Rail

Add value.
Inspire trust.

# Technical Report

on the

# Concept

of the

# Safety Component

# Safe Torque Off (STO)

**Manufacturer**

Texas Instruments

Haggertystrasse 1
85356 FREISING
GERMANY

**Report No. TF97657T**

Revision 1.1 of 09.02.2022

**Test Laboratory**

TÜV SÜD Rail GmbH
Rail Automation
Barthstrasse 16
D-80339 München

# Table of Contents page



# List of tables page



# List of figures page

## Revision history

| Rev. | Status | Date | Author | Modification / Description |
|---|---|---|---|---|
| 1.1 | Replaced | 15.11.2021 | A.Valente | Initial |
| 1.1 | Active | 09.02.2022 | A.Valente | Minor typo corrections |

Table 1: Revision History

## Acronyms and Abbreviations

| Abbreviation | Description |
|---|---|
| ASIL | Automotive Safety Integrity Level |
| CAT | Category |
| DC | Diagnostic Coverage |
| FMEDA | Failure Mode, Effects and Diagnosis Analysis |
| FSM | Functional Safety Management |
| $MTTF_D$ | Mean Time To Dangerous Failure |
| PFD | Probability of Dangerous Failure on Demand |
| PFH | Average Frequency of Dangerous Failure ($h^{-1}$) |
| PL | Performance Level |
| QMS | Quality Management System |
| SFF | Safe Failure Fraction |
| SIL | Safety Integrity Level |
| SILCL | SIL Claim Limit |
| ToE | Target of Evaluation |

Table 2: Acronyms and Abbreviations

# 1 Scope

Scope of this report is the concept approval for the Safety Component Safe Torque Off (STO) module for a reinforced isolated 3-phase inverter with isolated smart gate drivers from Texas Instruments. The Safe Torque Off (STO) is specified and described by the concept document [D1].

The Safe Torque Off (STO) module provides safety function according to SIL 3 / PL e / CAT 3 of the safety standards mentioned in chapter 2.1 .

## 1.1 Description of the Safe Torque Off (STO) concept

The Safe Torque Off (STO) has a dual channel architecture (1oo2), it is implemented following a de-energize to trip concept, when STO inputs (STO 1 and STO 2) go low the power supply to the primary and the secondary side of the isolated gate driver is cut in less than 10ms (typical), removing the possibility to control and energize the motor.

The MCU responsible for the diagnostic mechanisms is not in the scope of this report.

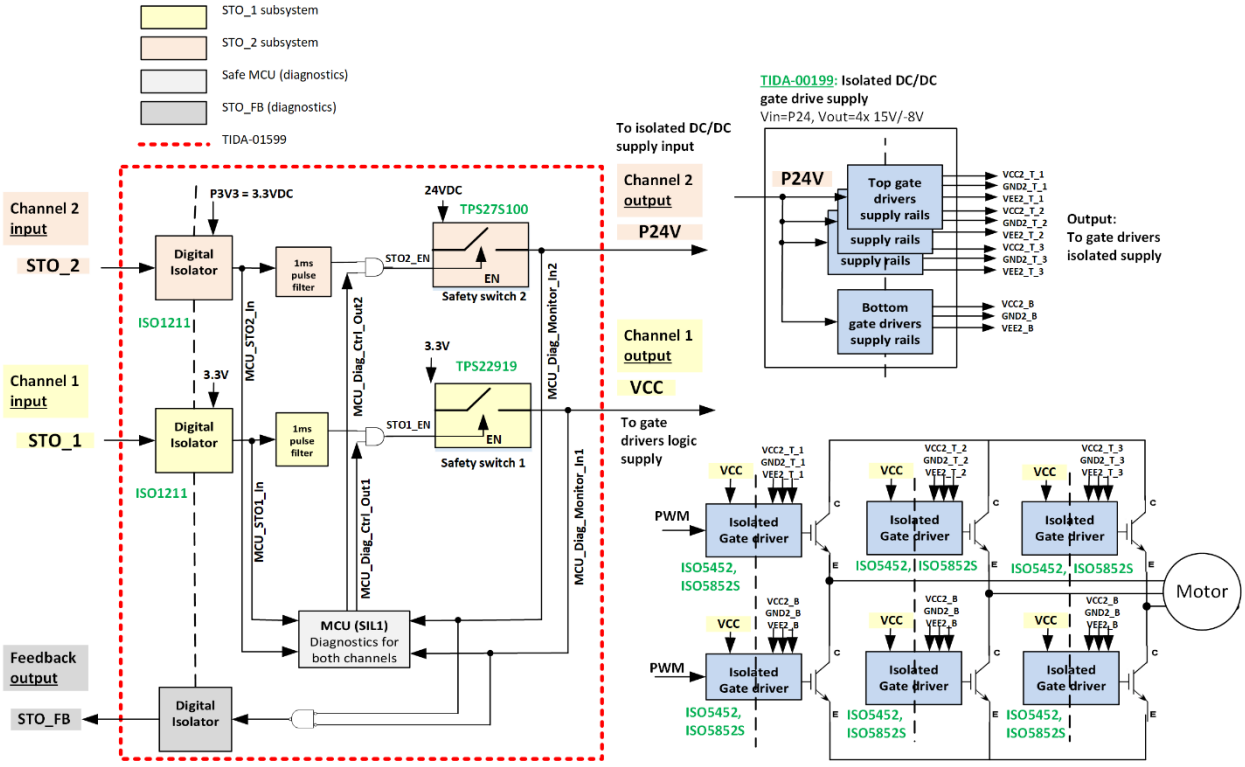


Figure 1: STO architecture

### 1.2 Basis of the Approval

The approval of the safety concept bases on the documents listed in clause 3 of this report. The concept was examined according to the standards and guidelines listed by clause 2 of this report. The following aspects were reviewed:

- Functional safety
  - Analysis of the concept and system structure
  - Review of block FMEA

# 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] | IEC 61508-1: 2010<br>(SIL 3) | Functional safety of electrical/electronic/programmable electronic safety-related systems<br>Part 1: General requirements |
| [N2] | IEC 61508-2: 2010<br>(SIL 3) | Functional safety of electrical/electronic/programmable electronic safety-related systems<br>Part 2: Requirements for electrical/electronic/ programmable electronic safety-related systems |
| [N3] | IEC 61508-4: 2010<br>(SIL 3) | Functional safety of electrical/electronic/programmable electronic safety-related systems<br>Part 4: Definitions and abbreviations |
| [N4] | EN ISO 13849-1: 2015<br>(PL e, Cat. 3) | Safety of machinery - Safety-related parts of control systems<br>Part 1: General principles for design |

Table 3: Functional Safety

### 2.2 Quality Management System

| No. | Reference | Description |
|---|---|---|
| [M1] | QMS | Quality Management System TÜV SÜD Rail GmbH |
| | TR_RA_P_04.50 | Test Program Functional Safety<br>TR_RA_P_04.51Definition Scope of testing<br>TR_RA_P_04.07Product Modification<br>TR_RA_P_04.52Concept Phase & Safety Lifecycle<br>TR_RA_P_04.53Detail Phase Hardware<br>TR_RA_P_04.54Detail Phase Software<br>TR_RA_P_04.55Safety Manual<br>TR_RA_P_04.56Result of Testing |
| [M2] | D-IS-11190-01-00 | DAkkS accreditation according to DIN EN ISO/IEC 17020:2012; inspection body type A |

| No. | Reference | Description |
|---|---|---|
| [M3] | D-PL-11190-08-00 | DAkkS accreditation according to DIN EN ISO 17025:2018 / EN ISO/IEC 17025:2017 |

Table 4: Quality Management System

# 3 Documents provided for the concept review

The following documents were provided by Texas Instruments as basis for the concept evaluation.

| No. | Title | Document-No./ File identifier | Revision | Date (yyyy.mm.dd) |
|---|---|---|---|---|
| [D1] | Safety concept | TIDA-01599_STO_Concept _FMEA_1v6 | 1.6 | 2021.11.11 |
| [D2] | FMEA | TIDA_01599_STO_Concept _FMEA_1v6 | 1.6 | 2021.11.11 |
| [D3] | Schematic | TIDA-01599E2.1(001)_Sch | E2.1 | - |

Table 5: Documents from Customer

# 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] | Review protocol | Review Protocol_Concept V1.3 | 1.3 | 2021.11.15 |

Table 6: Documents from Testing Agency

# 5 Result of the concept review

## 5.1 Project Management

Functional safety management is not in the scope of this evaluation. Life cycle is under the responsibility of the user of Texas Instruments concept design.

## 5.2 Safety Function and Specification

The documents [D1] and [D2] describe the safety requirements and safety function of the unit. Following safety functions have been identified:

- Safe Torque Off (STO)

All safety functions shall comply with the requirements of the standards mentioned in chapter 2.

**Result:**

The documents are sufficient to specify and to describe the safety concept of the device.

## 5.3 Analysis of system architecture

The Safe Torque Off (STO) hardware architecture consists mainly of a two-channel structure for the logic and the in- and outputs components, see [D1] and [D2].

The basic diagnostic principles are:

- Self-tests (not in scope, to be implemented by the end user)

**Result:**

The hardware architecture (1oo2) is generally suitable for SIL 3 / PL e / CAT 3 . The architecture, the effectiveness of the selected diagnostic measures and diagnostic test interval need to be re-evaluated in the context of the final implementation.

## 5.4 Block-FMEA

The manufacturer provided a block-based System-FMEA [D2]. The FMEA considers the relevant failure modes for all electronic elements and analyses the failure effects.

**Result:**

The FMEA demonstrates that the requirements of SIL 3 / PL e / CAT 3 could be achieved.

The effectiveness of the selected diagnostic measures needs to be re-evaluated in the context of the final implementation.

# 6 Summary

The Safety Component Safe Torque Off (STO) from Texas Instruments is capable to support safety architectures in accordance to SIL 3 / PL e / CAT 3 of the standards mentioned in chapter 2.1.

Implementation of internal diagnostic, integration and verification have to be done according to the applied safety standards including functional safety management and lifecycle handling.

Technical Certifier

Digital unterschrieben von Matthias Ramold
Datum: 2022.02.14 12:46:00 +01'00'

M.Ramold

Project Manager

Digitally signed by Andrea Valente
Date: 2022.02.10 15:46:58 +01'00'

A.Valente

# 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