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

Table of Contents

Revision history 3
1 Target of Evaluation 4
1.1 Scope of Testing 4
1.2 Basis of the evaluation 4
2 Basis of Evaluation 5
2.1 Functional Safety 5
3 Documents provided for review 6
4 Performance and result of tests 6
4.1 Test reports 6
5 Result of the concept review 7
5.1 Approach of the concept study 7

Revision history

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

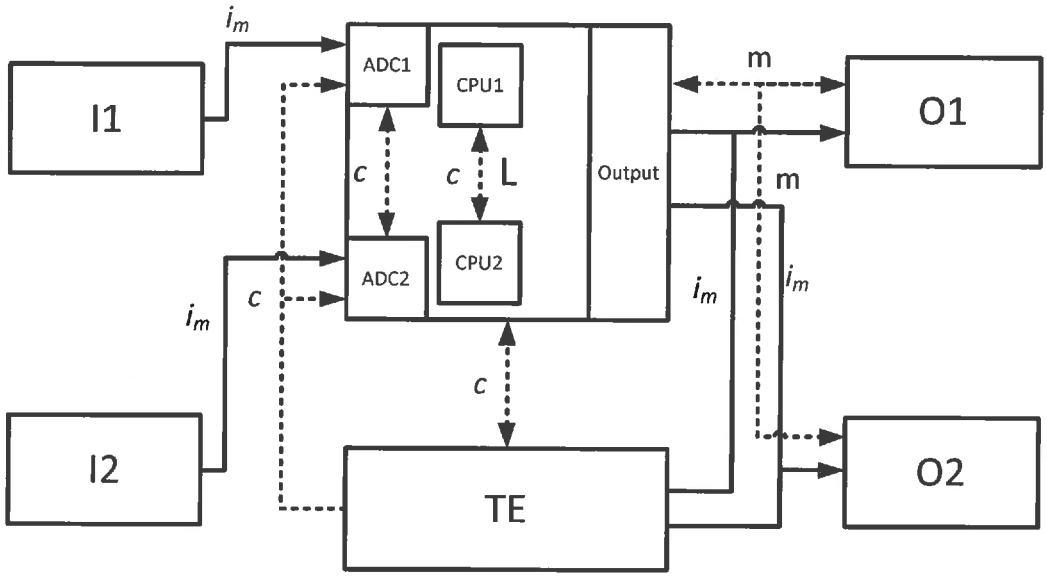
Table 1: Revision history

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 micro-controller 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	Con-cept_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

Texas Instruments Incorporated and its subsidiaries (TI) reserve the right to make corrections, enhancements, improvements and other changes to its semiconductor products and services per JESD46, latest issue, and to discontinue any product or service per JESD48, latest issue. Buyers should obtain the latest relevant information before placing orders and should verify that such information is current and complete. All semiconductor products (also referred to herein as “components”) are sold subject to TI’s terms and conditions of sale supplied at the time of order acknowledgment.

TI warrants performance of its components to the specifications applicable at the time of sale, in accordance with the warranty in TI’s terms and conditions of sale of semiconductor products. Testing and other quality control techniques are used to the extent TI deems necessary to support this warranty. Except where mandated by applicable law, testing of all parameters of each component is not necessarily performed.

TI assumes no liability for applications assistance or the design of Buyers’ products. Buyers are responsible for their products and applications using TI components. To minimize the risks associated with Buyers’ products and applications, Buyers should provide adequate design and operating safeguards.

TI does not warrant or represent that any license, either express or implied, is granted under any patent right, copyright, mask work right, or other intellectual property right relating to any combination, machine, or process in which TI components or services are used. Information published by TI regarding third-party products or services does not constitute a license to use such products or services or a warranty or endorsement thereof. Use of such information may require a license from a third party under the patents or other intellectual property of the third party, or a license from TI under the patents or other intellectual property of TI.

Reproduction of significant portions of TI information in TI data books or data sheets is permissible only if reproduction is without alteration and is accompanied by all associated warranties, conditions, limitations, and notices. TI is not responsible or liable for such altered documentation. Information of third parties may be subject to additional restrictions.

Resale of TI components or services with statements different from or beyond the parameters stated by TI for that component or service voids all express and any implied warranties for the associated TI component or service and is an unfair and deceptive business practice. TI is not responsible or liable for any such statements.

Buyer acknowledges and agrees that it is solely responsible for compliance with all legal, regulatory and safety-related requirements concerning its products, and any use of TI components in its applications, notwithstanding any applications-related information or support that may be provided by TI. Buyer represents and agrees that it has all the necessary expertise to create and implement safeguards which anticipate dangerous consequences of failures, monitor failures and their consequences, lessen the likelihood of failures that might cause harm and take appropriate remedial actions. Buyer will fully indemnify TI and its representatives against any damages arising out of the use of any TI components in safety-critical applications.

In some cases, TI components may be promoted specifically to facilitate safety-related applications. With such components, TI’s goal is to help enable customers to design and create their own end-product solutions that meet applicable functional safety standards and requirements. Nonetheless, such components are subject to these terms.

No TI components are authorized for use in FDA Class III (or similar life-critical medical equipment) unless authorized officers of the parties have executed a special agreement specifically governing such use.

Only those TI components which TI has specifically designated as military grade or “enhanced plastic” are designed and intended for use in military/aerospace applications or environments. Buyer acknowledges and agrees that any military or aerospace use of TI components which have ***not*** been so designated is solely at the Buyer's risk, and that Buyer is solely responsible for compliance with all legal and regulatory requirements in connection with such use.

TI has specifically designated certain components as meeting ISO/TS16949 requirements, mainly for automotive use. In any case of use of non-designated products, TI will not be responsible for any failure to meet ISO/TS16949.

Products		**Applications**	
Audio	www.ti.com/audio	Automotive and Transportation	www.ti.com/automotive
Amplifiers	amplifier.ti.com	Communications and Telecom	www.ti.com/communications
Data Converters	dataconverter.ti.com	Computers and Peripherals	www.ti.com/computers
DLP® Products	www.dlp.com	Consumer Electronics	www.ti.com/consumer-apps
DSP	dsp.ti.com	Energy and Lighting	www.ti.com/energy
Clocks and Timers	www.ti.com/clocks	Industrial	www.ti.com/industrial
Interface	interface.ti.com	Medical	www.ti.com/medical
Logic	logic.ti.com	Security	www.ti.com/security
Power Mgmt	power.ti.com	Space, Avionics and Defense	www.ti.com/space-avionics-defense
Microcontrollers	microcontroller.ti.com	Video and Imaging	www.ti.com/video
RFID	www.ti-rfid.com		
OMAP Applications Processors	www.ti.com/omap	**TI E2E Community**	e2e.ti.com
Wireless Connectivity	www.ti.com/wirelessconnectivity		

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265