Functional Safety for PLCs and IO Controllers

Christian Herget
System and Application Engineer
Texas Instruments

Christian Dirmeier,
Senior Expert and Trainer
Functional Safety, TÜV SÜD Rail, Munich
Global expertise. Local experience.

Legend:
- Countries with TÜV SÜD offices
- Regional headquarters

Note: Figures have been rounded off, as of 31.12.2015.

<table>
<thead>
<tr>
<th></th>
<th>GERMANY</th>
<th>INTERNATIONAL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Euro 1,283 mio</td>
<td>Euro 939 mio</td>
</tr>
<tr>
<td></td>
<td>11,600 staff</td>
<td>10,800 staff</td>
</tr>
</tbody>
</table>
Safety – Why?
Risk Reduction

- Residual risk
- Acceptable risk
- EUC Risk

Increasing Risk

Necessary Risk Reduction

Actual Risk Reduction

Partial Risk covered by E/E/PE safety related systems

Partial risk covered by other technology safety related systems

Partial risk covered by external risk reduction facilities
Aspects for Risk reduction

The combination of probability of occurrence and severity of hazardous events may not exceed the tolerable risk.

Requirements of reliability of safety related functions necessary to sustain or fulfil the required safety = Functional Safety

Control of dangerous failures during operation → robust design

Avoidance of systematic failures during design, production and operation of the system → robust development process
Hierarchical Structure of Standards

Basic Safety Standards

- TYPE A
  - Basic design guidelines and basic terminology for machinery

Group Safety Standards

- TYPE B
  - B1 Standards: General safety aspects
  - B2 Standards: Reference to special protective devices

Product standards

- TYPE C
  - Specific safety features for individual machinery groups

- EN 692 Machine tools—Mechanical presses

- ISO 12100
- ISO 13849
- IEC 62061
- IEC 61508
- ISO 13850
- EN 692
TÜV SÜD certification process

**Safety Case**
- Requirements for each function: SIL, operation mode/ modi, process safety time, safe state, measure & method
- Checklist Safety Requirement Spec. (SRS)

**Technical Safety Concept**
- System architecture, interface, HFT, SFF goal, conditions of use, maintenance, error handling & diagnosis
- Checklist Safety Requirement Spec. (SRS)

**Functional Safety Concept**
- Requirements for each function: SIL, operation mode/ modi, process safety time, safe state, measure & method
- Checklist Safety Requirement Spec. (SRS)

**Safety Requirement Spec. (SRS)**
- Requirements for each function: SIL, operation mode/ modi, process safety time, safe state, measure & method
- Checklist Safety Requirement Spec. (SRS)

**System-Analysis**
- System-FMEA / FTA
- Checklist System Analysis

**System Test**
- System Test Specification, System Test Reports
- Checklist System Tests

**System Design**
- System architectur, interface, HFT, SFF goal, conditions of use, maintenance, error handling & diagnosis

**Hardware Spec.**
- Hardware SRS
- Checklist HW Spec

**Software Spec.**
- Software SRS
- Checklist Software Spec

**Hardware Design**
- Hardware Analysis
  - FMEDA, ZBD, Markov, SFF, PFH/ PFD
  - Checklist HW Analysis

**Software Design**
- SW Analysis
  - Criticality Analysis
  - Checklist SW-Analysis

**SW Tests**
- SW-Modul Tests
- Checklist SW Tests

**SW-Verification**
- Test spec. + report
- Checklist SW Verification

**Hardware Integration**
- HW-Test
  - Fault Insertion Tests
  - HW/ SW Interface SRS
  - Checklist HW Tests
## Differences between IEC 61508 and ISO 13849 I

<table>
<thead>
<tr>
<th></th>
<th>IEC 61508</th>
<th>EN ISO 13849</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk reduction</td>
<td>SIL</td>
<td>PL</td>
</tr>
<tr>
<td>Safety values</td>
<td>PFD/PFH</td>
<td>MTTF&lt;sub&gt;D&lt;/sub&gt;</td>
</tr>
<tr>
<td></td>
<td>SFF/DC</td>
<td>DC&lt;sub&gt;AVG&lt;/sub&gt; Category</td>
</tr>
<tr>
<td>Common Cause</td>
<td>β, β&lt;sub&gt;D&lt;/sub&gt;</td>
<td>Annex F</td>
</tr>
</tbody>
</table>

Much more like: FPGAs/ASICs, Data Communication, Functional Safety Management, SW Development, Other technologies, Systematic Capability, …
IEC 61508 – probabilistic approach

**Example:**

- **Sensor(s):** Steering sensor / Break sensor
  - SFF<sub>S</sub> / DC<sub>S</sub> (Type, HFT)
  - PFD<sub>S</sub> / PFH<sub>S</sub>

- **Logic:** Control unit incl. Software e.g. PLC
  - SFF<sub>L</sub> / DC<sub>L</sub> (Type, HFT)
  - PFD<sub>L</sub> / PFH<sub>L</sub>

- **Actor(s):** Motor/ Break actuator
  - SFF<sub>A</sub> / DC<sub>A</sub> (Type, HFT)
  - PFH<sub>A</sub>

\[ PFH_{SYS} = PFH_{S} + PFH_{L} + PFH_{A} < PFH_{SIL_X} \]

- PFH: "average frequency of a dangerous failure per hour “
- SFF: Safe Failure Fraction – architecture requirement **per Element**
ISO 13849, Architecture Category 3

Deterministic Approach

Characteristics

• A single fault does not lead to the loss of the safety function
• Accumulation of undetected faults can lead to the loss of the safety function

ISO 13849, 6.2.1:
The designated architectures cannot be considered only as circuit diagrams but also as logical diagrams. For categories 3 and 4, this means that not all parts are necessarily physically redundant but that there are redundant means of assuring that a fault cannot lead to the loss of the safety function.
How does TI help me with my development for ISO 13849?
Architecture for Category 3

Designated architecture for category 3
ISO 13849-1:2015 6.2.1:
The designated architectures cannot be considered only as circuit diagrams but also as logical diagrams. For categories 3 and 4, this means that not all parts are necessarily physically redundant but that there are redundant means of assuring that a fault cannot lead to the loss of the safety function.

Designated architecture for category 3

Diagram showing I1, L1, O1, I2, L2, O2 with arrows and notations.
ISO 13849-1:2015 6.2.1: The designated architectures cannot be considered only as circuit diagrams but also as logical diagrams. For categories 3 and 4, this means that not all parts are necessarily physically redundant but that there are redundant means of assuring that a fault cannot lead to the loss of the safety function.
ISO 13849-1:2015 6.2.1:
The designated architectures cannot be considered only as circuit diagrams but also as logical diagrams. For categories 3 and 4, this means that not all parts are necessarily physically redundant but that there are redundant means of assuring that a fault cannot lead to the loss of the safety function.

Designated architecture for category 3
ISO 13849 Cat3 (PLd) Safety Concept Study

**Generic Architecture**

- **I1**: Input device
- **I2**: Input device
- **L**: Logic (e.g., MCU)
- **TE**: Test Equipment (e.g., intelligent watchdog)
- **O1**: Output device
- **O2**: Output device

Symbols:
- $i_m$: interconnect
- $c$: cross monitor
- $I1, I2$: input device
- $L$: Logic (e.g., MCU)
- $TE$: Test Equipment (e.g., intelligent watchdog)
- $m$: monitoring
- $O1, O2$: output device
ISO 13849 Cat3 (PLd) Safety Concept Study

- TÜV Süd assessed that it is possible to achieve Cat 3 equivalent PL d with a single MCU + external monitor for a specific use case.
- MCU must have multiple logical channels and high diagnostic coverage.
- Assessment report from TÜV Süd is available (SPNU604)

**Generic Architecture**

- **I1, I2**: input device
- **L**: Logic (e.g. MCU)
- **TE**: Test Equipment (e.g. intelligent watchdog)
- **O1, O2**: output device
- **i_m**: interconnect
- **c**: cross monitor
- **m**: monitoring

Diagram:

```
    +----------------+     +----------------+     +----------------+
   /                 |     /                 |     /                 |
  i_m              i_m  /                 |     /                 |
   |                 |     |                 |     |                 |
  |                   |     |                   |     |                   |
  |                   |     |                   |     |                   |
  |                   |     |                   |     |                   |
  |                   |     |                   |     |                   |
  I1  +----------------+     +----------------+     +----------------+
    |                   |     |                   |     |                   |
    |                   |     |                   |     |                   |
    |                   |     |                   |     |                   |
    |                   |     |                   |     |                   |
    +----------------+     +----------------+     +----------------+
           \                     \                     \                     
            T                     T                     T
           |                     |                     |                     |
           |                     |                     |                     |
           |                     |                     |                     |
           |                     |                     |                     |
           |                     |                     |                     |
    +----------------+     +----------------+     +----------------+
   /                 |     /                 |     /                 |
  m                 m  /                 |     /                 |
   |                 |     |                 |     |                 |
  |                   |     |                   |     |                   |
  |                   |     |                   |     |                   |
  |                   |     |                   |     |                   |
  |                   |     |                   |     |                   |
  O1, O2  +----------------+     +----------------+     +----------------+
```

Legend:
- **i_m**: interconnect
- **c**: cross monitor
- **I1, I2**: input device
- **L**: Logic (e.g. MCU)
- **TE**: Test Equipment (e.g. intelligent watchdog)
- **m**: monitoring
- **O1, O2**: output device
ISO 13849 Cat3 (PLd) Safety Concept Study

Generic Architecture

- **I**1, **I**2: input device
- **L**: Logic (e.g., MCU)
- **TE**: Test Equipment (e.g., intelligent watchdog)
- **O**1, **O**2: output device
- \( i_m \): interconnect
- \( c \): cross monitor
- \( i_m \): monitoring

Safe Torque Off use-case

- **RM46L852 MCU**
- **TPS65381 PMIC**
- **Temp Sensor 1**
- **Temp Sensor 2**
- ** Grüne Linie**
- **M**: Monitor Relay 1
- **Relays 1, 2**
- **ENDRV**

TÜV Süd assessed that it is possible to achieve Cat 3 equivalent PLd with a single MCU + external monitor for a specific use case.

- MCU must have multiple logical channels and high diagnostic coverage.
- Assessment report from TÜV Süd is available (SPNU604)
ISO 13849 Cat3 (PLd) Safety Concept Study

**Generic Architecture**

- **i_m** interconnect
- **c** cross monitor
- **I1, I2** input device
- **L** Logic (e.g. MCU)
- **TE** Test Equipment (e.g. intelligent watchdog)
- **m** monitoring
- **O1, O2** output device

**Safe Torque Off use-case**

- **RM46L852**
  - MCU
  - GIOA2
  - HETx (GIO mode)
  - GIOA7 (Enable Diag)
- **TPS65381**
  - PMIC
- **ENDRV**

**TÜV Süd assessed that it is possible to achieve Cat 3 equivalent PL d with a single MCU + external monitor for a specific use case**

- **MCU** must have multiple logical channels and high diagnostic coverage.
- Assessment report from TÜV Süd is available (SPNU604)

- **RM46 + TPS65381** as a possible implementation
- Both TPS and RM46 must drive enable function
- Diverse input and output paths
- Lockstep MCU provides dual logical processing
- MCU monitors all feedback
- TPS monitors MCU
- Customer must confirm for their specific use-case
Hercules MCU functional safety features

- Safe Island Hardware diagnostics

- CPU Self Test Controller requires little S/W overhead
- Memory Protection Unit
- ECC for flash / RAM evaluated inside the Cortex R

- 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

- Physical design optimized to help reduce probability of common cause failure
- Lockstep CPU & Lockstep Interrupt Fault Detection

- ARM® Cortex™ R
- MPU
- ARM® Cortex™ R
- Flash w/ ECC
- RAM w/ ECC
- Flash EEPROM w/ ECC
- Compare Module for Fault Detection
- Memory Protection Unit
- ECC for flash / RAM evaluated inside the Cortex R

- Enhanced System Bus and lockstep Vectored Interrupt Module
- Lockstep CPU
- MPU
- Compare Module for Fault Detection

- Bold items are available only on Cortex-R5 devices
Hercules MCU
functional safety features

- CPU Self Test Controller requires little S/W overhead
- Memory Protection Unit
- ECC for flash / RAM evaluated inside the Cortex R
- Physical design optimized to help 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

- 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

Bold items are available only on Cortex-R5 devices
Hercules MCU functional safety features

- Safe Island Hardware diagnostics
- Blended HW diagnostics
- Non Safety Critical Functions

**CPU Self Test Controller**
- Requires little S/W overhead

**Memory Protection Unit**

**ECC for flash / RAM**
- Evaluated inside the Cortex R

**Physical design optimized**
- To help 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**

**Lockstep CPU**

**ARM® Cortex™ R**

**MPU**

**Compare Module for Fault Detection**

**Memory**
- Flash w/ ECC
- RAM w/ ECC
- Flash EEPROM w/ ECC
- Calibration
- JTAG Debug
- Embedded Trace

**Power, Clock, & Safety**
- OSC PLL
- PBIST/LBIST
- POR
- ESM
- CRC
- RTI/DWWD

**Memory Interface**
- External Memory

**DMA**

**Enhanced System Bus and lockstep Vectored Interrupt Module**

**Serial Interfaces**

**Network Interfaces**

**Dual ADC Cores Available**

**Dual High-end Timers Available**

**GIO**

**Protected Bus and lockstep Interrupt Manager**

**IO Loop Back, ADC Self Test, …**

**Dual ADC Cores with shared channels**

**Error Signaling Module w/ External Error Pin**

**On-Chip Clock and Voltage Monitoring**

**Memory BIST on all RAMS for fast memory test**

**Bold items are available only on Cortex-R5 devices**
TPS65381-Q1 Companion PMIC

- **Functional safety architecture features**
- **Includes multiple power supply rails in a single device**
- **Additional sensor supply built-in**
- **Diagnostic interfaces**

**Features**:
- SAFETY / DIAGNOSTICS
  - BIST
  - Q&A Watchdog
  - Diagnostic State
  - uC Error Monitoring
  - Oscillator Monitoring
  - Voltage Monitoring
  - Loss of lock Monitoring
  - Temp Monitoring
  - Sensor LDO

**Supplies**:
- VIN (6 – 36V)
- 6V @ 1.5A (Pre-regulator)
- 5V @ 300mA (CAN or ADC supply)
- 3.3/5V @ 300mA (uC I/O supply)
- 0.8-3.3V (uC core supply)
- 3.3 – 9.5V @ 100mA (sensor supply)

- SPI Interface
- MUX
- Wake-Up

**Qualifications**:
- AEC 100 qualified and temperature grades to 125°C
Traditional dual channel vs. Lockstep

**Standard Controller Approach**

- **Standard MCU 1**
  - IN1 → Health Check → SW Function → OUT1
  - IN2 → Health Check → SW Function → OUT2

- **Standard MCU 2**
  - IN1 → MCU 2 Monitor → OUT1
  - IN2 → MCU 2 Monitor → OUT2

- **Power Supply**
- **Sensor**
- **Relay**
- **Actuator**

**Hercules Lockstep MCU**

- **Checker CPU**
  - IN1 → SW Function → OUT1
  - IN2 → SW Function → OUT2

- **Functional CPU**
  - IN1 → SW Function
  - IN2 → SW Function

- **TPS 65381 (SafeTI Power Supply)**
- **Sensor**
- **Relay**
- **Actuator**

**Lockstep Controller Approach**

- + Traditional physical 2 channel system
- + MCU component level diversity possible
- - Fault detection depends on software latency
- - Fault coverage depends on software
- - Memory corruption protected by mirroring
- - Extra software developed
  1. CPU Sync
  2. Safety checks
  3. Self Test
- - More components can increase cost, board space, power consumption

- + Fault detection in 2 cycles
- + Hard, Transient, AC faults detected
- + Memory corruption detected by ECC
- + Minimal software developed for safety checks
- + Self Test by Hardware
- + Module level (within MCU) diversity possible
- + Software isolation via Memory Protection Unit
- - Non-traditional logical 2 channel system

**Diagnostics**

- **CCM Core Compare Module**

**Key Features**

- SW Function
- IN1 → OUT1
- IN2 → OUT2
- Enable
- Wdog
- Reset
- nError
- Checker CPU
- Functional CPU
- TPS 65381
- IN1
- CC Core Compare Module
Which documentation is required by IEC 61508 and how can TI help?
Safety manual for compliant items

D.1 General

The purpose of the safety manual for compliant items is to document all the information, relating to a compliant item, which is required to enable the integration of the compliant item into a safety-related system, or a subsystem or element, in compliance with the requirements of this standard.
Safety manual for compliant items

D.1 General
The purpose of the safety manual for compliant items is to document all the information, relating to a compliant item, which is required to enable the integration of the compliant item into a safety-related system, or a subsystem or element, in compliance with the requirements of this standard.

Hercules Device Safety Manual (SM)
- Details product safety architecture and recommended usage
Safety manual for compliant items

D.1 General

The purpose of the safety manual for compliant items is to document all the information, relating to a compliant item, which is required to enable the integration of the compliant item into a safety-related system, or a subsystem or element, in compliance with the requirements of this standard.

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

Safety Analysis Report Summary (SAR1)
- Summary of FIT rate and FMEDA at DEVICE 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
4.4 **Summary of IEC 61508 Safety Metrics at Device Level (BGA Package)**

Table 7 provides estimates of FIT rates and calculated safety metrics IEC 61508-2:2010 using previously noted assumptions for the device in BGA package.

**NOTE:** IEC 61508 beta factor is not currently included in these calculations.

<table>
<thead>
<tr>
<th></th>
<th>Die</th>
<th>Package</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Permanent</td>
<td>Transient</td>
</tr>
<tr>
<td>Total FIT (Raw FIT)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Safety related FIT</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Probability of Hardware Failures - PFH (in FIT)</td>
<td>99.76%</td>
<td>99.11%</td>
</tr>
<tr>
<td>Safe Failure Fraction - SFF</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
What else does TI provide to help me with my development?
SafeTI™ Software Framework

Customer Application

Application Libraries
- Motor
- Flash
- Math DSP

SAFETY RTOS
- USB
- Ethernet
- CAN

Peripheral Drivers (HALCoGen)
(Software Unit)

SafeTI™
Diagnostic Library
(Software Unit)

Hercules™ MCUs

Texas Instruments
SafeTI™ Software Framework

SafeTI™ Software Development Process Certified by TÜV NORD meeting ISO 26262 and IEC 61508 requirements

Customer Application

Application Libraries

SafeTI™ Diagnostic Library (Software Unit)

Motor

Flash

Math DSP

SAFETY RTOS

USB

Ethernet

CAN

Peripheral Drivers (HALCoGen) (Software Unit)

Hercules™ MCUs

SafeTI™ Compliance Support Packages Available
IEC 61508 Software Development Flow

IEC 61508-3:2010-04 Figure 6 – Software systematic capability and the development lifecycle (the V-model)
SafeTI™ CSPs Artifacts

IEC 61508-3:2010-04 Figure 6 – Software systematic capability and the development lifecycle (the V-model)
SafeTI™ Compliance Support Package (CSP)

- Assists customers using Hercules software components to comply to functional safety standards
- SafeTI software development process certified by TUV NORD to IEC 61508 and ISO 26262
- CSPs Include:
  - Documentation:
    - Safety Requirements
    - Safety Manual
    - Static and Dynamic test results
    - Code coverage reports
    - MISRA-C results
    - Traceability report
  - Unit Test Capability:
    - TI Unit Level Test Cases
    - Test Automation Unit (TAU) based on LDRAunit®
- Available NOW! for HALCoGen and SafeTI Hercules Diagnostic Library
  - [www.ti.com/tool/safeti-halcogen-csp](http://www.ti.com/tool/safeti-halcogen-csp)
  - Customers can download the demo or submit request for production version

SafeTI Compliance Support Packages available now!
SafeTI™ Compiler Qualification Kit

- Assists in qualifying TI C/C++ Compilers to functional safety standards
- Flexible integration into development processes due to the model-based qualification method
- 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
- Solid Sands SuperTest™ qualification suite
- TI compiler validation test cases
- Test Automation Unit (TAU)
- 24hrs of Validas consulting services
- TÜV Nord assessment report

http://www.ti.com/tool/safeti_cqkit
What are Hercules™ ARM® Cortex®-R Microcontrollers?

www.ti.com/Hercules

Broad MCU Portfolio
• 80MHz to 330MHz ARM® Cortex®
• 128kB to 4MB Flash
• 32kB to 512kB RAM

Handling of Systematic and Random Faults
• Certified Development Flow
• Integrated diagnostics to help detect random faults

Certification
• Hercules MCUs
• H/W development process
• S/W development process

Time To Market
• Hardware Features
• Software Compliance Support Packages
• Safety Documentation

www.ti.com/SafeTI