Functional Safety Information

TCAN1167-Q1
Functional Safety Analysis Report Summary

Table of Contents

Trademarks

1 Introduction

This document is a Safety Analysis Report for the Texas Instruments TCAN1167-Q1. Device numbers covered by this Safety Analysis Report include the following products:

- TCAN1167-Q1

The following information is documented in the *Device Safety Manual*, and will not be repeated in this document. This document will be referred to as the *Safety Manual* through the remainder of this document.

- An overview of the superset product architecture
- An overview of the development process utilized to reduce systematic failures
- An overview of the safety architecture for management of random failures
- The details of architecture partitions and implemented safety mechanisms

The following information is documented in the *Safety Report* and will not be repeated in this document:

- Results of assessments of compliance to targeted standards

The user of this document should have a general familiarity with the TCAN1167-Q1. This document is intended to be used in conjunction with the pertinent data sheets, technical reference manuals, and other documentation for the products under development.

The following functional safety analyses are described in this document:

- Hardware component FMEDA (Failure Modes Effects and Diagnostics Analysis) - The complete FMEDA will be provided in a separate Excel document. The assumptions made in the FMEDA and the settings for tailoring the FMEDA to a specific application are described in this document.

2 Hardware Component Failure Modes Effects and Diagnostics Analysis (FMEDA)

This section describes the device FMEDA, the assumptions made within, the options for tailoring, and provides an example calculation of device functional safety metrics.

2.1 Random Fault Estimation

In order to conduct quantitative failure analysis, estimates of the random failure rates for the components that will be considered in the analysis must be generated. There are many different models and techniques that can be used for failure rate estimation. Neither IEC 61508 nor ISO 26262 mandate the use of a particular failure estimation methodology. Estimation methods commonly used include:

- IEC/TR 62380:2004, "Reliability Data Handbook - Universal Model for Reliability Prediction of Electronics, PCBs, and Equipment"
- Siemens Norm SN29500:2010, "Failure Rates of Components"
- IEC 61709:2017, "Electric components - Reliability - Reference conditions for failure rates and stress models for conversion"
- Supplier reliability data from similar products already in production and deployed under similar operating conditions
- Targeted studies and experiments that seek to induce failures on silicon under conditions that simulate accelerate lifespan (such as temperature, voltage, frequency, vibration, humidity, or radiation exposure).

Estimations of failure rate are often defined in terms of Failures In Time (FIT). TI's data respects FIT in terms of failures per 10^9 hours of operation, as is consistent with most handbooks. However, certain handbooks, such as those for military applications, may refer to FIT based on failures per 10^6 hours of operation. Take care when using such data to respect a common definition of FIT in all calculations.

In TI's experience, all of the models generate estimations of failure rate that are not consistent with failure rates which are observed and reported in the field or predicted based on data generated from targeted experiments. The models consistently predict higher failure rates than those observed in the field or predicted via targeted experiments. One possible reason for this discrepancy is that these standards consider reliability data that does not make a distinction between random and systematic failure. In both IEC 61508 and ISO 26262, the focus for quantitative analysis is on random failure rate. TI's data indicates that the vast majority of field failure issues seen in semiconductors are due to systematic failures, whether traced to semiconductor supplier, system integrator, or end user. TI has quality and reliability programs in place that constantly improve our products and processes to reduce these systematic failures.

The failure rates derived from SN29500 tend to be conservative as compared to TI product field failure rate data or TI accelerated lifetime testing. TI considers the IEC 61709 to be similar to the SN29500 and we refer to this model as the IEC 61709/SN29500 model in the FMEDA. The IEC/TR 62380, while still conservative, provides the closest match available to TI product data. Although this standard has been formally withdrawn, the equations have been incorporated inside ISO 26262-11:2018 section 4.6.2. As such, TI has used IEC/TR 62380 as the basis for our random failure rate estimation, augmented with data from targeted studies for failure modes not considered in the base model.

When considering failure rates for semiconductors, TI applies the following partition and methodology:

Table 2-1. Summary of TI Random Failure Rate Estimation

Design Element	Failure Mode	Estimation Method
Device Packaging	Permanent faults	IEC/TR 62380
Die (silicon)	Permanent faults	IEC/TR 62380
Die (silicon)	Transient faults (soft error)	Targeted radiation exposure

2.1.1 Fault Rate Estimation Theory for Packaging

TI uses the IEC/TR 62380 model to estimate package FIT rate for the DMT package used for this device. The IEC/TR 62380 package model is primarily concerned with wear-out due to thermal expansion between the package and the PCB. The model includes several variables that have been replaced with device-specific data when available, such as power consumption and package thermal characteristics. It is highly recommended that the user applies their own application mission profile in the 'Mission Profile Tailoring' tab as this has a

large impact on the base package FIT rate. The automotive motor control profile is used as the default in TI's estimates.

Note

TI field data in high volume automotive and industrial applications indicates a random package failure rate and a silicon permanent fault rate that is at least two orders of magnitude lower than the estimates generated using the IEC/TR 62380. TI devices are designed with a high degree of margin to the wear out failure mechanisms respected in IEC/TR 62380; most applications will not approach the wear-out limits within product lifetime. It has also been argued that wear-out mechanisms should be considered a systematic failure mode and as such should not be included in safety metric analysis. Data generated using the IEC/TR 62380 standard should be considered conservative estimates.

2.1.2 Fault Estimation Theory for Silicon Permanent Faults

TI uses the IEC/TR 62380 model to estimate FIT rate due to silicon permanent faults. The IEC/TR 62380 model focuses primarily on gate oxide integrity type faults that are accelerated by voltage and temperature. This is a traditional approach to semiconductor fault modeling, as gate oxide failure is a primary wear-out mechanism. However, in recent product generations additional failure modes have become significant and are not always accelerated by the same conditions as a gate oxide failure. JEDEC JEP122G, "Failure Mechanisms and Models for Semiconductor Devices", can provide additional details. Management of these failure modes may require additional testing and diagnostics, which are not well comprehended in IEC 61508:2010 and ISO 26262:2011.

TI's application of the IEC/TR 62380 model follows the guidance found in ISO 26262-11:2018. Permanent faults are separated into five classes, each estimated with a separate intrinsic FIT rate: MOS digital circuits, low-power consumption SRAM, ROM, block erasable flash, and low voltage linear (analog). The process FIT factor of the five circuitry types is averaged, as the standard does not comprehend a process that allows integration of digital, analog, ROM, SRAM, and flash. Please note that some devices may not have every category listed above, in that case, the absent categories are excluded from the calculation. The automotive motor control profile is used as default in TI's estimates.

2.1.3 Fault Estimation Theory for Silicon Transient Faults

TI uses experimental data collected on process test chips to estimate silicon transient faults. Other data from vendors and foundries may also be used in this calculation, depending on the process technology used for the device. TI has been conducting targeted radiation exposure testing on process test chips since 2000 and is considered an industry leader in this area. TI's data correlates strongly to estimates for soft error provided in the International Technology Roadmap for Semiconductors (ITRS). At present, TI is not aware of any failure estimation standard that includes models to estimate FIT rate for transient faults.

Data taken on test chips has been utilized to establish base failure rates for single event upset (SEU) on SRAM bits and sequential digital logic. A further estimation is made for single event transient (SET) events for combinatorial logic. This failure mode is theoretically possible but TI has not been able to generate this failure mode in any testing done to date. ROM, analog, and package FIT have no contribution to transient faults and are therefore excluded from this calculation.

SEU failure rates consider exposure to two elementary particles: alphas and neutrons. Alpha particle exposure occurs primarily from radioactive material in the package mold compound. Low-alpha mold compound is utilized to minimize this failure rate. Neutron particle exposure is primarily due to cosmic particles bombarding the Earth. The altitude of operation and location on the Earth have impact on the rate of exposure, with high altitude locations near the equator having worst exposure. There is no effective way to manage neutron particles other than operation of the unit behind several feet of lead, water, or similar barrier. All of the estimations used in this report are based on JEDEC JESD89A, *Measurement and Reporting of Alpha Particle and Terrestrial Cosmic Ray Induced Soft Errors in Semiconductor Devices*, with assumption of neutron flux = 1 (measured exposure to neutrons as seen at sea level in New York City, USA).

2.1.4 The Classification of Failure Categories and Calculation

TI uses ISO 26262-10, Figure 9 as the basis for all FMEDA calculations. Each of the rows in the FMEDA is given a portion of the overall device failure rate based on its transistor count or area (package FIT is calculated separately based on the number of device pins). Then based on the selections that are made in Section 2.2.3,

the FMEDA will categorize the failure rate accordingly. The user can see the details of this categorization in the 'Details - ISO26262' tab.

2.2 Using the FMEDA Spreadsheet Tool

A FMEDA is a common functional safety analysis technique used to determine the effectiveness of a functional safety architecture. For failure modes of the design blocks identified, a probability of occurrence is quantified. For diagnostics implemented, the effectiveness of the diagnostic is quantified. The quantification of these values enables the calculation of safety metrics per targeted functional safety standards such as the IEC 61508 safe failure fraction or the ISO 26262 single point fault metric, which estimates the effectiveness of the implemented safety architecture.

TI has created a FMEDA for this device that allows the user to tailor the metrics to their specific use case based on which features or design blocks are being used as part of the safety function. This tool additionally allows the user to modify the environmental factors, device power consumption, and other factors that affect the raw (base) FIT rates. Finally, this tool allows the user to customize the diagnostics that are applied that can detect faults within the device itself. All of the green cells in the spreadsheet can be modified by the user. All other cells have been populated by TI based on the specifics of the device or are calculated based on the user selections. This Excel workbook is locked to protect the user from incorrectly modifying the calculations. The sections below go into detail on how to use these tailoring options. Any tab not mentioned below is informational.

See Section 2.3.1 for the default values of these fields in this device's FMEDA.

2.2.1 Mission Profile Tailoring Tab

The user is expected to tailor this sheet to their specific use-case.

This section describes the steps needed to configure the 'Mission Profile Tailoring' tab of the device FMEDA for a specific application or use-case. All of the selections that can be made in this tab will impact the raw (base) FIT rate of the device or the safety related FIT of the device.

2.2.1.1 Confidence Level

The confidence level field sets the probability that the data calculated in the FMEDA spreadsheet will fall within the specified range of values. In short, the higher the confidence level, the more conservative the data. The user may scale this confidence level, to match the FIT calculation for other components in their system. The lower the confidence level, the smaller the raw (base) FIT rate will be. TI gives the user the ability to adjust the permanent FIT confidence level separately from the transient FIT confidence level.

2.2.1.2 Geographical Location

The relative neutron flux field sets the radiation exposure rates relative to a certain elevation in the world. The user may alter these assumptions to meet their specific use case. The higher the relative neutron flux, the larger the raw (base) transient FIT rate will be.

2.2.1.3 Life Cycle

The default vehicle lifetime field sets the amount of hours the vehicle (or system) is in use. This field is not directly used in the FMEDA calculation, however in conjunction with the on time (Ton), this sets the total Power On Hours (POH) which is directly used in the calculation of the raw (base) FIT rate of the device. The user may alter this assumptions to meet their specific use case. The longer the vehicle lifetime, a larger number of Power On Hours (POH) will be used in the calculation resulting in a larger the raw (base) FIT rate. Please note that for many automotive and industrial devices, this increase in raw (base) FIT rate will be too small to be observable in the 'Totals' tabs.

2.2.1.4 Use Case Thermal Management Control (Theta-Ja) and Use Case Power

There are several inputs related to thermal management and use case power consumption. TI has assumed a thermal management strategy and use-case power. The user may alter these assumptions to meet their specific use case. The most critical parameter to result from these equations is the maximum junction temperature. Be sure not to exceed the maximum junction temperature rating of the component. The higher the junction temperature, the larger the raw (base) FIT rate will be.

2.2.1.5 Safe vs Non-Safe (Safe Fail Fraction) for Each Component Type

For each failure mode of a fundamental design element, a determination should be made as to whether the failure is safe or dangerous. Safe failures do not result in a loss of the safety function or violation of a safety goal (this can include failure to perform the safety function so long as the design fails into the pre-defined safe state). Dangerous failures result in a loss of safety function or violation of a safety goal.

The usage the ratio safe versus dangerous failures varies based on the system's utilization of the hardware. In many systems, it is not feasible for the system integrator to prove the safe versus dangerous ratio due to technical complexity, design visibility and the time necessary for exhaustive testing. To manage this concern, a probabilistic approach can be taken, in which a ratio of safe versus dangerous failures is estimated. Many standards suggest that this ratio can be set to 50% safe and 50% dangerous if no detailed data is available. TI has conservatively used a 50% safe failure estimate for transient faults of the SRAM, digital logic, and Flash memory. All other faults are considered to be 0% safe. The user may alter these assumptions to meet their specific use case. These selections will impact the "Safety related FIT" for permanent, transient, and package.

2.2.1.6 Analog FIT Distribution Method

This section is informational only, there is no user input required. IEC62380 and SN29500 use the total Mbit and/or transistor count to determine a base level FIT. If "Transistor" is selected, we proportion out the Analog FIT based on its raw transistor count. If "Area" is selected, we proportion out the FIT rate based on the part's relative size to the chip. This does not change the overall Base FIT of the device, just the distribution of the Base FIT.

2.2.1.7 Operational Profile

The operational profile has a set of inputs to configure the thermal environment expected for the component. TI has made an assumption about the expected ambient temperatures of a typical use case - for example the IEC62380 Motor Control Profile. The user may alter these assumptions to meet their specific use case. The ambient temperature combined with the power consumption increases the junction temperature, which in turn, increases the raw (base) FIT rate.

2.2.2 Pin Level Tailoring Tab

The user is expected to tailor this sheet to their specific use-case.

The 'Pin Level Tailoring' tab takes the raw (base) package FIT rate and distributes it among each of the pins (or balls) of the device. Each pin gets an equal percentage of the package FIT. The user should use the FMEDA and safety manual to determine which device pins are used in their application for a safety-related function. The device pins that are not used can be marked as "No" for "Safety related HW element to be considered in the analysis?". This will remove these pins from the FIT calculation, which affects the safety related FIT and all derived metrics. Additionally, a Safety Mechanism can be applied to each pin to provide diagnostic coverage for pin failures. The list of diagnostics can be found in the "Pin Level Coverage" section in the bottom right of the 'Diagnostic Coverage' tab. TI may pre-populate the pin level tailoring selections in the pin level tailoring tab based on one or more expected use cases for the device. Altering the selection of Safety Mechanisms will impact the package contribution to Probabilistic Metrics for random Hardware Failures (PMHF) and Single Point Fault Metric (SPFM) in the 'Totals - ISO26262' tab.

2.2.3 Function and Diag Tailoring Tab

The user is expected to tailor this sheet to their specific use-case.

The 'Function and Diag tailoring' tab takes the raw (base) permanent and transient rates and distributes them among each of the design blocks (sometimes referred to hardware elements or IPs) of the device. Each row represents the lowest part of this analysis and each row gets a percentage of the FIT based on its transistor count or memory size. The user should refer to the Safety Manual in combination with this FMEDA to determine which design blocks are used in their application for a safety-related function. The design blocks that are not used can be marked as "No" for "Safety related HW element to be considered in the analysis?". This will remove these rows from the FIT calculation, which affects the safety related FIT and all derived metrics. Additionally, a set of Safety Mechanisms can be applied to each row to provide diagnostic coverage for faults associated with its function (please note that each selection here represents multiple safety mechanisms applied. For each row, the diagnostics that are applied to provide coverage for permanent faults, transient faults, and latent faults are split into separate columns so that the diagnostics can be applied to each. The list of Safety Mechanisms can be

found in the 'Diagnostic Coverage' tab. TI may pre-populate the function and diagnostic tailoring selections in the function and diag tailoring tab based on one or more expected use cases for the device. Altering the selection of Safety Mechanisms will impact the Probabilistic Metrics for random Hardware Failures (PMHF) and Single Point Fault Metric (SPFM) in the 'Totals - ISO26262' tab.

The definition for each row in this FMEDA can be found in the Description of Hardware Component Parts chapter of the device safety manual in addition to the diagnostic options available and the full list of diagnostics available. For additional guidance on how to determine which parts are related to the system safety function, refer to 'An In-Context Look at this Safety Element out of Context' chapter of the Device Safety Manual as well.

2.2.4 Diagnostic Coverage Tab

This tab is informational only. There are no selections the user can make in this tab.

The 'Diagnostic Coverage' tab is the source for the diagnostic groupings that are selected in the 'Pin Level Tailoring' tab and 'Function and Diag Tailoring' tab. Each design block (Part Level) will have one or more diagnostic options (which appear as the drop-down options in those tabs). The FMA values field represents all of the unique diagnostics that are applied when that diagnostic option is selected. The diagnostic detection, diagnostic coverage, and latent coverage fields indicate the diagnostic coverage claimed for each diagnostic option that will be populated into the 'Function and Diag Tailoring' tab when that option is selected.

For each failure mode of a fundamental design element, a diagnostic may be allocated in the safety architecture to detect failures. Often a single diagnostic is able to detect multiple failure modes. Diagnostics may take the form of software-based tests, hardware test structures, or additional logical channels, amongst other possible implementations. Diagnostics may have continuous, periodic, or one time execution. The frequency of necessary diagnostic application should be determined by the system integrator based on relevant safety constraints (such as fault tolerant time interval, desired detection rate, and so forth), which are necessary to support the targeted safety function or safety goal.

2.2.5 Customer Defined Diagnostics Tab

The user may or may not need to tailor this sheet depending on their specific use-case.

The 'Customer Defined Diagnostics' tab is present for the user to further modify the diagnostics beyond the defaults in the 'Diagnostic Coverage' tab. These customer defined diagnostic are built into the selections in the 'Pin Level Tailoring' tab and 'Function and Diag Tailoring' tab. If the user has a unique set of diagnostics that will be run to replace the TI recommended diagnostics, they can use one of the customer defined options, fill in the coverage details, and then move to the 'Function and Diag Tailoring' tab and apply that diagnostic to the appropriate row.

2.2.6 Totals - ISO26262 Tab

This tab is informational only. There are no selections the user can make in this tab.

The 'Totals - ISO26262' tab contains the results of the chip level FMEDA metrics based on the selections in the previous tabs. This tab summarizes the metrics as described by the ISO 26262 functional safety standard. The top table breaks out the overall FIT and diagnostic coverage for permanent faults of the die, transient faults of the die, package faults, and finally the overall sum of faults for each row. The following information is provided:

- Total FIT (Raw FIT): The total base failure rate of the device using the described base FIT model under the environmental conditions input in the 'Mission Profile Tailoring' tab.
- Safety related FIT: A subset of the total FIT that includes only the design blocks or device pins that are indicated as safety related on the 'Pin Level Tailoring' and 'Function and Diag Tailoring' tabs.
- Probabilistic Metrics for random Hardware Failures (PMHF) (in FIT): The selection of diagnostics in the 'Pin Level Tailoring' and 'Function and Diag Tailoring' tabs directly impact this percentage.
- Single Point Fault Metric - SPFM: The percentage coverage for detecting or preventing single point faults.
- Latent Fault Metric - LFM: The percentage coverage for detecting or preventing latent faults.

There are also some intermediate calculations based on the terms in the ISO 26262 standard:

- Total faults (λ)
- Total safety related faults (λ_{SR})
- Total non safety related faults (λ_{nSR})
- Total safe faults (λ_{S})

- Total not safe faults (λ_{nS}).
- Total faults with prob. of violate the SG (λ_{PVSG})
- Total single point faults (λ_{SPF})
- Total residual faults (λ_{RF})
- Total multi point (primary) [non-PVSG] (λ_{MPF}Primary)
- Total multi point (secondary) [PVSG] (λ_{MPF}Secondary)
- Total multi point detected faults (λ_{MPF_det})
- Total multi point latent faults ($\lambda_{MPF,l}$)

The concept of perceived faults is not applicable at the semiconductor level since the fault detection ability of the driver cannot be considered at this level of analysis.

2.2.7 Details - ISO26262 Tab

This tab is informational only. There are no selections the user can make in this tab.

The 'Details - ISO26262' tab contains the results of the chip level FMEDA metrics based on the selections in the previous tabs. This tab shows the metrics as described by the ISO 26262 functional safety standard, broken down by each design block. This tab may be useful if the user is interested in the failure distribution or the intermediate metrics of a certain design block. For many users, this level of detail may not be needed.

2.3 Example Calculation of Metrics

This section provides an example of functional safety metric calculation for the MCU. The results of this example can be used to evaluate the suitability of the MCU product for use in a system design. This example is not intended to be a guarantee of performance in all system implementations.

Note

This reference does not incorporate all recommendations of the *Safety Manual*. Changes in assumptions of use, such as application of a different set of diagnostics in the *Safety Manual*, can result in changes to the resulting safety metrics. Any changes made by the user should be validated for correctness.

2.3.1 Assumptions of Use for Calculation of Safety Metrics

A number of assumptions must be made in order to calculate the safety metrics according to ISO 26262:2018. The assumptions of use for the reference are detailed below:

- Confidence level applied to permanent FIT rates:
- Confidence level applied to transient FIT rates:
- Neutron flux: set to 1 (equivalent to exposure at sea level, as measured in New York City)
- Thermal management (Theta-Ja):
- Use case power:
- Safe vs non-safe: All permanent faults are considered 0% safe by default. Transient faults of digital SRAM, digital logic, and flash are considered 50% by default.
- Operational (mission) profile used:
- Special considerations on pin level tailoring:
- Special considerations on function and diag tailoring:
- Special considerations on the application of diagnostics:

2.3.2 Summary of ISO 26262 Safety Metrics at Device Level

Table 2-2 provides estimates of FIT rates and calculated safety metrics per ISO 26262-5:2018 using previously noted assumptions for the device.

Table 2-2. ISO 26262 FIT Rate Estimates and Safety Metrics

		Die		Package	Overall
		Permanent	Transient	Permanent	Sum
Total FIT (Raw FIT)	λ	8.13	1.20	9.98	19.31
Safety Related FIT	λ_{SR}	8.13	1.20	9.74	19.08
Probabilistic Metrics for Random Hardware Failures (in FIT)	PMHF	2.49	0.60	0.58	3.67
Single Point Fault Metric	SPFM	69.36%	50.00%	94.06%	80.75%
Latent Fault Metric	LFM	83.77%	NA	94.44%	90.37%

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