Choose certainty.
Add value.

Technical Report

on the

Concept Study

of a

Safety Architecture

Manufacturer:

Texas Instruments Incorporated
12201 Southwest Freeway
Stafford TX 77477
USA

Report no. TF85875T

Revision 1.0 of 2014-06-18

Test Laboratory

TÜV SÜD Rail GmbH
Barthstrasse 16
D-80339 Munich

This technical report may be represented 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.

Table of Contents

Revision history

Revision	Status	Date	Author	Changed chapters	Reason of change
1.0	Initial	2014-06-18	M. Ramold / W. Velten-Philipp / G. Neumann		

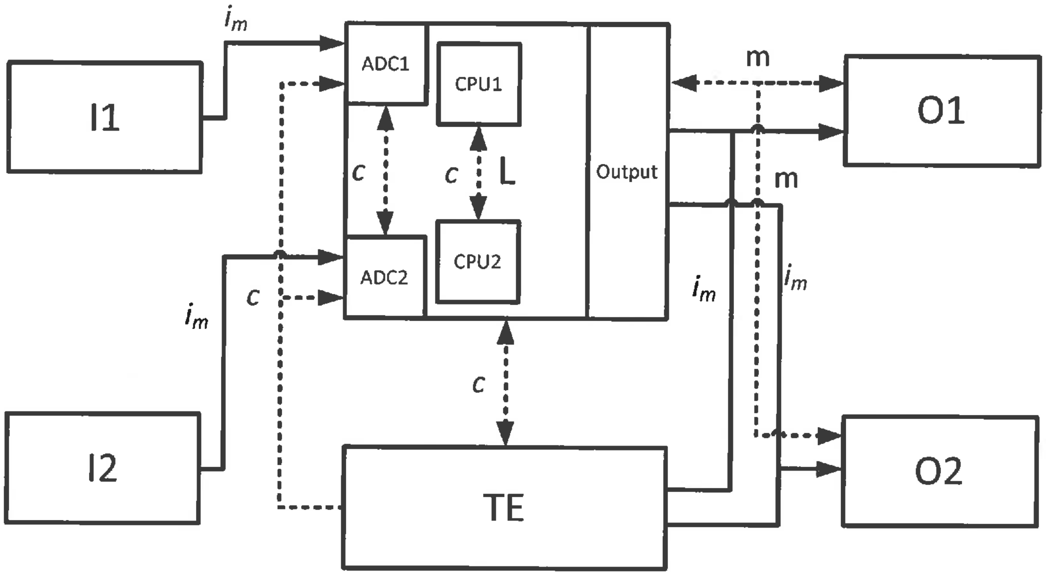
Table 1: Revision history

1 Target of Evaluation

In June, 2011 Texas Instruments Incorporated requested TÜV SÜD Rail GmbH to participate at a concept study. The Project No. related to this Technical Report was as follows: 717505473.

1.1 Scope of Testing

Target of the concept study is to evaluate if it is feasible to reach an equivalent risk reduction of category 3 according to EN ISO 13849-1:2008 with a safety architecture consisting of a microcontroller device with on-chip safety integrity measures and an external supply and monitoring device. An overview of the principle Safety architecture is shown in figure 1.



Dashed lines represent measures to detect faults

Key	
i_m	interconnecting means
c	cross monitoring
I1, I2	input device, e.g. temperature sensor
L	logic, e.g. MCU
TE	test equipment, e. g. intelligent watchdog
m	monitoring
O1, O2	output device, e.g. relay

Figure 1: Block diagram of safety architecture

The safety function is executed by a microcontroller. The microcontroller has on-chip implemented safety integrity measures. Furthermore the microcontroller is monitored by external test equipment / external device. The intended safety architecture does not comply with the designated architecture according to EN ISO 13849-1:2008 for category 3. Therefore a concept study was set up to evaluate if it is feasible to reach an equivalent risk reduction of category 3 according to EN ISO 13849-1:2008.

1.2 Basis of the evaluation

The concept study was based on the documents listed in clause 3 of this report.

2 Basis of Evaluation

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

2.1 Functional Safety

No.	Standard	Title
[N1]	EN ISO 13849-1: 2008 (Category 3)	Safety of machinery - Safety-related parts of control systems Part 1: General principles for design
[N2]	IEC 61508-2: 2010 (SIL 2)	Functional safety of electrical/electronic/programmable electronic safety-related systems Part 2: Requirements for electrical/electronic/ programmable electronic safety-related systems
[N3]	BGIA Report 2/2008	Functional safety of machine controls – Application of EN ISO 13849 -

Table 2: Functional Safety

3 Documents provided for review

The following documents were provided by Texas Instruments Incorporated:

No.	Title	Document-No./ File identifier	Revision	Date
[D1]	ISO13849 Safety Analysis	ISO13849 Safety Analysis v0.15 Draft.xlsx	0.15	2014-03-27

Table 3: Documents provided for review

4 Performance and result of tests

4.1 Test reports

Following test reports were issued by TÜV SÜD Rail GmbH or other accredited test laboratories.

No.	Title	Document-No./ File identifier	Revision	Date
[R1]	Minutes of meeting	MoM_TI_21062012.docx	1.0	2012-06-21
[R2]	Minutes of meeting	MoM_TI_Concept Study_2013_07_18.docx	1.0	2013-07-18
[R3]	Review report	Concept_Study_TI_2014_03_10_draft.docx	3.0	2014-03-10
[R4]	Minutes of meeting	Workshop Kat 3 vs. HFT 61508 20130719.docx	1.0	2013-07-19

Table 4: Documents from Testing Agency

5 Result of the concept review

5.1 Approach of the concept study

For the evaluation of the safety architecture for equivalence related to category 3 of [N1] an example application was defined. The impact of faults on this safety function and the control of different fault scenarios according to [N1] and [N2] was analyzed with a Failure Mode and Effects Analysis (FMEA). Within this FMEA diagnostic measures and timing aspects have been regarded.

Result:

Based on [D1], [N3] and [R4] the following main criteria have been identified for reaching the equivalence of category 3 according to [N1]:

- The system and its components comply with a systematic capability (SC) ≥ 2 according to IEC 61508:2010 including measures to control and avoid systematic faults
- The safety function is performed in a high demand or continuous demand mode and has a defined safe state
- Faults are detected and the safe state is achieved within the process safety time
- An independent achievement of the safe state is ensured by a mandatory monitoring device
- An independent supervision of the execution of the on-chip safety mechanism is ensured
- An additional diagnostic ability like using information redundancy is provided by the application
- For each safety relevant element a combination of (minimum two) diagnostic measures has to be implemented. At least one of these diagnostic measures has to provide a diagnostic coverage of high. The following safety measures have been regarded in the concept study:
    - Information redundancy techniques supported by the application
    - Independent fault detection by the monitoring device
    - On-chip hardware implemented diagnostic measures with fault indication to the monitoring device
    - By software implemented diagnostic measures with fault indication to the monitoring device
- Measures against common cause failures covering the different devices
- Measures against common cause and cascading failures covering on-chip elements
- Limitation of usage up to performance level d
- Integration and verification has to be done according to the applied safety standards including functional safety management and lifecycle handling

The reaching of equivalence to category 3 according to [N1] has to be evaluated for each safety function separately.

TÜV SÜD Rail GmbH
Embedded Systems

i.V.
M. Ramold

i.A.
G. Neumann

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATA SHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, regulatory or other requirements.

These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you will fully indemnify TI and its representatives against, any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI’s products are provided subject to TI’s Terms of Sale or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI’s provision of these resources does not expand or otherwise alter TI’s applicable warranties or warranty disclaimers for TI products.

TI objects to and rejects any additional or different terms you may have proposed.

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265
Copyright © 2022, Texas Instruments Incorporated