
  - Cortex-R – up to 550 DMIPs

TMS570
Transportation and Automotive Safety MCUs
- 80MHz to 300MHz
- 256KB to 4MB Flash
- Automotive Q100 Qualification
- -40 to 125°C Operation
- FlexRay, ENET, CAN, LIN/UART
- Developed to Safety Standards
  - ISO 26262 ASIL-D
  - IEC 61508 SIL-3
  - Cortex-R – up to 500 DMIPs

Lockstep MCUs for functional Safety
Applying Functional Safety Standards

SafeTI™ design packages help meet functional safety requirements while managing both systematic and random failures.

**Safety Life Cycle**
- Development Process
- Safety Plan
- Documentation
- Config Management
- Change Management
- V&V
- Personnel Competence
- Certification

**SIL - 1/2/3/4**
- Systematic Failures
  - Software
  - Tools
- Random Failures
  - Diagnostics
  - Architectural Metric
  - Failure Rate

**Process Certification**
- Software CSP
- Compiler Qual. Kit

Hercules Architecture (FMEDA)

CSP = Compliance Support Package

**Hercules Architecture (FMEDA)**

Texas Instruments
Hercules MCU safety features

- **CPU Self Test Controller** requires little S/W overhead
- **Physical design** optimized to reduce probability of common cause failure
- **Lockstep CPU & Lockstep Interrupt Fault Detection**
- **ECC or Parity on select Peripheral, DMA and Interrupt controller RAMS**
- **Parity or CRC in Serial and Network Communication Peripherals**
- **ECC for flash / RAM evaluated inside the Cortex R**
- **Memory Protection Unit**
- **Memory BIST on all RAMS for fast memory test**
- **Error Signaling Module w/ External Error Pin**
- **On-Chip Clock and Voltage Monitoring**
- **Protected Bus and lockstep Interrupt Manager**
- **IO Loop Back, ADC Self Test, …**
- **Dual ADC Cores with shared channels**

**Safe Island Hardware diagnostics**

**Blended HW diagnostics**

**Non Safety Critical Functions**

**Bold items are introduced with the new Cortex-R5 devices**
Hercules TMS570LS and RM4x Architecture Concept Assessment

Technical Report on the Concept of the Hercules TMS570LSx and RM4x Platform Architecture

Manufacturer:
Texas Instruments Incorporated
12201 Southwest Freeway
Stafford TX 77477
USA

Report no. TH954673T
Revision 1.0 of 2014-03-26

Test Laboratory
TÜV SÜD Rail GMBH
Generic Safety Systems
Barthstrasse 16
D-80339 Munich

This technical report may be reproduced only in complete wording. The use for promotion needs written permission. It contains the result of a unique investigation of the product being tested and places no generally valid judgment about characteristics out of the running fabrication. Official translations of this technical report are to be authorized by the test and certification agency.

2 Basis of Evaluation
The regulations and guidelines which form the basis of the type testing are listed below.

2.1 Functional Safety

<table>
<thead>
<tr>
<th>No.</th>
<th>Standard</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems</td>
</tr>
</tbody>
</table>

Table 2: Functional Safety

5 Result of the concept review

5.1 Concept review based on IP-FMEAs
To evaluate the Platform Architecture according to the required failure modes defined in [N1] and [N2] for SIL 3 and ASIL D the analysis method Failure Mode and Effects Analysis (FMEA) was used. For each IP an own FMEA was created. Within these FMEAs diagnostic measures and timing aspects have been analysed. These FMEAs should be used in further development as input for the Safety requirement specification of several safety microcontroller devices.

Result:
The FMEAs provided in the documents [D1] - [D38] were made by Texas Instruments Incorporated and reviewed by TÜV SÜD. The results of the FMEAs meet the requirements according to [N1] and [N2]. These review results are recorded in [R1] - [R38]. The effectiveness of the selected diagnostic measures has to be verified on the final device.

6 Summary
For the analyzed failure modes according to [N1] - [N2] appropriate diagnostic measures to reach SIL 3 or ASIL D have been specified. A concluding re-evaluation of the IP-FMEAs has to be done in context of the final device.
SafeTI™ Hitex Safety Kit

**Kit Overview**
- Fault injection and reaction monitoring via GUI
- MCU Diagnostic features profiling
- SafeTI Software Framework + SafeRTOS included

**Hitex Safety Kit Software**

**SAFETI-HSK-RM48**
**SAFETI-HSK-570LS31**

- On Board Display
- TPS65381 Power Supply & Safety Monitor
- ControlCard Interface
- Hercules™ MCU
Hercules Safety Documents

Documents provided by TI *some under NDA* to assist in the safety certification process:

- **Hercules component Safety Manual (SM)**
  Details product safety architecture and recommended usage

- **Safety Analysis Report Summary (SAR1)**
  Summary of FIT rate and FMEDA at component level for IEC 61508 and ISO 26262

- **Detailed Safety Analysis Report (SAR2)**
  - Full details of all safety analysis executed down to MODULE level for IEC 61508 and ISO 26262
  - Software tool for customizing analysis results to customer use case

- **Safety Report**
  Summary of compliance to IEC 61508 and/or ISO 26262
Hercules Safety Documents

Safety Manual

Table 2. Summary of Safety Features and Diagnostics

<table>
<thead>
<tr>
<th>Device Partition</th>
<th>Unique Identifier</th>
<th>Safety Feature or Diagnostics</th>
<th>Feature Recommendation</th>
<th>Possible ISO 26262-2011 Latest Diagnostics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power Supply</td>
<td>PWR1</td>
<td>Voltage monitor (VMON)</td>
<td>M</td>
<td>Internal Voltage Superviser</td>
</tr>
<tr>
<td></td>
<td>PWR2</td>
<td>External voltage supervisor</td>
<td>++</td>
<td>Voltage monitor (VMON)</td>
</tr>
<tr>
<td>Power Management</td>
<td>PMM1</td>
<td>Lockstep PCON</td>
<td>M</td>
<td>PCON lockstep self-test</td>
</tr>
<tr>
<td>Module (PMM)</td>
<td>PMM2</td>
<td>Privileged mode access and multi-bit keys for</td>
<td>M</td>
<td>Software test of register configuration and error response</td>
</tr>
<tr>
<td></td>
<td>PMM3</td>
<td>Periodic software readback of static</td>
<td>+</td>
<td>CPU lockstep</td>
</tr>
<tr>
<td></td>
<td>PMM4</td>
<td>Software readback of written configuration</td>
<td>++</td>
<td>CPU lockstep</td>
</tr>
<tr>
<td></td>
<td>PMM5</td>
<td>PCON lockstep comparator self-test</td>
<td>++</td>
<td>Self-test self-test</td>
</tr>
</tbody>
</table>

Detailed Safety Analysis Report

4.2 Summary of IEC 61508 Safety Metrics at Device Level (BGA Package)

Table 3 provides estimates of FIT rates and calculated safety metrics per IEC 61508-2:2010 using previously noted assumptions for the device in BGA package.

<table>
<thead>
<tr>
<th>Safety Metric</th>
<th>Notation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total faults</td>
<td>( \lambda )</td>
</tr>
<tr>
<td>Total non safety related faults</td>
<td>( \lambda_{en} )</td>
</tr>
<tr>
<td>Total safe faults</td>
<td>( \lambda_0 )</td>
</tr>
<tr>
<td>Total dangerous faults</td>
<td>( \lambda_d )</td>
</tr>
<tr>
<td>Total dangerous detected faults</td>
<td>( \lambda_{d0} )</td>
</tr>
<tr>
<td>Total dangerous undetected faults</td>
<td>( \lambda_{d0u} )</td>
</tr>
</tbody>
</table>
TI’s hardware functional safety development process has been certified for:

- IEC 61508 SIL-3
- ISO 26262 ASIL-D

The certification demonstrates TI’s commitment to have a process suitable for developing hardware components that are compliant to ISO 26262 and IEC 61508
Hercules™ and SafeTI™ Software and Tool Packages

Hercules Software and Tools

- Production quality software to easily use Hercules MCU
- Includes GUI configurator (where relevant)
- Includes User Guide and Release Notes

SafeTI Compliance Support Package

- Provide evidence to safety standards
- Includes Test Reports, Quality Metrics, Safety Manual, etc.
- Software developed to IEC 61508 & ISO 26262 requirements

SafeTI Tool Qualification Kit

- Assists in qualifying the TI ARM Compiler to functional safety standards
- Model-based tool qualification methodology
- Assessed to comply with both IEC 61508 and ISO 26262
SafeTI™ Compiler Qualification Kit

- Assists in qualifying the TI ARM C/C++ Compiler to functional safety standards
- Qualification of customer specific use case can be less restrictive than certified compilers
- Application of kit assessed by TÜV Nord to comply with both IEC 61508 and ISO 26262

Includes:
- Qualification Support Tool (model-based)
- Process specific documentation:
  - Tool Classification Report
  - Tool Qualification Plan
  - Tool Qualification Report
  - Tool Safety Manual
- ACE SuperTest™ qualification suite
- TI compiler validation test cases
- Test Automation Unit (TAU)
- 24hrs of Validas consulting services
- TÜV Nord assessment report

Approved by TÜV Nord

Systematic
## Typical Usage of Hercules MCU per Functional Safety Standard*

<table>
<thead>
<tr>
<th>Functional Safety Standard</th>
<th>Typical Hercules MCU Usage</th>
<th>Specific Diagnostic Requirements per Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>IEC 61508</td>
<td>Single MCU for SIL1 - SIL 3, Dual MCU for SIL 4</td>
<td>No</td>
</tr>
<tr>
<td>ISO 26262 Automotive</td>
<td>Single Hercules MCU ASIL A to D</td>
<td>No</td>
</tr>
<tr>
<td>EN 50129 Railway</td>
<td>Single MCU for SIL1 - SIL 3, Dual MCU for SIL 4</td>
<td>Examples provided, not requirements</td>
</tr>
<tr>
<td>ISO 22201 Elevator</td>
<td>Single MCU for SIL1 - SIL 2, Dual MCU for SIL 3</td>
<td>Yes</td>
</tr>
<tr>
<td>IEC 61511 Process Safety</td>
<td>Single MCU for SIL1 - SIL 3, Dual MCU for SIL 4</td>
<td>No</td>
</tr>
<tr>
<td>IEC 61800 Motor Drive</td>
<td>Single Hercules MCU for SIL1 - SIL 3</td>
<td>No</td>
</tr>
<tr>
<td>IEC 62061 Machine Safety</td>
<td>Single Hercules MCU for SIL1 - SIL 3</td>
<td>No</td>
</tr>
<tr>
<td>ISO 13849 Machine Safety</td>
<td>Single MCU for Cat B, 1, 2 from PL a to PLe Single MCU + Safety Companion for PL d/e CAT3/4</td>
<td>No</td>
</tr>
<tr>
<td>IEC 60730 White Goods</td>
<td>Single MCU for Class A – C, Dual MCU for some Class C</td>
<td>Yes</td>
</tr>
</tbody>
</table>

* Items shown are typical examples. Achieved safety integrity level is the responsibility of the system developer.
Project Flowchart

exida Analysis Reports
- Gap Analysis Report
- FMEA Report
- FMEDA Report
- Detail FMEDA Sheets
- Fault Injection Test List
- Software Hazop Report
- Communications Safety Report

exida Certification Reports
- Assessment Report
- Certificate

Start Project

Gap Analysis Required?
- Yes: Perform Gap Analysis & Initial Training
- No:
  - Specific Training Required?
    - Yes: Perform Specific Training
    - No: Customer Corrects Gaps

Baseline Safety Case

Final Safety Case

Audit Safety Case

Issue Certification

All Requirements Met?
- Yes
- No:
  - Fault Injection Test List
  - Software Hazop Report

Consultant / Client Documentation
- FSM Plan
- SRS
- Validation Test Plan
- Tool Justification
- Software Process
- Coding Standard
- Software Module Test Plan
- Software Integration Test Plan
- Safety Manual

IEC 61508 Typical Certification Process

✓ Hercules™ MCU data available through SafeTI™ design package
Thank You

Stay tuned for future webinars!

• In-depth discussion of functional safety development and certification flow

• How Hercules™ SafeTI™ documentation facilitates the end equipment certification process?

Contact Information:
Chris O’Brien: cobrien@exida.com
Hoiman Low: hm-low@ti.com