High Voltage Seminar

Introduction to Functional Safety
for high-voltage systems

Martin Staebler

Systems engineer, Industrial systems motor drives team

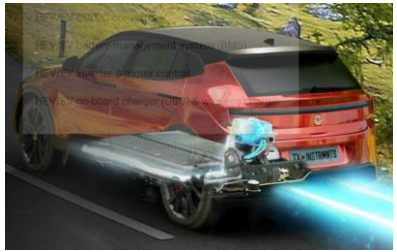
Ashish Vanjari

Systems engineer, C2000™ real-time MCUs

Agenda

- Introduction
- Overview to industrial drives and automotive functional safety standards
- Safe torque off concepts and industrial drive STO example
- Safe motion MCU architectures and C2000 MCU safety support
- Automotive functional safety example
- Conclusion

Introduction | Why safety matters in high-voltage applications



- **Hazard example**: Electrical shock

- **Hazard example**: Robot moves **unintended** and may injure the human operator
- **Hazard example:** During an **unintended** power loss robot arm may injure the human operator
- How to reduce the probability of a hazard to an acceptable risk?

- **Isolation** is key for overall reliable and safe system operation with a **human interface** ***(electrical safety)***

- **Functional safety** is key for the **overall risk reduction of hazards**: Sensing & real-time processing of faulty scenarios and actuating to the safe state to prevent accidents

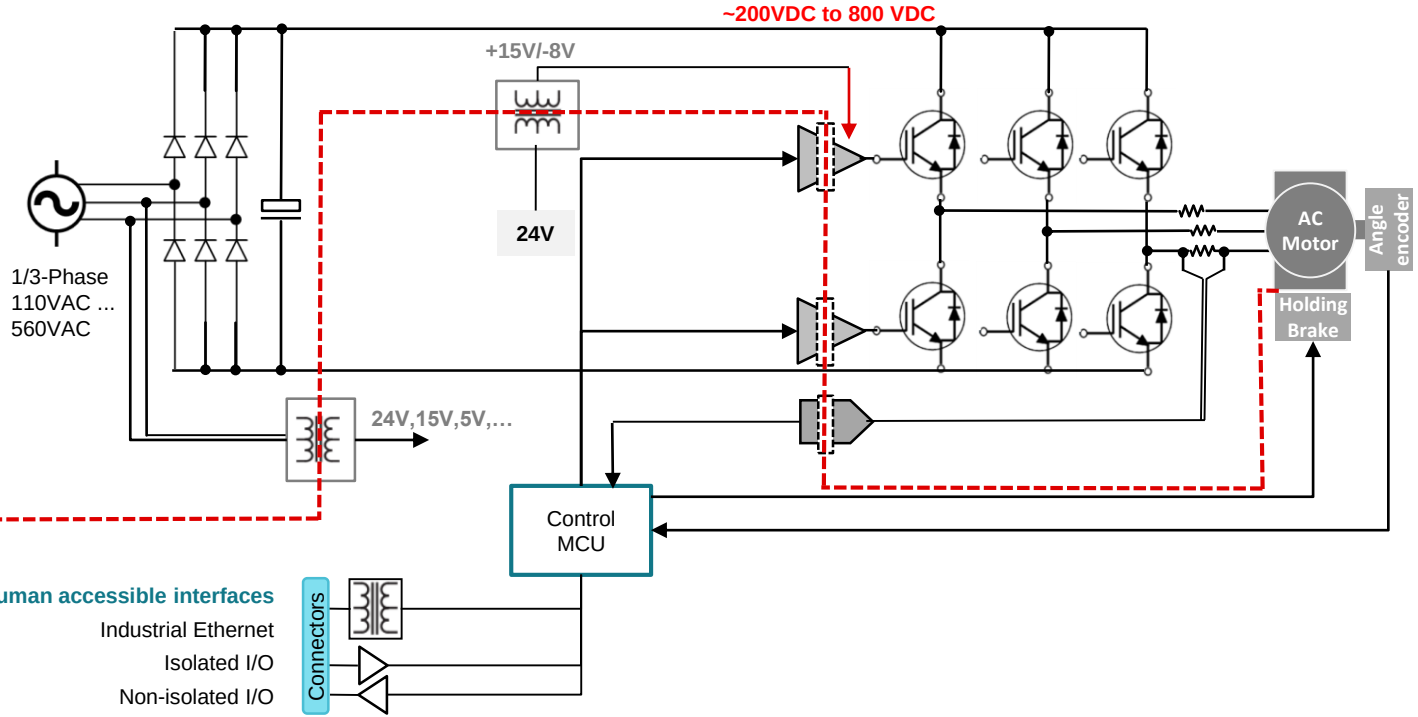
High voltage servo drive | Simplified block diagram

- ✓ **Industrial drives isolation** need to comply to IEC61800-5-1 **Safety requirements – Electrical**, thermal and energy

High voltage area
≥ 60VDC/35VAC

Reinforced isolation
(electrical safety)

Low voltage area
≤ 60VDC/35VAC



High voltage servo drive | Simplified block diagram

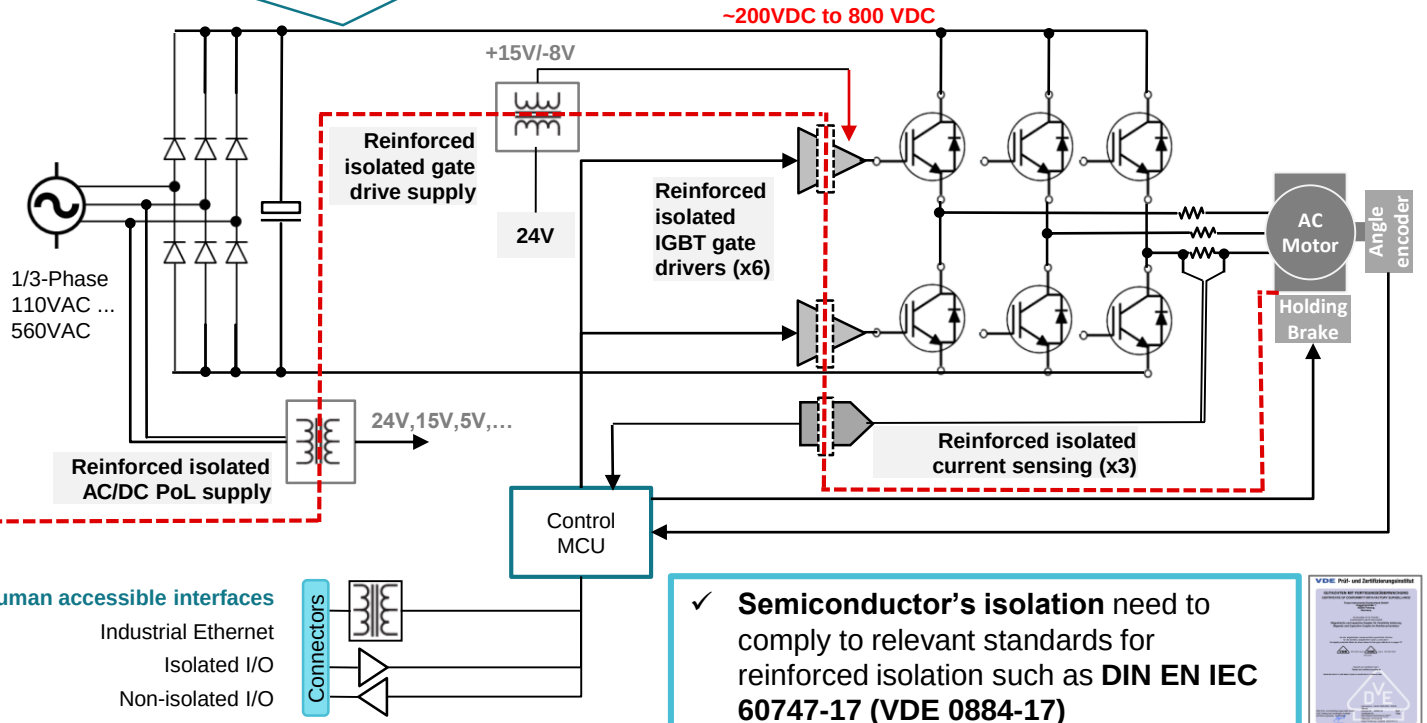
- What does it take to make it a functional safety enabled drive?

✓ **Industrial drives isolation** need to comply to IEC61800-5-1 **Safety requirements – Electrical**, thermal and energy

High voltage area
≥ 60VDC/35VAC

Reinforced isolation
(electrical safety)

Low voltage area
≤ 60VDC/35VAC



Human accessible interfaces

Industrial Ethernet

Isolated I/O

Non-isolated I/O

✓ **Semiconductor's isolation** need to comply to relevant standards for reinforced isolation such as **DIN EN IEC 60747-17 (VDE 0884-17)**

Source: www.ti.com/lit/cr/szzq123r/szzq123r.pdf

Industrial drives/machinery standards | Predefined safety function examples

Standard	Title
ISO 13849	**Safety of machinery** Safety-related parts of control systems
IEC 61508	**Functional safety of electrical/electronic/programmable electronic safety-related systems**
IEC 62061	**Safety of machinery** - Functional safety of safety-related electrical, electronic and programmable electronic control systems
IEC 61800-5-2	**Adjustable speed electrical power drive systems** – Part 5-2: Safety requirements – Functional

- **Based on Performance Level (PL) and Category (Cat)**
- **Based on Safety Integrity Level (SIL)**

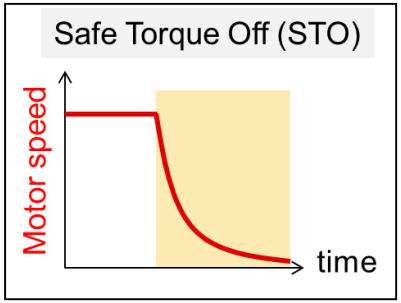
Industrial drives/machinery standards | Predefined safety function examples

Standard	Title
ISO 13849	**Safety of machinery** Safety-related parts of control systems
IEC 61508	**Functional safety of electrical/electronic/programmable electronic safety-related systems**
IEC 62061	**Safety of machinery** - Functional safety of safety-related electrical, electronic and programmable electronic control systems
IEC 61800-5-2	**Adjustable speed electrical power drive systems** – Part 5-2: Safety requirements – Functional

- **Based on Performance Level (PL) and Category (Cat)**
- **Based on Safety Integrity Level (SIL)**

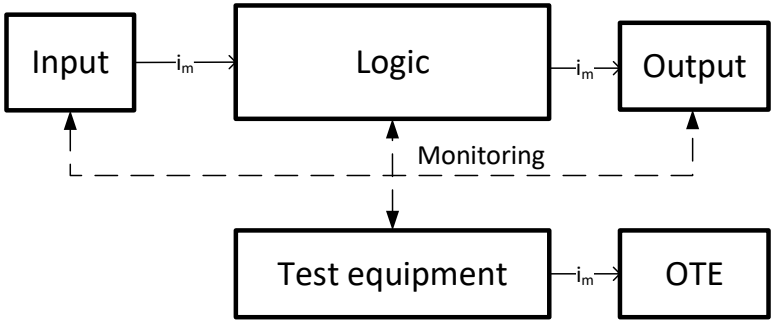
Safety function IEC 61800-5-2	Acronym
Safe Torque Off	**STO** (1)
Safe Stop 1	SS1
Safe Stop 2	SS2
Safe Operating Stop	SOS
Safe Brake Control	SBC
…	…
Safely-Limited Speed	SLS
Safely-Limited Torque	SLT
…	…
Safe Speed Monitor	SSM
Safe Motor Temperature	SMT
Safe Cam	SCA

(1) Safe torque off (STO) prevents force-producing power from being provided to the motor.

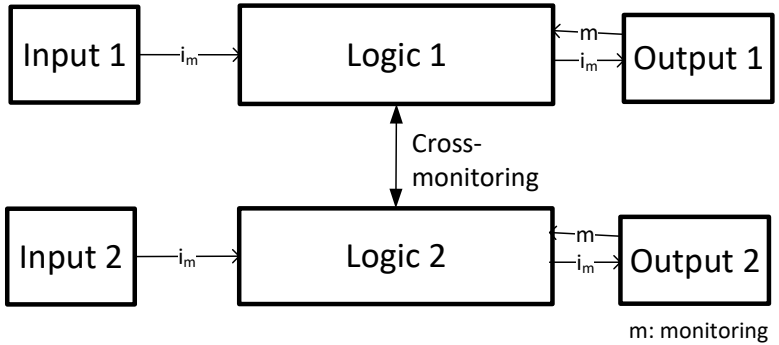


Industrial machinery | ISO 13849 designated safety architecture

- **ISO13849** categories examples and hardware fault tolerance (HFT)



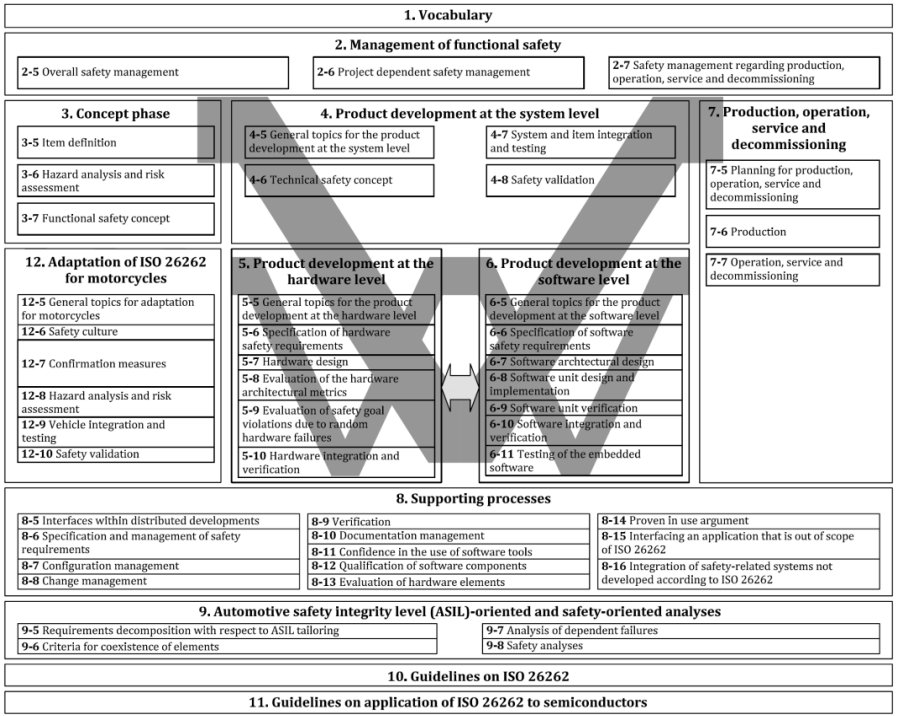
Category 2, HFT=0



Category 3 and 4, HFT=1

- **IEC 61800-5-2 (IEC 61508): Hardware fault tolerance (HFT) <u>not designated</u>, as long desired SIL level met**
- **IEC61800 SIL 3** equivalent to ISO13849 Performance Level **PL e requires min. category 3** (HFT=1)
- Safe drives often certified for both safety standards, typically see dual channel systems with HFT=1

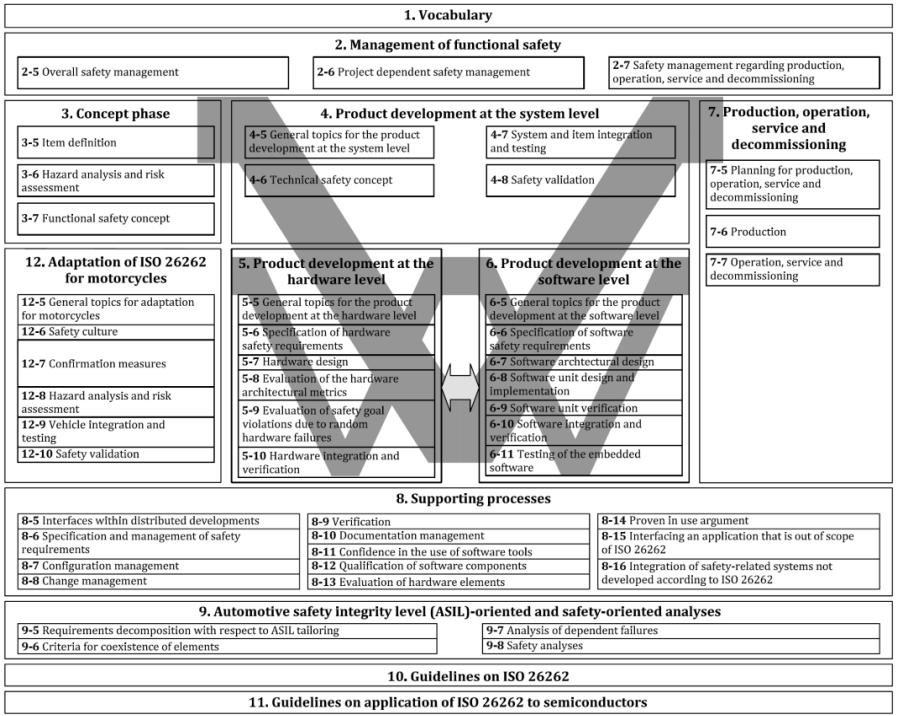
ISO 26262 Functional Safety



Source : ISO 26262-1:2018 Figure 1 — Overview of the ISO 26262 series of standards

- **Automotive-specific** risk-based approach for ASIL determination
- Provides guidelines across **lifecycle phases**, i.e., Concept → development → production → operation, service, and → decommissioning
  - V-model as reference for phases of product development

ISO 26262 Functional Safety

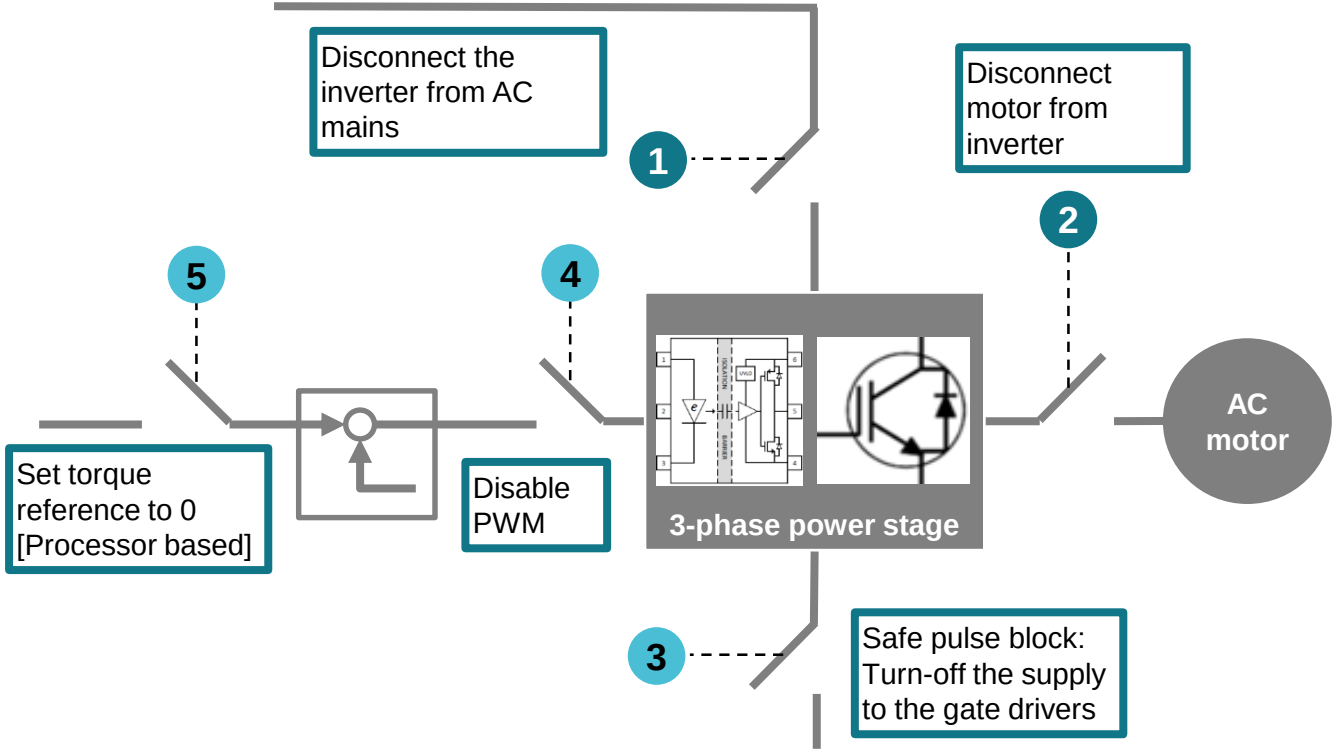


Source : ISO 26262-1:2018 Figure 1 — Overview of the ISO 26262 series of standards

- **Automotive-specific** risk-based approach for ASIL determination
- Provides guidelines across **lifecycle phases**, i.e., Concept → development → production → operation, service, and → decommissioning
  - V-model as reference for phases of product development

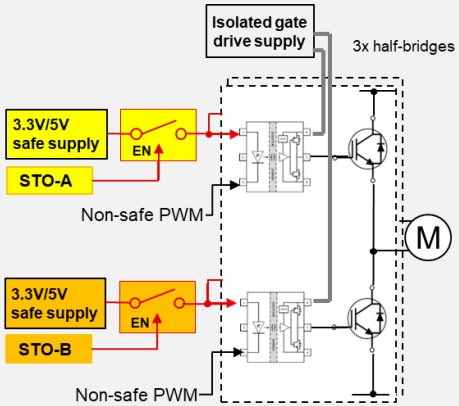
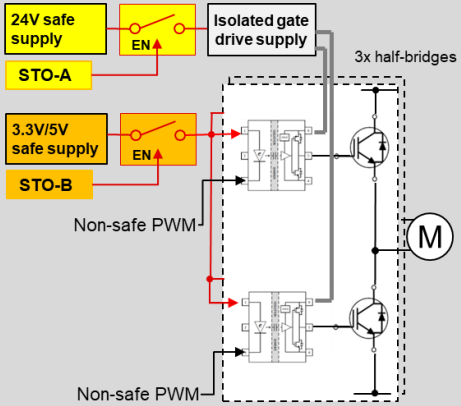
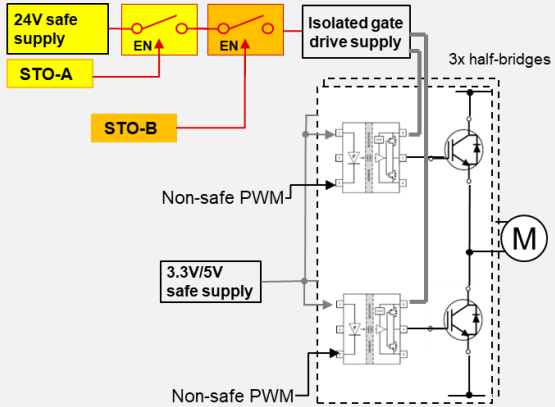
- **Key Differences with Industrial Functional Safety:**
  1. Industrial system identifies Equipment Under Control (EUC) and the associated Safety Instrumented Function. This **distinction of the safety function** is not always possible in Automotive
  2. **Risk assessment** in automotive takes into account the Severity, Exposure, and **Controllability** of the situation by the driver
  3. Low-volume Industrial systems vs Automotive systems are **mass-market, production-related** lifecycle phases
  4. Automotive development is **across multiple organizations**, relations between customers and suppliers
  5. Typical System safety architecture for higher functional safety is **1oo2 for Industrial** and **1oo1D for Automotive** applications

Realizing safe torque off | Options to disable torque generating power to the motor

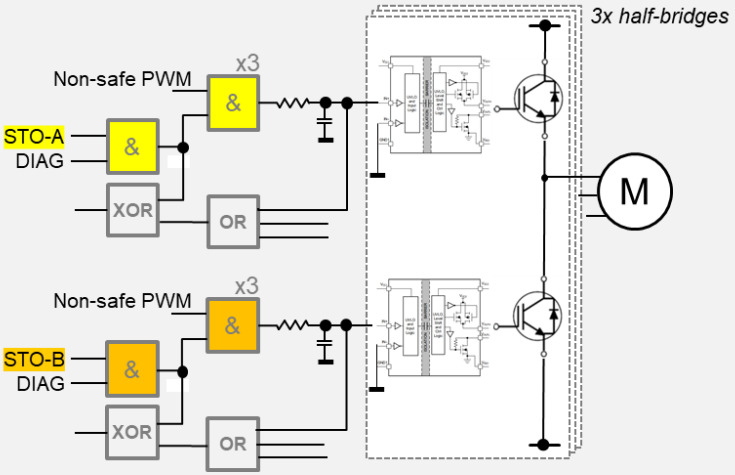


Mechanical relays	
Electronic solution	Typical approach today

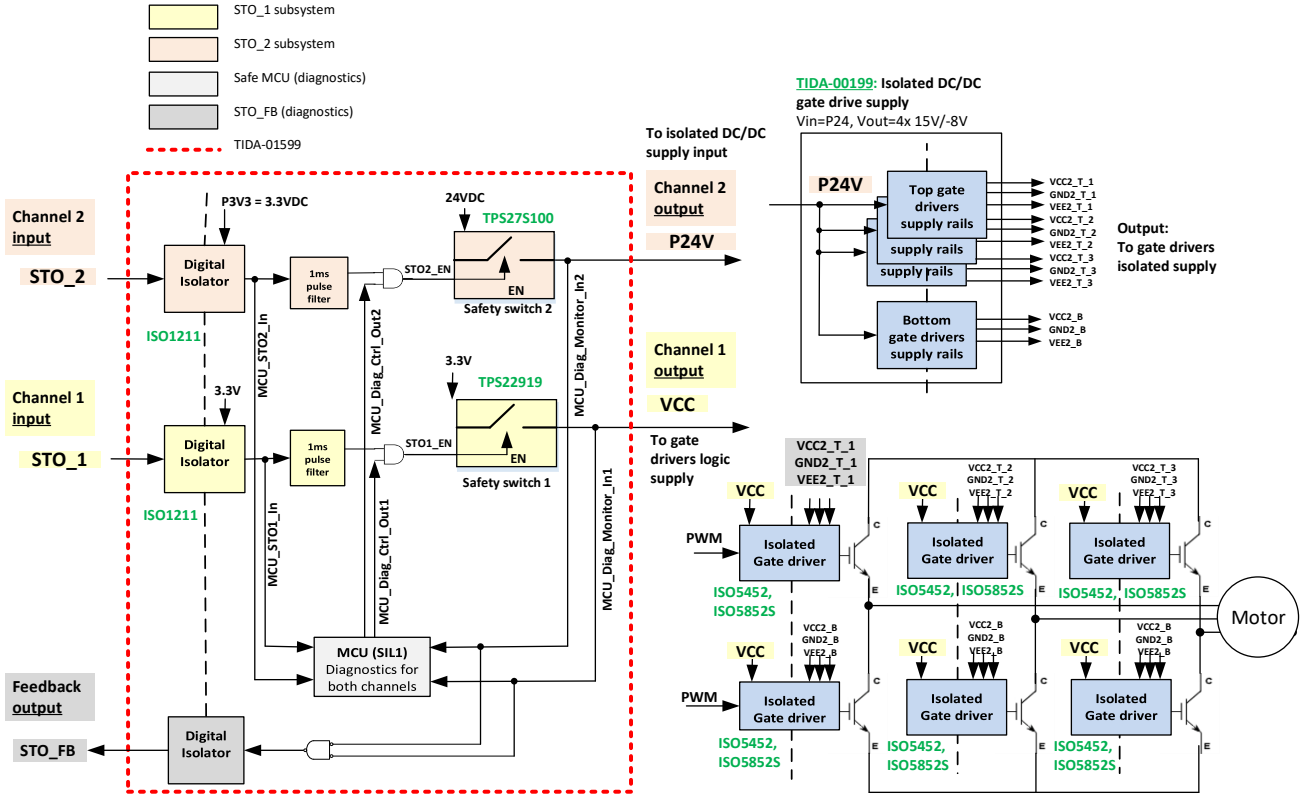
STO subsystem | Architecture examples cutting off supply

	Architecture 1	Architecture 2	Architecture 3
Block diagram Safe subsystem A Safe subsystem B			
Gate drive logic supply	STO-A (top side), STO-B (bottom side)	STO-B (logic side, top and bottom)	-
Isolated gate drive supply	-	STO-A (isolated supply, top and bottom side)	STO-A and STO-B (isolated supply, top and bottom side)
Comment	✓ Popular for isolated opto-input / compatible devices (IEC 61800-5-2 Annex B ✓ 5V or 3V3 load switches	✓ Option for isolated CMOS-input devices, 6-channel isolators, half-bridge gate drivers ○ 24V load switch ✓ TUEV assessed concept (TIDA-01599)	✓ Generic option ✓ Likely easier retrofit (separate module) - 24V load switches (x2)

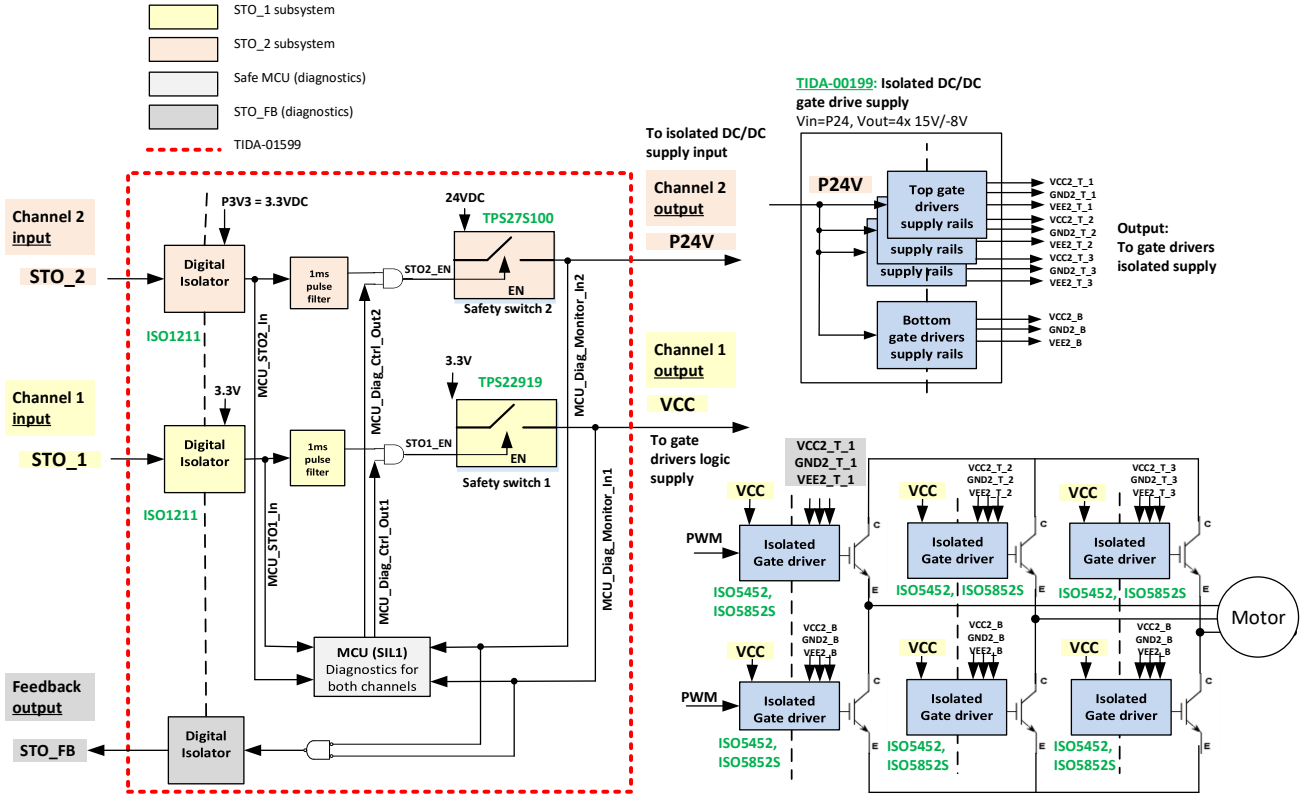
STO subsystem | Architecture examples disabling PWM

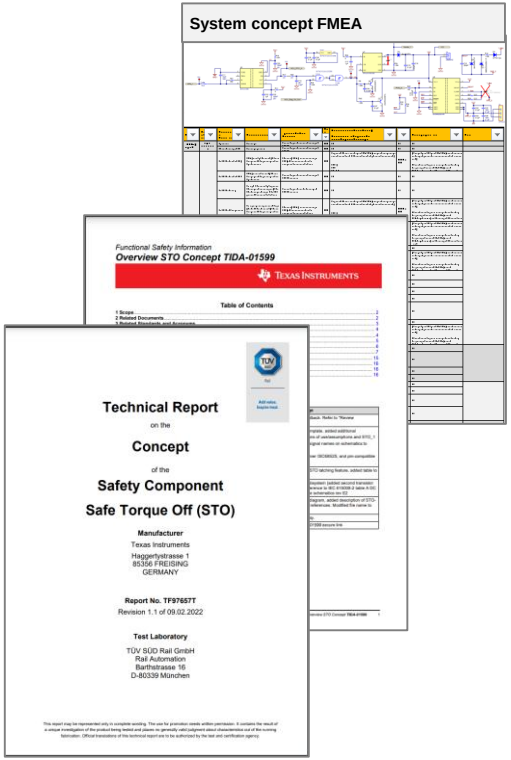
	Architecture 4
Block diagram Safe subsystem A Safe subsystem B	
Buffer (cold side)	STO-A (top side) STO-B (bottom side)
Buffer (hot-side)	-
Comment	✓ Power not cut-off ✓ Fast buffer with short diagnostic pulse (e.g. 20ns) ○ RC filter to remove diagnostic test pulses, contributes to PWM propagation delay

Architecture 2 system example | TÜV SÜD-assessed safe torque off (STO) reference design for industrial drives



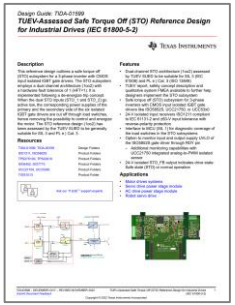
Architecture 2 system example | TÜV SÜD-assessed safe torque off (STO) reference design for industrial drives



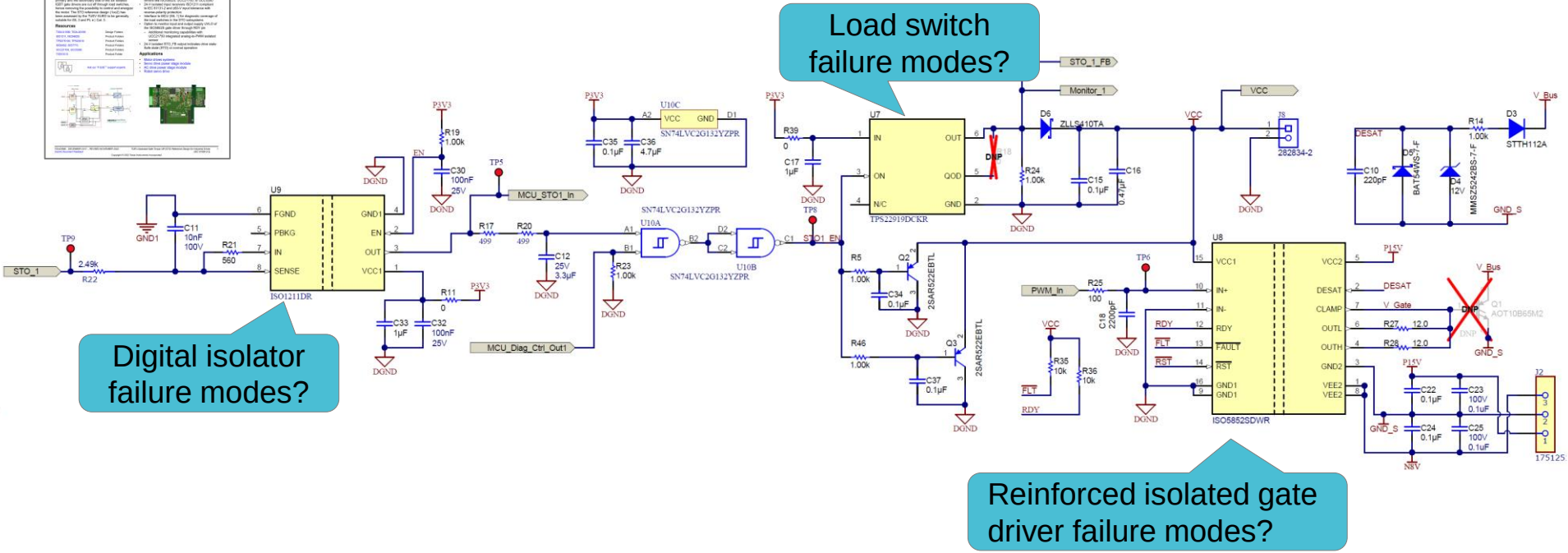


Source: www.ti.com/lit/fs/tiduf02/tiduf02.pdf

Concept example | STO-1 load switch subsystem



Reference: TÜV SÜD-assessed safe torque off (STO) reference design for industrial drives (IEC 61800-5-2)



Failure modes and diagnostic coverage | Where to get the information?

Challenge? *ISO13849-2:2012 Annex D does not list magnetic and capacitive isolators*

- ISO 13849-2:2012 Annex D
- IEC 61800-5-2:2016 paragraph D.3 Fault Models
- ISO 26262 Part 11 – section 5.1.4, 5.2.2, 5.3.2
- IEC 61508 Part 2 Annex A
- IEC 61709 Annex A
- Handbooks and References Databases
  - Exida - Electronic Component Reliability Handbook
  - Quaterion.com - FMD-2016

Isolator fault model | Reference to IEC 61800-5-2

IEC 61800-5-2 is generic and does not specify the type of isolation (optical, magnetic or capacitive)

Table D.5 – Signal Isolation components

Fault considered	Fault exclusion	Remarks
Open-circuit of individual connection	None	
Short-circuit between any two input connections	None	
Short-circuit between any two output connections	None	
Short-circuit between any two connections across the isolation barrier	Short-circuit across the isolation barrier can be excluded if remarks 1) and 2) are fulfilled.	1) The Signal Isolation component is built in accordance with OVC III according to IEC 61800-5-1. If a SELV/PELV power supply is used, pollution degree 2/ OVC II applies. NOTE All requirements of IEC 61800-5-1:2007, 4.3.6 apply. 2) Measures are taken to ensure that an internal failure of the Signal Isolation component cannot result in excessive temperature of its insulating material.

Fault exclusion: See an example with TI's isolated gate drivers on next two slides

Source: *IEC 61800-5-2:2016, D.3.13 Signal Isolation components (the requirements of Table D.5 apply)*

Insulation specification | UCC21750 5.7kVrms, single-channel isolated gate driver

6.6 Insulation Specifications

PARAMETER		TEST CONDITIONS	VALUE	UNIT
GENERAL				
CLR	External clearance[1]	Shortest terminal-to-terminal distance through air	> 8	mm
CPG	External creepage[1]	Shortest terminal-to-terminal distance across the package surface	> 8	mm
DTI	Distance through the insulation	Minimum internal gap (Internal clearance) of the double insulation (2 × 0.0085 mm)	> 17	µm
CTI	Comparative tracking index	DIN EN 60112 (VDE 0303-11); IEC 60112	> 600	V
	Material group	According to IEC 60664–1	I	
	Overvoltage Category per IEC 60664–1	Rated mains voltage ≤ 300 V_{RMS}	I-IV	
		Rated mains voltage ≤ 600 V_{RMS}	I-IV	
		Rated mains voltage ≤ 1000 V_{RMS}	I-III	

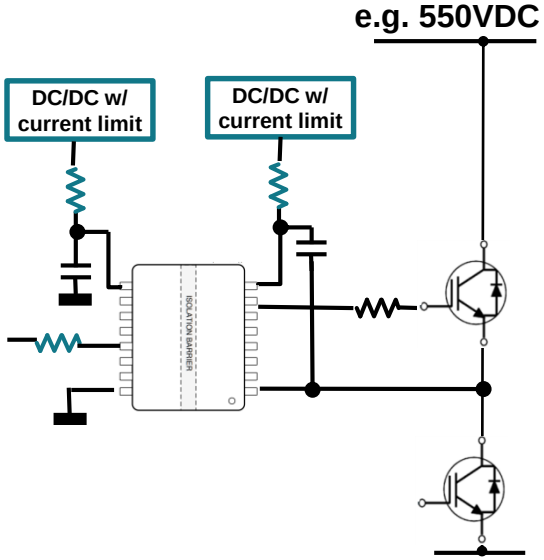
✓ UCC21750 insulation meets IEC 61800-5-2 table D.5 overvoltage category **III** for AC mains ≤ 1000Vrms

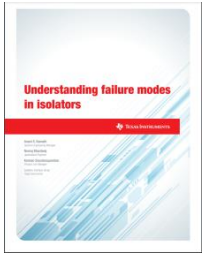
Safety limiting values to avoid excessive temperatures | Example UCC21750

6.7 Safety Limiting Values [UCC21750 data sheet example]

PARAMETER		TEST CONDITIONS	MIN	TYP	MAX	UNIT
I_S	Safety input, output, or supply current	$R_{\theta JA}$ = 68.3°C/W, V_{DD} = 15 V, V_{EE} = –5 V, T_J = 150°C, T_A = 25°C			61	mA
		$R_{\theta JA}$ = 68.3°C/W, V_{DD} = 20 V, V_{EE} = –5 V, T_J = 150°C, T_A = 25°C			49	
P_S	Safety input, output, or total power	$R_{\theta JA}$ = 68.3°C/W, V_{DD} = 20 V, V_{EE} = –5 V, T_J = 150°C, T_A = 25°C			1220	mW
T_S	Safety temperature				150	°C

- intend to minimize potential damage to the isolation barrier upon failure of input or output circuitry.

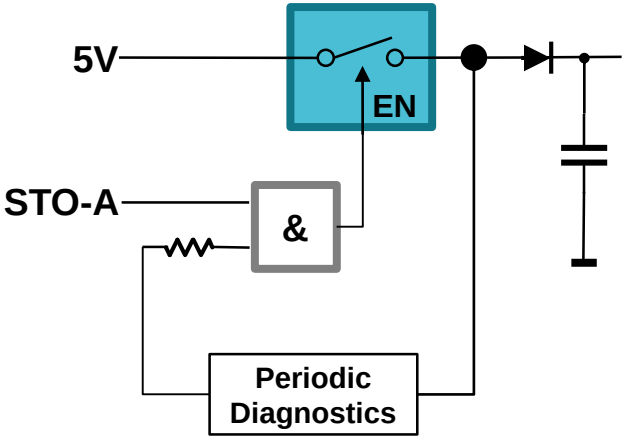




See also application note: Understanding failure modes in isolators

✓ Limit e.g. supply current with resistor or LDO/DCDC with current limit

Load switch safe subsystem | Safe Failure Fraction example using FMEA with TPS22918-Q1 load switch



TPS22918-Q1 load switch subsystem

Functional Safety Information
TPS22918-Q1
Functional Safety FIT Rate, FMD and Pin FMA

TEXAS INSTRUMENTS

Table of Contents

- ✓ Component Failure Rates per IEC TR 62380 / ISO 26262 Part 11 and Siemens norm SN29500
- ✓ FMD (below)

3 Failure Mode Distribution (FMD)

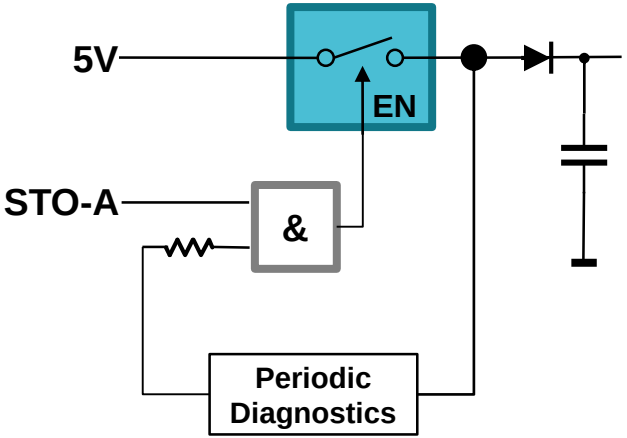
The failure mode distribution estimation for TPS22918-Q1 in Table 3-1 comes from the combination of common failure modes listed in standards such as IEC 61508 and ISO 26262, the ratio of sub-circuit function size and complexity and from best engineering judgment.

The failure modes listed in this section reflect random failure events and do not include failures due to misuse or overstress.

Table 3-1. Die Failure Modes and Distribution

Die Failure Modes	Failure Mode Distribution (%)
VOUT open or Hi-Z	25%
VOUT stuck on (VIN)	15%
VOUT outside specification (voltage or rise time)	45%
QOD stuck on	5%
QOD stuck off	5%
Pin to pin short (any two pins)	5%

Load switch safe subsystem | Safe Failure Fraction example using FMEA with TPS22918-Q1 load switch



TPS22918-Q1 load switch subsystem

Functional Safety Information
TPS22918-Q1
Functional Safety FIT Rate, FMD and Pin FMA

TEXAS INSTRUMENTS

Table of Contents

- ✓ Component Failure Rates per IEC TR 62380 / ISO 26262 Part 11 and Siemens norm SN29500
- ✓ FMD (below)

3 Failure Mode Distribution (FMD)

The failure mode distribution estimation for TPS22918-Q1 in Table 3-1 comes from the combination of common failure modes listed in standards such as IEC 61508 and ISO 26262, the ratio of sub-circuit function size and complexity and from best engineering judgment.

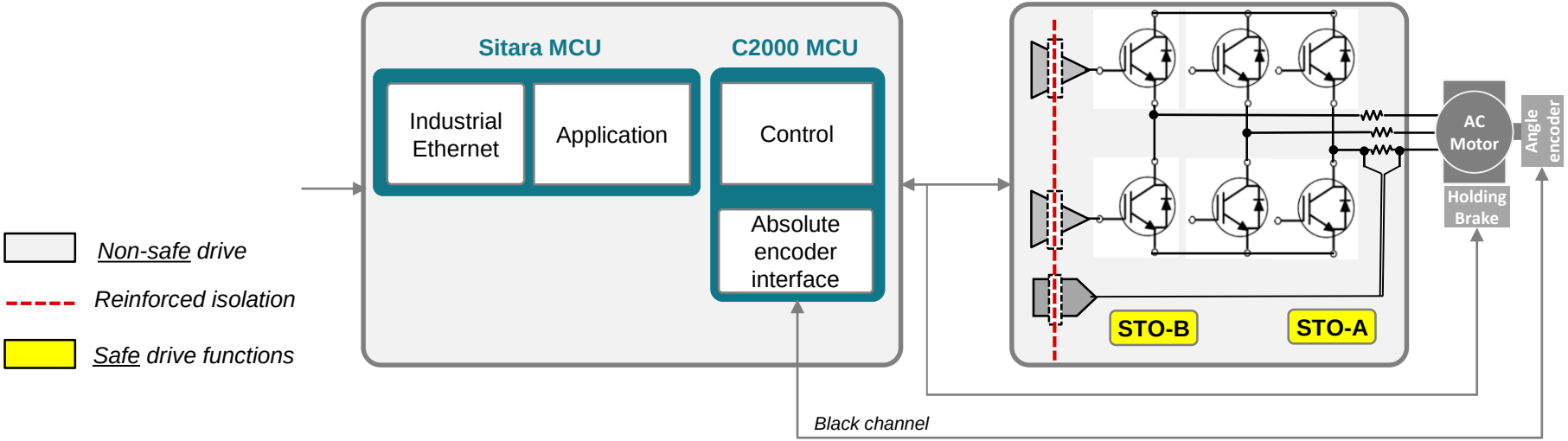
The failure modes listed in this section reflect random failure events and do not include failures due to misuse or overstress.

Table 3-1. Die Failure Modes and Distribution

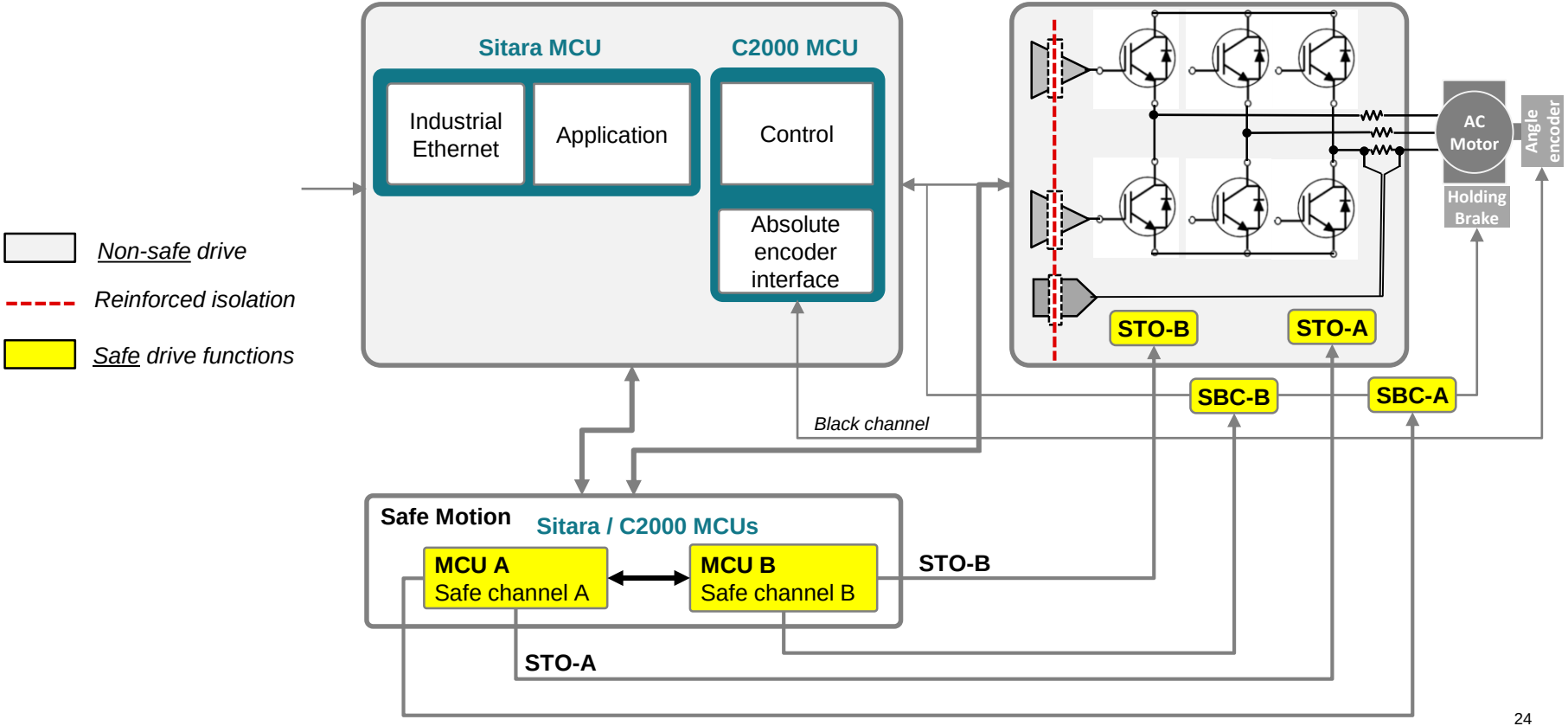
Die Failure Modes	Failure Mode Distribution (%)	
VOUT open or Hi-Z	25%	Safe failure
VOUT stuck on (VIN)	15%	Dangerous failure detected
VOUT outside specification (voltage or rise time)	45%	Dangerous failure detected
QOD stuck on	5%	Not used, safe Failure
QOD stuck off	5%	Not used, safe Failure
Pin to pin short (any two pins)	5%	Example assume 50% safe failures and diagnostics identifies 90% of dangerous faults

✓ **SFF_{TPS}: 99.75%**

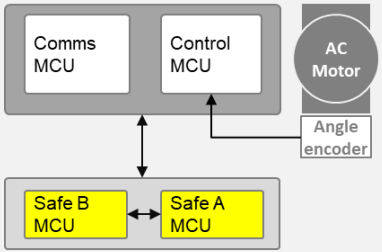
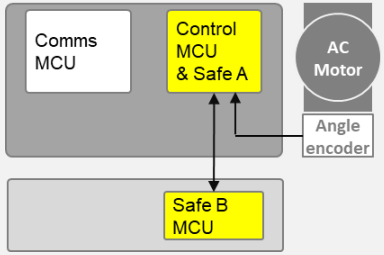
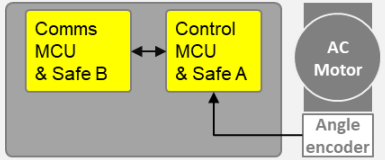
Example | Functional-safety-enabled servo drive



Example | Functional-safety-enabled servo drive



Safe motion architectures with HFT=1 | Comparison

Parameter	Separate safety MCUs	One MCU with integrated safety	Two MCUs with integrated safety
Block diagram			
BOM / Space	-	o	+
Scalability HW	+	o	-
Firmware upgrade	+	o or +(1)	o or +(1)
Diversity	o(2) or +	+	+
Example EE	AC inverter, servo drive, robotics	AC inverter, servo drives, robotics	Robotics
TÜV concept report	✓ C2000 MCU (requires NDA)	✓ C2000/Sitara MCU (requires NDA)	

System safety	Diagnostic coverage (each MCU) (3)
SIL 3, Cat 3 PL e	≥90%
SIL3, Cat 4 PL e	≥99%

(1) If dual core systems, free from interference
(2) Typically safe MCU1 equal to MCU 2
(3) Functional safety certified MCUs with multi-core CPUs like TMS320F28388D and Sitara AM6441 ease functional safety development and accelerate time to market

C2000™ Real-time microcontrollers overview

Scalable, **ultra-low latency**, **real-time controller** platform designed for efficiency in power electronics, such as high power density, high switching frequencies, GaN and SiC technologies

C2000 Real-Time MCU

Highly accurate sensing
- 12-/16-bit ADCs, up to 24 channels
- Full analog comparators with built-in DACs
- Quadrature Encoder and Capture Logic

Sense

Process

High performance processing
Floating-point DSP C28x™ core + parallel multi-core architecture + instructions set optimized for control math, up to 925 MIPS

Highly flexible, High-resolution PWMs:
- Up to 32 outputs
- Tightly coupled with Sensing domain for fast response time
- Buffered Output DACs

Control

Interface

CAN, CAN-FD, LIN, UART, SPI, I2C, PMBus, USB, 10/100 Ethernet MAC, EtherCAT®, XEMIF

Expertise and support:
Software libraries, Reference designs, and Functional Safety-Compliant devices and Certification collateral.

25 years expertise in real-time control systems

Leading innovation:
Configurable Logic Block for peripheral customization, Fast Serial Interface for high-speed communication, ERAD for enhanced diagnostics and profiling

1.2-V core, 3.3-V I/O design	Up to 1.5 MB Flash, 256 kB RAM (ECC protected)	QFN, QFP, BGA packages	-40 to 125C temperature range	Q100 automotive qualified options

Over 900 million units shipped for industrial and automotive applications with compatible software

C2000 MCU architecture | Key safety mechanisms

Sense

- **Redundant and diverse sensing** peripherals, ADC and CMPSS
- Built-in HW sensor data **processing** & result **comparison**
- Extensive interconnection between Sensors and Actuators via XBAR → **Activate safe state independent of CPU**

Process

- Dual Core **Lock-step CPU**
- **Diverse architecture** CPUs, 2-Cores (C28x and CLA) for implementation of "Reciprocal Comparison"
- **HWBIST for CPU**: Periodic, online detection of faults with 90%DC → Provides diagnostics for long runtime Industrial

Actuate

- **Redundant** PWM modules with **configurable safe-state control** (TRIP, Hi, Low states of output on faults detected)
- **Smart on-chip monitoring** of outputs supported in HW (eCAP, WADI)
- **CLB**: Implement complex safe states ASC and complex safety functions, eliminating CPLD/FPGA

Communicate

- Support for **End-to-end safety** for Communication peripherals
- **Systematic & Independent Fault/Error Handling**, End-to-End safety on MCU interconnect, **ECC/Parity** on all SRAMs → Reduce the probability of dangerous failure, and increase the availability of safety functions

DFA

- Coexistence, Common Cause Failures(CCF)
- Dedicated **on-chip clock monitors** to detect CCF
- **MPU, DCSM**: "Achieve co-existence of safety functions with real-time control": white paper
- **Built-in HW support** for diagnostics: Logic Power-On Self Test, MCU Diagnostics – ERAD, BG-CRC, EPG to help implementation of diagnostic functions

C2000 MCU safety support

MCU Safety built-in **HW** Features

Key safety features	F2838x	F2837x F2807x	F28003x	F28002x	F280015x
SIL-3 Compliant Development Process	✓	✓	✓	✓	✓
Random Hardware Capability	SIL-2	SIL-2	SIL-2	QM	SIL-2
Systematic Capability	SIL-3	SIL-3	SIL-3	SIL-3	SIL-3
Redundant and diverse processing units (C28x and CLA) for implementing safety functions	✓	✓	✓	X	Lockstep C28x
Memory parity	✓	✓	X	X	✓
Memory ECC	✓	✓	✓	✓	✓
Memory BIST (MPOST)	✓	X	✓	✓	✓
Dual Core Security Module (DCSM) to achieve non-interference between software elements	✓	✓	✓	✓	✓
Windowed watch-dog timer with independent clock	✓	✓	✓	✓	✓
Hardware CRC acceleration	✓	✓	✓	✓	✓
Hardware BIST (HWBIST): Permanent fault coverage of 90%+ for C28x CPU	✓	✓	✓	✓	X C28x-STL (60% coverage)
CLA-Self Test Library (STL)	✓	✓	✓	N/A	N/A
Redundant and independent ADC / PWM Modules	✓	✓	✓	✓	✓
Redundant Configurable Logic Block (CLB) option	✓	✓	✓	✓	N/A
Safety Manual: detailed product overview, capabilities and constraints, TI development process, safety elements, and safety diagnostics.	SFFS022	SPRUI78	Beta available - contact TI	SPRUIT5	Beta available - contact TI
Device Certification	SSZQQM2	SWAQ009	Coming soon	Not planned	Coming soon

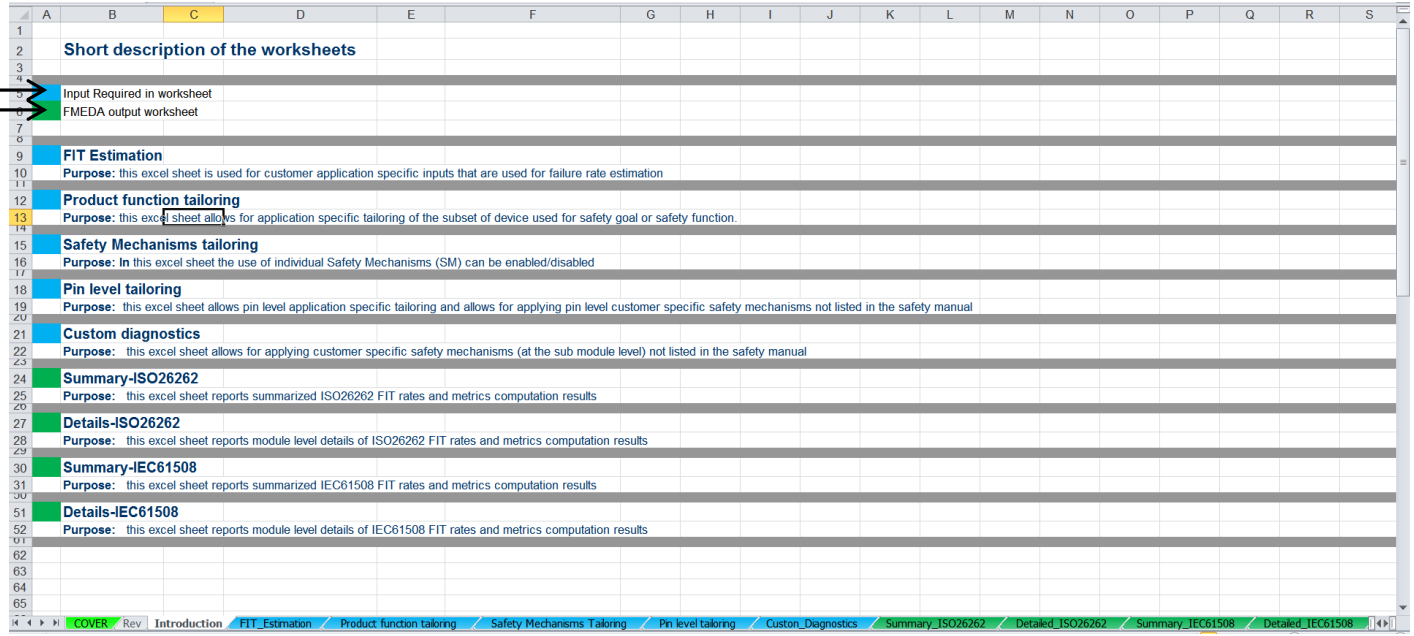
Collateral, **SW** library support for system-level certification

Safety collateral	
Development Process Certificate Hardware | Software	TUV-SUD certificate for QRAS-AP00210. Functional safety development process for IEC 61508-2 and ISO 26262-5 Compliant Components
C2000 Safety package*	By request and NDA required. Package includes below elements: • **Technical Report on Random HW Capability** • **Technical Report on Systematic Capability** • **FMEDA**: A failure mode, effects and diagnostic analysis (FMEDA) is used in the development stage to provide a detailed analysis of different failure modes, the associated effects of failure modes, diagnostics and the impact of any implemented diagnostics/ safety mechanisms in terms of diagnostic coverage. 5 part FMEDA training video series. • **Device Concept Assessment** • **SAR (Safety Analysis Report)**: Contains results of safety analysis according to the targeted functional safety standards.
Software diagnostic library	A library of modules and examples demonstrating safety features and mechanisms. Examples include CPU, memory, clocks/ watchdogs, HWBIST, etc. F2837x/07x supported through this library. All other F28x series supported by libraries released in C2000Ware.
CLA co-processor self-test library*	Library to perform start-up and periodic tests for CLA logic integrity
Compiler qualification kit	Compare compiler coverage for customer use cases against coverage of TI compiler release validations
Safety certified RTOS (SafeRTOS)	Pre-certified safety Real Time Operating System (RTOS)
MathWorks simulation & code generation	IEC certification kit helps you qualify MathWorks code generation and verification tools to streamline certification of your embedded systems

Source : www.ti.com/lit/swab013

FMEDA | Customize to your requirements

Blue Tabs
Green Tabs



Short description of the worksheets

Input Required in worksheet
FMEDA output worksheet

FIT Estimation
Purpose: this excel sheet is used for customer application specific inputs that are used for failure rate estimation

Product function tailoring
Purpose: this excel sheet allows for application specific tailoring of the subset of device used for safety goal or safety function.

Safety Mechanisms tailoring
Purpose: In this excel sheet the use of individual Safety Mechanisms (SM) can be enabled/disabled

Pin level tailoring
Purpose: this excel sheet allows pin level application specific tailoring and allows for applying pin level customer specific safety mechanisms not listed in the safety manual

Custom diagnostics
Purpose: this excel sheet allows for applying customer specific safety mechanisms (at the sub module level) not listed in the safety manual

Summary-ISO26262
Purpose: this excel sheet reports summarized ISO26262 FIT rates and metrics computation results

Details-ISO26262
Purpose: this excel sheet reports module level details of ISO26262 FIT rates and metrics computation results

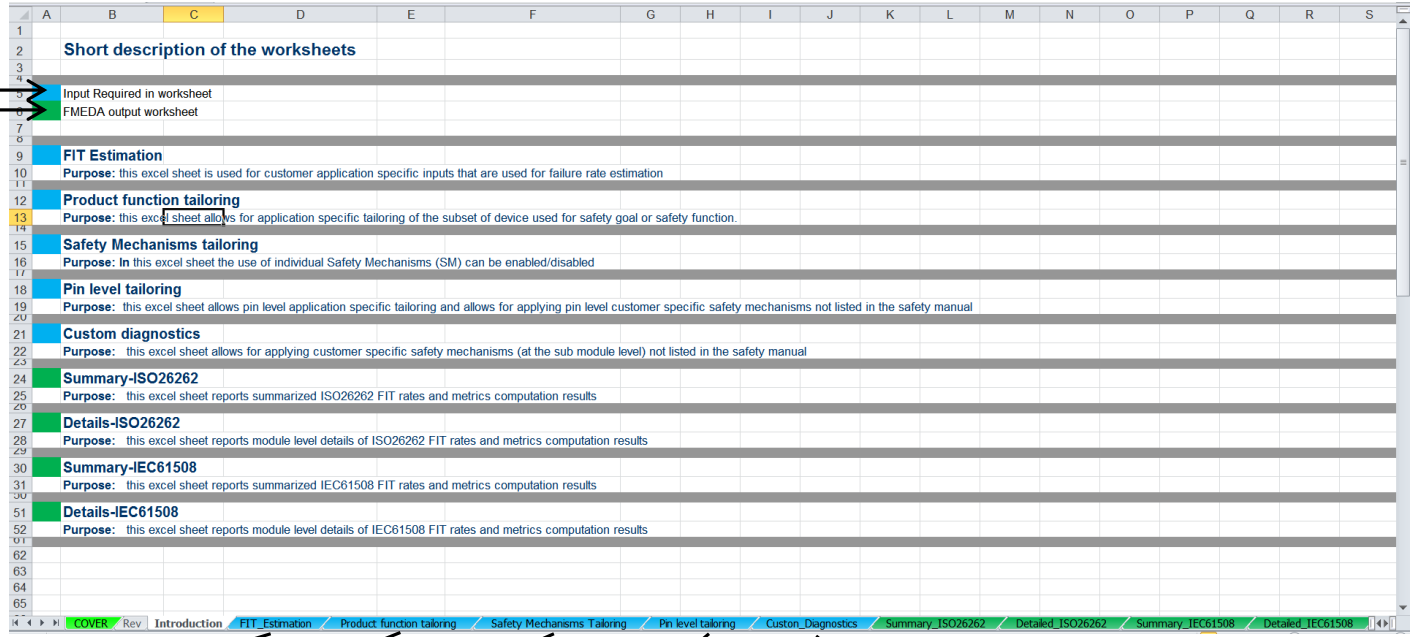
Summary-IEC61508
Purpose: this excel sheet reports summarized IEC61508 FIT rates and metrics computation results

Details-IEC61508
Purpose: this excel sheet reports module level details of IEC61508 FIT rates and metrics computation results

COVER | Rev | Introduction | FIT_Estimation | Product function tailoring | Safety Mechanisms Tailoring | Pin level tailoring | Custon_Diagnostics | Summary_ISO26262 | Detailed_ISO26262 | Summary_IEC61508 | Detailed_IEC61508

FMEDA | Customize to your requirements

Blue Tabs
Green Tabs



Short description of the worksheets

Input Required in worksheet
FMEDA output worksheet

FIT Estimation
Purpose: this excel sheet is used for customer application specific inputs that are used for failure rate estimation

Product function tailoring
Purpose: this excel sheet allows for application specific tailoring of the subset of device used for safety goal or safety function.

Safety Mechanisms tailoring
Purpose: In this excel sheet the use of individual Safety Mechanisms (SM) can be enabled/disabled

Pin level tailoring
Purpose: this excel sheet allows pin level application specific tailoring and allows for applying pin level customer specific safety mechanisms not listed in the safety manual

Custom diagnostics
Purpose: this excel sheet allows for applying customer specific safety mechanisms (at the sub module level) not listed in the safety manual

Summary-ISO26262
Purpose: this excel sheet reports summarized ISO26262 FIT rates and metrics computation results

Details-ISO26262
Purpose: this excel sheet reports module level details of ISO26262 FIT rates and metrics computation results

Summary-IEC61508
Purpose: this excel sheet reports summarized IEC61508 FIT rates and metrics computation results

Details-IEC61508
Purpose: this excel sheet reports module level details of IEC61508 FIT rates and metrics computation results

COVER | Rev | Introduction | FIT_Estimation | Product function tailoring | Safety Mechanisms Tailoring | Pin level tailoring | Custon_Diagnostics | Summary_ISO26262 | Detailed_ISO26262 | Summary_IEC61508 | Detailed_IEC61508

FIT Estimation

Product Function Tailoring

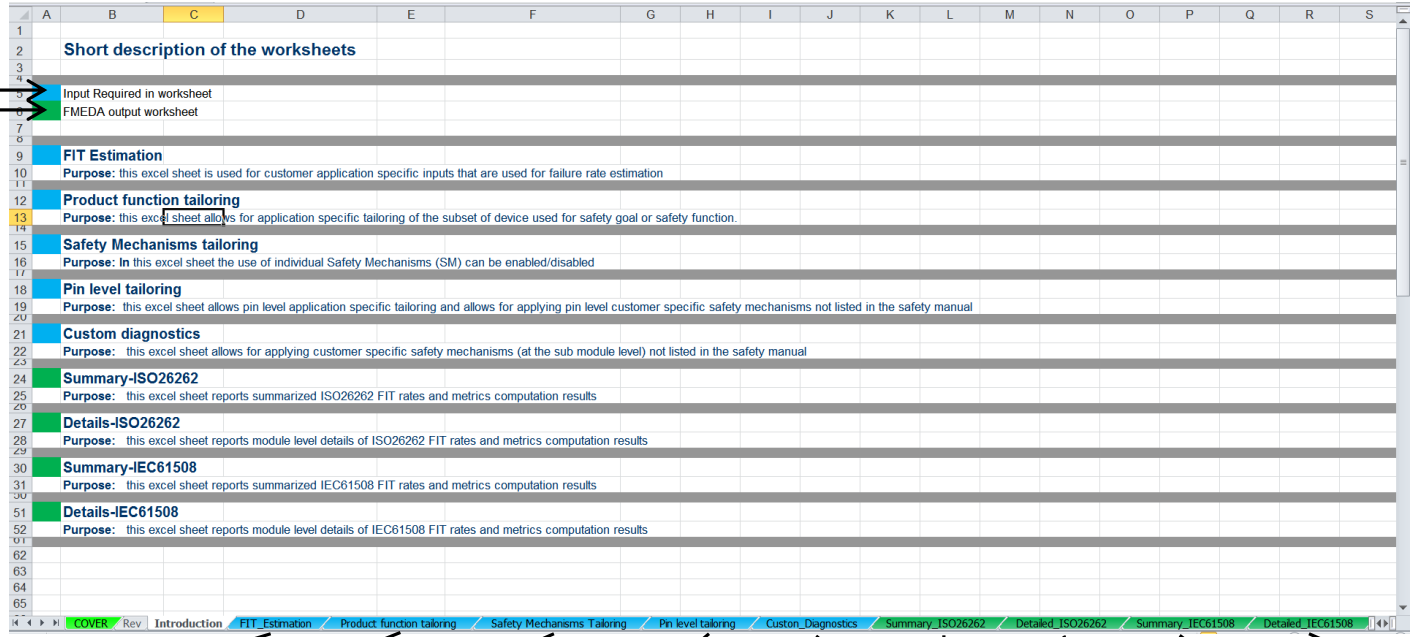
Safety Mechanism Tailoring

Pin Level Tailoring

Custom Diagnostics

FMEDA | Customize to your requirements

Blue Tabs
Green Tabs



Short description of the worksheets

Input Required in worksheet
FMEDA output worksheet

FIT Estimation
Purpose: this excel sheet is used for customer application specific inputs that are used for failure rate estimation

Product function tailoring
Purpose: this excel sheet allows for application specific tailoring of the subset of device used for safety goal or safety function.

Safety Mechanisms tailoring
Purpose: In this excel sheet the use of individual Safety Mechanisms (SM) can be enabled/disabled

Pin level tailoring
Purpose: this excel sheet allows pin level application specific tailoring and allows for applying pin level customer specific safety mechanisms not listed in the safety manual

Custom diagnostics
Purpose: this excel sheet allows for applying customer specific safety mechanisms (at the sub module level) not listed in the safety manual

Summary-ISO26262
Purpose: this excel sheet reports summarized ISO26262 FIT rates and metrics computation results

Details-ISO26262
Purpose: this excel sheet reports module level details of ISO26262 FIT rates and metrics computation results

Summary-IEC61508
Purpose: this excel sheet reports summarized IEC61508 FIT rates and metrics computation results

Details-IEC61508
Purpose: this excel sheet reports module level details of IEC61508 FIT rates and metrics computation results

COVER | Rev | Introduction | FIT_Estimation | Product function tailoring | Safety Mechanisms Tailoring | Pin level tailoring | Custon_Diagnostics | Summary_ISO26262 | Detailed_ISO26262 | Summary_IEC61508 | Detailed_IEC61508

FIT Estimation | Product Function Tailoring | Safety Mechanism Tailoring | Pin Level Tailoring | Custom Diagnostics | Summary ISO26262 | Detailed ISO26262 | Summary IEC61508 | Detailed IEC61508

Application-specific customization of FMEDA

Assumed safety integrity target for MCU ASIL-B (Default)

C28x CPU is safety related and requires to satisfy,

CPU SPFM > 90%
CPU LFM > 60%

6.2.8 Reciprocal Comparison by Software

Each CPU subsystem has a pair of diverse processing units (C28 and CLA) with different architecture and instruction set. This enables one processing unit to be used for handling the time critical portion code (control CPU) and other processing unit (supervisor CPU) to execute non critical portion of the code, perform diagnostic functions and supervise execution of the control CPU as indicated in Figure 13.

In case of identification of fault during diagnostic functions of the supervisor CPU, it can cause the C2000 MCU to move to a safe state. This concept, "reciprocal comparison by software in separate processing units" acts as a 1oo1D structure providing high diagnostic coverage for the processing units as per ISO26262-5, Table D.4. The comparison need to be performed several times during a FTTI. Reciprocal comparison is a software diagnostic feature and hence care should be taken to avoid common mode failures. The final attained coverage will depend on quality of comparison (determined by extend and frequency of cross checking). The proposed cross checking mechanism allows for hardware and software diversity since different processors with different instruction set and compiler is used for enabling this. The diversity can be further increased by having separate algorithms being executed in both the cores. In case, failure is identified during reciprocal comparison, NMI can be triggered by software and this in turn will assert ERRORSTS.

(DC = 90%)

Application-specific customization of FMEDA

Assumed safety integrity target for MCU ASIL-B (Default)

C28x CPU is safety related and requires to satisfy,

CPU SPFM > 90%
CPU LFM > 60%

Updated target for CPU - ASIL-D

SPFM>99%
LFM>90%

Change in Safety Requirements or Safety concept

6.2.8 Reciprocal Comparison by Software

Each CPU subsystem has a pair of diverse processing units (C28 and CLA) with different architecture and instruction set. This enables one processing unit to be used for handling the time critical portion code (control CPU) and other processing unit (supervisor CPU) to execute non critical portion of the code, perform diagnostic functions and supervise execution of the control CPU as indicated in Figure 13.

In case of identification of fault during diagnostic functions of the supervisor CPU, it can cause the C2000 MCU to move to a safe state. This concept, "reciprocal comparison by software in separate processing units" acts as a 1oo1D structure providing high diagnostic coverage for the processing units as per ISO26262-5, Table D.4. The comparison need to be performed several times during a FTTI. Reciprocal comparison is a software diagnostic feature and hence care should be taken to avoid common mode failures. The final attained coverage will depend on quality of comparison (determined by extend and frequency of cross checking). The proposed cross checking mechanism allows for hardware and software diversity since different processors with different instruction set and compiler is used for enabling this. The diversity can be further increased by having separate algorithms being executed in both the cores. In case, failure is identified during reciprocal comparison, NMI can be triggered by software and this in turn will assert ERRORSTS.

(DC = 90%)

Application-specific customization of FMEDA

Assumed safety integrity target for MCU ASIL-B (Default)

C28x CPU is safety related and requires to satisfy,

CPU SPFM > 90%
CPU LFM > 60%

Updated target for CPU - ASIL-D

SPFM>99%
LFM>90%

Change in Safety Requirements or Safety concept

6.2.8 Reciprocal Comparison by Software

Each CPU subsystem has a pair of diverse processing units (C28 and CLA) with different architecture and instruction set. This enables one processing unit to be used for handling the time critical portion code

6.2.x My New Custom1 Safety Mechanism

This is our new safety mechanism implemented at application level, achieves **higher diagnostic coverage (99%)** due to application level redundancy of processing units with diverse software implementation. This safety mechanism will **replace** already existing safety mechanism *CPU1 – Reciprocal comparison by Software*.

diversity since different processors with different instruction set and compiler is used for enabling this. The diversity can be further increased by having separate algorithms being executed in both the cores. In case, failure is identified during reciprocal comparison, NMI can be triggered by software and this in turn will assert ERRORSTS.

DiagnosticCoverageofcustomersafetymechanisms	SM	Resulttype	on/off
99.000%	New1	E	1

Application-specific customization of FMEDA

Assumed safety integrity target for MCU ASIL-B (Default)

C28x CPU is safety related and requires to satisfy,

CPU SPFM > 90%
CPU LFM > 60%

Updated target for CPU - ASIL-D

SPFM>99%
LFM>90%

Change in Safety Requirements or Safety concept

6.2.8 Reciprocal Comparison by Software

Each CPU subsystem has a pair of diverse processing units (C28 and CLA) with different architecture and instruction set. This enables one processing unit to be used for handling the time critical portion code

6.2.x My New Custom1 Safety Mechanism

This is our new safety mechanism implemented at application level, achieves **higher diagnostic coverage (99%)** due to application level redundancy of processing units with diverse software implementation. This safety mechanism will **replace** already existing safety mechanism *CPU1 – Reciprocal comparison by Software*.

diversity since different processors with different instruction set and compiler is used for enabling this. The diversity can be further increased by having separate algorithms being executed in both the cores. In case, failure is identified during reciprocal comparison, NMI can be triggered by software and this in turn will assert ERRORSTS.

DiagnosticCoverageofcustomersafetymechanisms	SM	Resulttype	on/off
99.000%	New1	E	1

Change in device usage in safety-related application

Inputs for application specific tailoring of failure rates

Memory size

Type	Total Size	User Size	Unit
CPU1-Mx	4	4	Kbytes
CPU1-Dx	8	8	Kbytes
CPU1-LSx	24	24	Kbytes
CPU2-Mx	4	4	Kbytes
CPU2-Dx	8	8	Kbytes
CPU2-LSx	24	24	Kbytes
GSx	128	128	Kbytes
FLASH	1	1	Mbytes

Modules used for Safety Function / Safety Goal

	CPU SubSystem	CPU1_CORE	YES
	CPU SubSystem	CPU2_CORE	YES
	CPU SubSystem	MCLA1	YES
	CPU SubSystem	MCLA2	YES
	CPU SubSystem	Cpu1_DCSM	YES
	CPU SubSystem	Cpu2_DCSM	YES
	SYSTEM	CPU1 TIMER0	YES
	SYSTEM	CPU1 TIMER1	YES

Application-specific customization of FMEDA

Assumed safety integrity target for MCU ASIL-B (Default)

C28x CPU is safety related and requires to satisfy,

CPU SPFM > 90%
CPU LFM > 60%

Updated target for CPU - ASIL-D

SPFM>99%
LFM>90%

Change in Safety Requirements or Safety concept

6.2.8 Reciprocal Comparison by Software

Each CPU subsystem has a pair of diverse processing units (C28 and CLA) with different architecture and instruction set. This enables one processing unit to be used for handling the time critical portion code

6.2.x My New Custom1 Safety Mechanism

This is our new safety mechanism implemented at application level, achieves **higher diagnostic coverage (99%)** due to application level redundancy of processing units with diverse software implementation. This safety mechanism will **replace** already existing safety mechanism *CPU1 – Reciprocal comparison by Software*.

diversity since different processors with different instruction set and compiler is used for enabling this. The diversity can be further increased by having separate algorithms being executed in both the cores. In case, failure is identified during reciprocal comparison, NMI can be triggered by software and this in turn will assert ERRORSTS.

DiagnosticCoverageofcustomersafetymechanisms	SM	Resulttype	on/off
99.000%	New1	E	1

Change in device usage in safety-related application

Inputs for application specific tailoring of failure rates

Memory size

Type	Total Size	User S	User Size	Unit
CPU1-Mx	4	4	2.9	Kbytes
CPU1-Dx	8	8	8	Kbytes
CPU1-LSx	24	24	10	Kbytes
CPU2-Mx	4	4	3.5	Kbytes
CPU2-Dx	8	8	7.2	Kbytes
CPU2-LSx	24	24	16	Kbytes
GSx	128	128	98	Kbytes
FLASH	1	1	0.8	Mbytes

Modules used for Safety Function / Safety Goal

	CPU SubSystem	CPU1_CORE	YES	YES
	CPU SubSystem	CPU2_CORE	YES	YES
	CPU SubSystem	MCLA1	YES	NO
	CPU SubSystem	MCLA2	YES	NO
	CPU SubSystem	Cpu1_DCSM	YES	YES
	CPU SubSystem	Cpu2_DCSM	YES	YES
	SYSTEM	CPU1 TIMER0	YES	YES
	SYSTEM	CPU1 TIMER1	YES	YES

Application-specific customization of FMEDA

Assumed safety integrity target for MCU ASIL-B (Default)

C28x CPU is safety related and requires to satisfy,

CPU SPFM > 90%
CPU LFM > 60%

Updated target for CPU - ASIL-D

SPFM>99%
LFM>90%

Change in Safety Requirements or Safety concept

6.2.8 Reciprocal Comparison by Software

Each CPU subsystem has a pair of diverse processing units (C28 and CLA) with different architecture and instruction set. This enables one processing unit to be used for handling the time critical portion code

6.2.x My New Custom1 Safety Mechanism

This is our new safety mechanism implemented at application level, achieves **higher diagnostic coverage (99%)** due to application level redundancy of processing units with diverse software implementation. This safety mechanism will **replace** already existing safety mechanism *CPU1 – Reciprocal comparison by Software*.

diversity since different processors with different instruction set and compiler is used for enabling this. The diversity can be further increased by having separate algorithms being executed in both the cores. In case, failure is identified during reciprocal comparison, NMI can be triggered by software and this in turn will assert ERRORSTS.

DiagnosticCoverageofcustomersafetymechanisms	SM	Resulttype	on/off
99.000%	New1	E	1

Change in device usage in safety-related application

Inputs for application specific tailoring of failure rates

Memory size

Type	Total Size	User S	User Size	Unit
CPU1-Mx	4	4	2.9	Kbytes
CPU1-Dx	8	8	8	Kbytes
CPU1-LSx	24	24	10	Kbytes
CPU2-Mx	4	4	3.5	Kbytes
CPU2-Dx	8	8	7.2	Kbytes
CPU2-LSx	24	24	16	Kbytes
GSx	128	128	98	Kbytes
FLASH	1	1	0.8	Mbytes

Modules used for Safety Function / Safety Goal

	CPU SubSystem	CPU1_CORE	YES	YES
	CPU SubSystem	CPU2_CORE	YES	YES
	CPU SubSystem	MCLA1	YES	NO
	CPU SubSystem	MCLA2	YES	NO
	CPU SubSystem	Cpu1_DCSM	YES	YES
	CPU SubSystem	Cpu2_DCSM	YES	YES
	SYSTEM	CPU1 TIMER0	YES	YES
	SYSTEM	CPU1 TIMER1	YES	YES

Customer input for failure rate estimation

Package Used — TI ZWT

Customer input for transient fault estimation
Application specific Flux Factor coeff. based on Jedec JESD89A — 1

Maximum power dissipation
Application specific power dissipation in Watts — 1.4
(0.8W is based on maximum datasheet value)

Safe / Dangerous Ratio — 0%
Derating to be applied to FIT rates

Confidence Level
Desired confidence level of FIT rates — 70%

Change in mission profile

Operational Profile from IEC/TR 62380:2004

	Temp1		Temp2		Temp3		Ratios on/off		2 night starts		4 day light starts		Non used vehicle	
	$(t_{jc})_1$ °C	τ1	$(t_{jc})_2$ °C	τ2	$(t_{jc})_3$ °C	τ3	T_{on}	T_{off}	n_1	$\Delta T_{1\ °C}$	n_2	ΔT_2	n_3	ΔT_3
Profile	32	0.02	60	0.015	85	0.023	0.058	0.942	670	ΔTj/3+55	1340	ΔTj/3+45	30	10

Application-specific customization of FMEDA

Assumed safety integrity target for MCU ASIL-B (Default)

C28x CPU is safety related and requires to satisfy,

CPU SPFM > 90%
CPU LFM > 60%

Updated target for CPU - ASIL-D

SPFM>99%
LFM>90%

Change in Safety Requirements or Safety concept

6.2.8 Reciprocal Comparison by Software

Each CPU subsystem has a pair of diverse processing units (C28 and CLA) with different architecture and instruction set. This enables one processing unit to be used for handling the time critical portion code

6.2.x My New Custom1 Safety Mechanism

This is our new safety mechanism implemented at application level, achieves **higher diagnostic coverage (99%)** due to application level redundancy of processing units with diverse software implementation. This safety mechanism will **replace** already existing safety mechanism *CPU1 – Reciprocal comparison by Software*.

diversity since different processors with different instruction set and compiler is used for enabling this. The diversity can be further increased by having separate algorithms being executed in both the cores. In case, failure is identified during reciprocal comparison, NMI can be triggered by software and this in turn will assert ERRORSTS.

DiagnosticCoverageofcustomersafetymechanisms	SM	Resulttype	on / off
99.000%	New1	E	1

Change in device usage in safety-related application

Inputs for application specific tailoring of failure rates

Memory size

Type	Total Size	User S	User Size	Unit
CPU1-Mx	4	4	2.9	Kbytes
CPU1-Dx	8	8	8	Kbytes
CPU1-LSx	24	24	10	Kbytes
CPU2-Mx	4	4	3.5	Kbytes
CPU2-Dx	8	8	7.2	Kbytes
CPU2-LSx	24	24	16	Kbytes
GSx	128	128	98	Kbytes
FLASH	1	1	0.8	Mbytes

Modules used for Safety Function / Safety Goal

	CPU SubSystem	CPU1_CORE	YES	YES
	CPU SubSystem	CPU2_CORE	YES	YES
	CPU SubSystem	MCLA1	YES	NO
	CPU SubSystem	MCLA2	YES	NO
	CPU SubSystem	Cpu1_DCSM	YES	YES
	CPU SubSystem	Cpu2_DCSM	YES	YES
	SYSTEM	CPU1 TIMER0	YES	YES
	SYSTEM	CPU1 TIMER1	YES	YES

Customer input for failure rate estimation

Package Used — TI ZWT — TI PTP

Customer input for transient fault estimation
Application specific Flux Factor coeff. based on Jedec JESD89A — 1

Maximum power dissipation
Application specific power dissipation in Watts — 1.4 — 0.8
(0.8W is based on maximum datasheet value)

Safe / Dangerous Ratio — 0%
Derating to be applied to FIT rates

Confidence Level
Desired confidence level of FIT rates — 70%

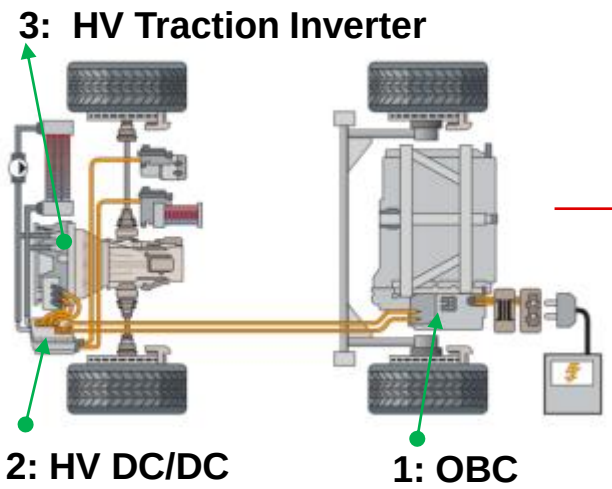
Change in mission profile

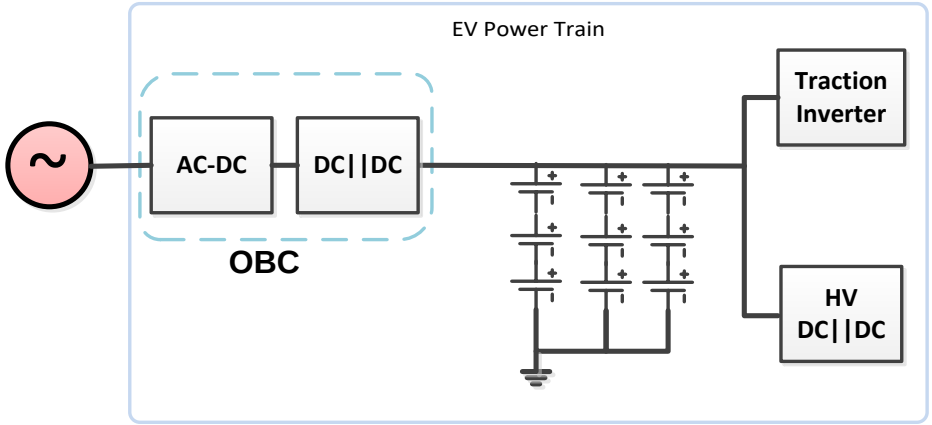
Operational Profile from IEC/TR 62380:2004

	Temp1		Temp2		Temp3		Ratios on/off		2 night starts		4 day light starts		Non used vehicle	
	$(t_{ac})_1$ °C	$\tau 1$	$(t_{ac})_2$ °C	$\tau 2$	$(t_{ac})_3$ °C	$\tau 3$	T_{on}	T_{off}	n_1	$\Delta T_{1\ °C}$	n_2	ΔT_2	n_3	ΔT_3
Profile	32	0.02	60	0.015	85	0.023	0.058	0.942	670	ΔTj/3+55	1340	ΔTj/3+45	30	10

125

High-voltage applications in automotive EV/HEV





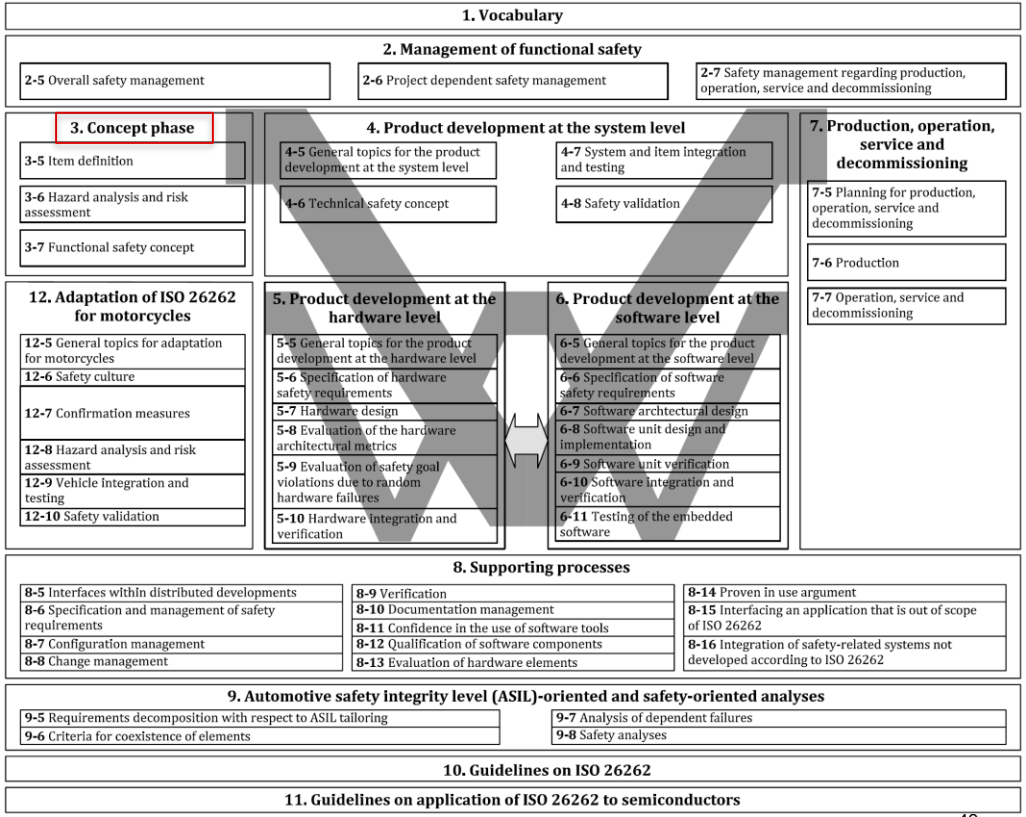
Top EV market care-about:

- Mechanical cost reduction
- Greater efficiency, Increased driving range + Safety, Security

EV/HEV market trends:

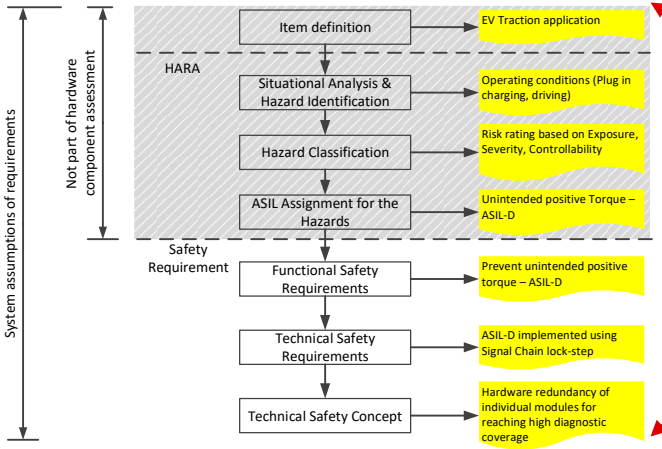
- Integration of powertrain sub-systems
  - OBC+ DC/DC | DC/DC+HVAC | OBC+DC/DC+traction
- GaN: higher switching frequency w/ C2000

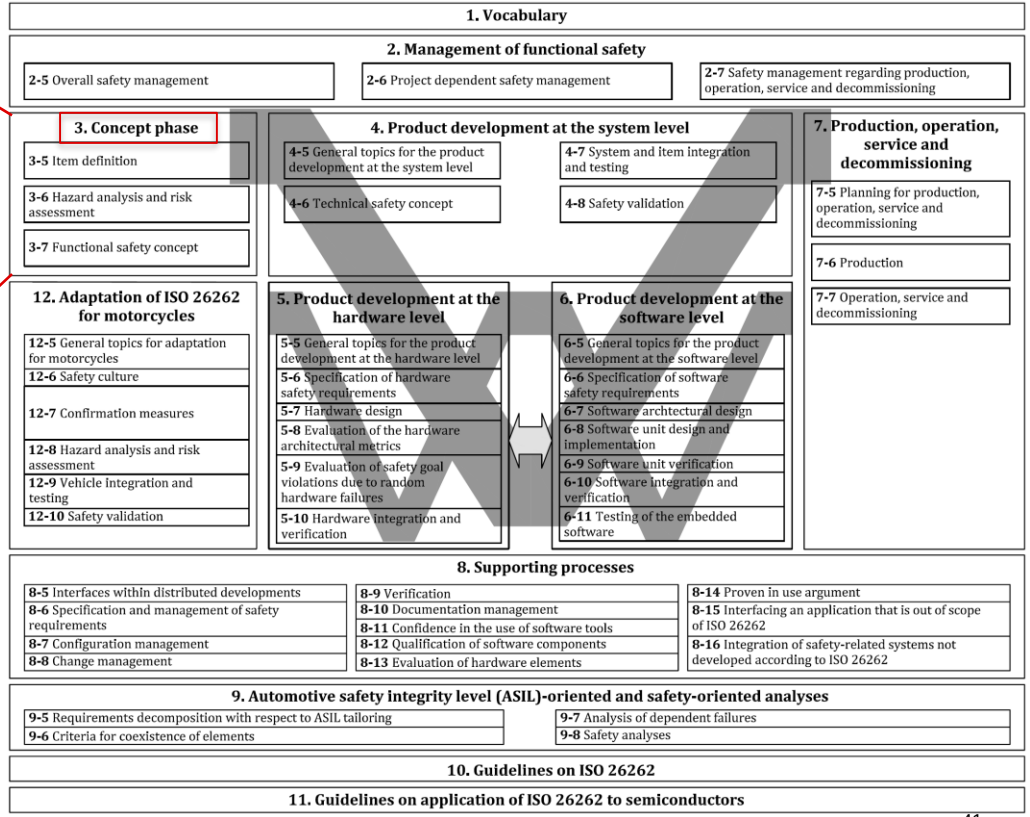
ISO 26262 V-model of development & safety concept



Source: ISO 26262-1:2018 Figure 1 — Overview of the ISO 26262 series of standards

ISO 26262 V-model of development & safety concept

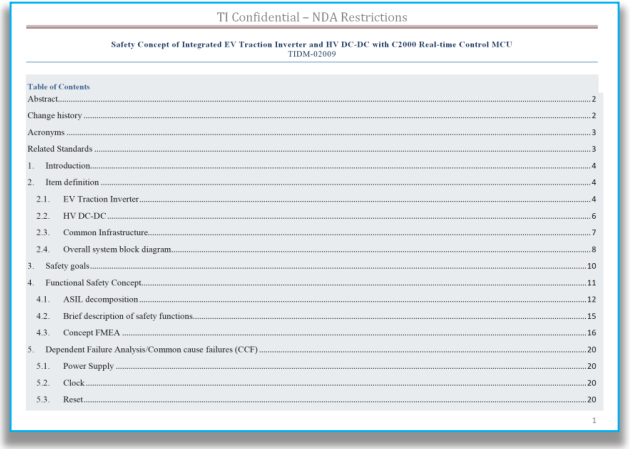




Source: ISO 26262-1:2018 Figure 1 — Overview of the ISO 26262 series of standards

- TI's Reference design with Functional Safety Concept Assessed by TUV-SUD, helps improve time to market for system integrators.

EV traction reference design | safety concept assessment by TUV-SUD



TI Confidential – NDA Restrictions

Safety Concept of Integrated EV Traction Inverter and HV DC-DC with C2000 Real-time Control MCU
TIDM-02009

Table of Contents

1

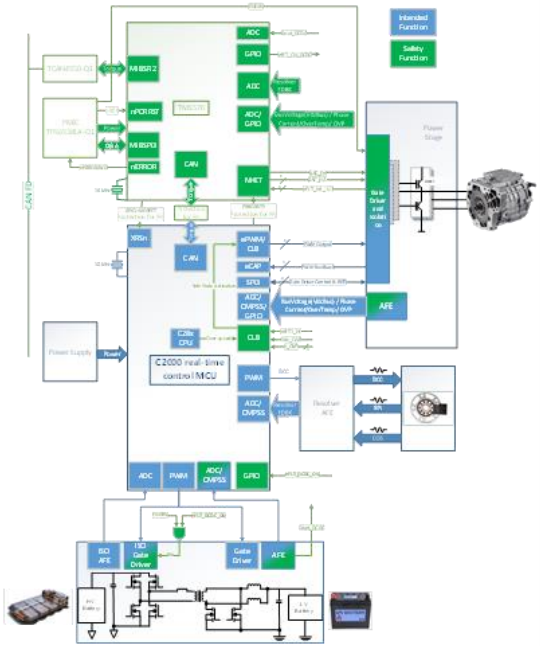
SI No:	Hazard	Safety Goal	Assumed System Safe State	MCU Safe State	ASIL	FTTI
EVTR_SG1	Motor over-torque	Avoid over-torque	Torque off Driver indication	(i) PWM Tripped (ii) ERROR reported	D	10ms
EVTR_SG2	Too low torque	Avoid unintended low torque	Driver indication	(i) ERROR reported	A	10ms
EVTR_SG3	Motor over speed	Avoid over speed	Apply torque off (over-speed) or apply ASC (over-Voltage & over-speed) Driver indication	(i) PWM Tripped (ii) ERROR reported	D	10ms
EVTR_SG4	Motor or inverter operating beyond permissible temp	Avoid operation of motor and inverter beyond the permissible temperature range	Limit Torque Driver indication	(i) Limit Torque (ii) ERROR reported	B	10ms

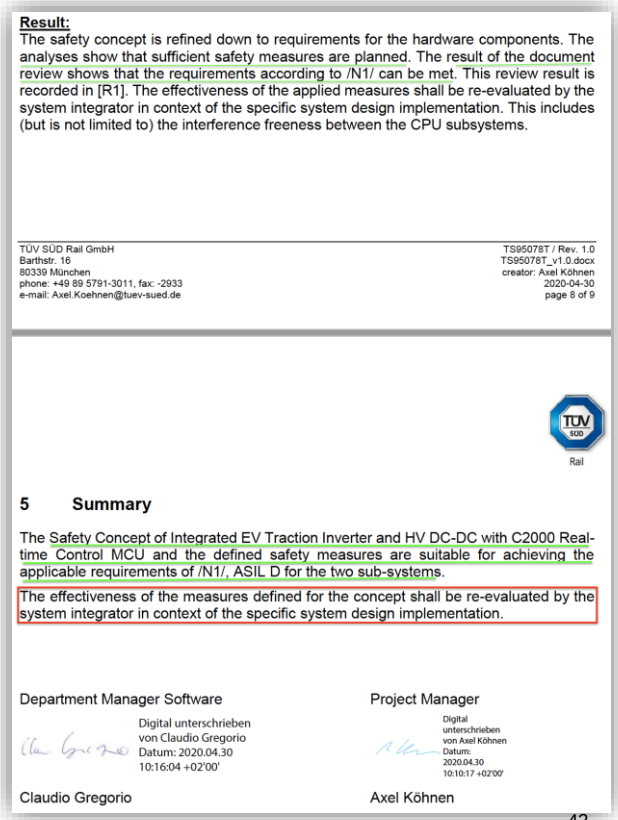
Table 1: EV traction inverter safety goals

following tables describe safety goals assumed for the HV DC-DC system.

SI No:	Hazard	Safety Goal	Assumed System Safe State	MCU Safe State	ASIL	FTTI
EVTR_SG5	Overvoltage on DC-DC output	Avoid over 14V on the LV side of DC-DC for more than continuous 10 ms	Turn off DC-DC and Driver indication	(i) Disable primary (HV side) gate driver (ii) ERROR reported	D	100 ms
EVTR_SG6	Overvoltage on DC-DC output	Avoid instantaneous over 16V on the LV side of DC-DC	Turn off DC-DC and Driver indication	(i) Disable primary (HV side) gate driver (ii) ERROR reported	D	100 us

Table 2: HV DCDC safety goals





Result:
The safety concept is refined down to requirements for the hardware components. The analyses show that sufficient safety measures are planned. The result of the document review shows that the requirements according to /N1/ can be met. This review result is recorded in [R1]. The effectiveness of the applied measures shall be re-evaluated by the system integrator in context of the specific system design implementation. This includes (but is not limited to) the interference freeness between the CPU subsystems.

TÜV SÜD Rail GmbH
Barthstr. 16
80339 München
phone: +49 89 5791-3011, fax: -2933
e-mail: Axel.Koehnen@tuev-sued.de

TS95078T / Rev. 1.0
TS95078T_v1.0.docx
creator: Axel Köhnen
2020-04-30
page 8 of 9

Rail

5 Summary

The Safety Concept of Integrated EV Traction Inverter and HV DC-DC with C2000 Real-time Control MCU and the defined safety measures are suitable for achieving the applicable requirements of /N1/, ASIL D for the two sub-systems.

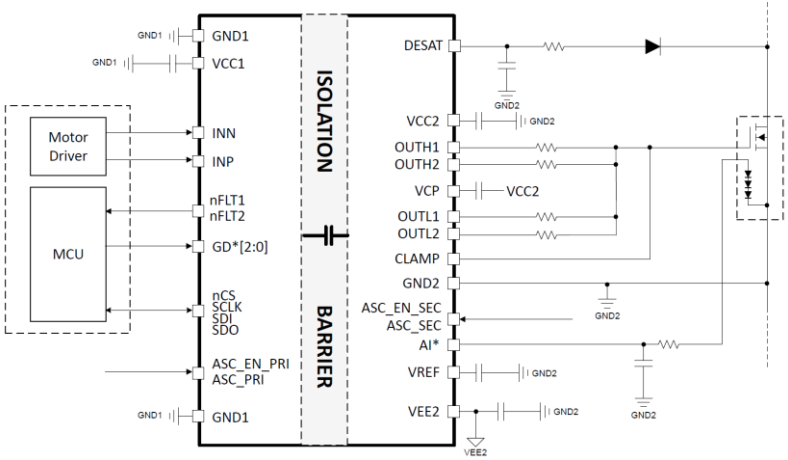
The effectiveness of the measures defined for the concept shall be re-evaluated by the system integrator in context of the specific system design implementation.

Department Manager Software
Digital unterschrieben von Claudio Gregorio
Datum: 2020.04.30 10:16:04 +02'00'
Claudio Gregorio

Project Manager
Digital unterschrieben von Axel Köhnen
Datum: 2020.04.30 10:10:17 +02'00'
Axel Köhnen

Request for Access : C2000 Safety package

UCC5880-Q1 | Isolated gate driver with advanced protection features



- **Functional Safety-Compliant**
  - System design up to ASIL D (ISO 26262)
  - AEC-Q100 qualified
- **Integrated diagnostics:**
  - Built-in self-test (BIST) for protection comparators
  - INP to transistor gate path integrity
  - ISO communication data integrity check
  - Internal clock monitoring, Integrated 10-bit ADC
  - Fault alarm and warning outputs (nFLT*)
  - Gate threshold voltage measurement for power device health monitoring
- **Protection Features**
  - Overcurrent protection with 75-ns response time
  - Programmable soft turnoff and two-level soft turnoff
  - ASC – Active Short Circuit Protection
  - Advanced VCE/VDS clamping circuit
  - Supply Undervoltage and overvoltage protection
  - Active output pulldown and default low outputs
  - Driver die temperature sensing and overtemperature protection

How does TI help | Streamline your functional safety system certification

http://www.ti.com/technologies/functional-safety/overview.html

		Functional Safety-Capable The simplest product category of analog products that can be evaluated for use in a functionally safe system	Functional Safety Quality-Managed Moderately complex products such as an MCU	Functional Safety-Compliant The most complex products such as MCUs, microprocessors and complex analog signal-chain products
Development process	TI quality-managed process	✓	✓	✓
	TI functional safety process			✓
Analysis report	Functional safety FIT rate calculation	✓	✓	✓
	Failure mode distribution (FMD) and/or pin FMA*	✓	Included in FMEDA	Included in FMEDA
	FMEDA		✓	✓
	Fault-tree analysis (FTA)**			✓
Diagnostics description	Functional safety manual		✓	✓
Certification	Functional safety product certificate**			✓


CERTIFICATE
No. Z10 084071 0024 Rev. 00

Holder of Certificate: Texas Instruments Incorporated
13405 University Blvd.
Sugar Land TX 77479
USA

Certification Mark:

Product: Safety components
Safety MCUs

The product was tested on a voluntary basis and complies with the essential requirements.
The certification mark shown above can be affixed on the product. It is not permitted to alter the
certificate in any way. Only the complete certificate may be reproduced or made available
to third parties. This certificate is valid until the latest date, unless it is cancelled earlier. All applicable
requirements of the testing and certification regulations of TÜV SÜD Group have to be complied.
For details see: www.tuvsud.com/ps-cert

Test report no.: TÜ065/18C

Valid until: 2027-12-12

Date, 2022-12-16

(Guido Neumann)

Page 1 of 2
TÜV SÜD Product Service GmbH – Certification Body – Ridlerstraße 65 – 80339 Munich – Germany

TMS320F2838x TUV-SUD Safety Certificate:
www.ti.com/lit/cr/sszqqm2/sszqqm2.pdf

** May only be available for analog power and signal chain products. ** Available for select products.*

Conclusions

- High-voltage technologies provide **energy efficiencies** and are key to a **sustainable future**
- **Semiconductor solutions** are necessary for a safer human interface with HV systems
- Industrial and automotive Functional Safety requirements have commonalities and differences
- TI products and support tools enable both types of applications and help **accelerate your time to market**
  - Compliant/certified products with differentiated Hardware features for Functional Safety
  - System-level safety concept collateral & support
  - Software support libraries

References

1. Texas Instruments functional safety landing page: https://www.ti.com/technologies/functional-safety.html
2. Streamlining Functional Safety Certification in Automotive and Industrial: https://www.ti.com/lit/pdf/ssiy007
3. TÜV SÜD-assessed safe torque off (STO) reference design for industrial drives (IEC 61800-5-2): https://www.ti.com/tool/TIDA-01599
4. UCC21750 5.7kVrms ±10A, single-channel isolated gate driver w/ DESAT & internal miller clamp for IGBT/SiCFETs, https://www.ti.com/product/UCC21750
5. TPS22918-Q1 1-ch, 5.5-V, 2-A, 52-mΩ automotive load switch with adj. rise time and adj. output discharge, https://www.ti.com/product/TPS22918-Q1
6. UCC5880-Q1 Isolated 20-A Adjustable Gate Drive IGBT/SiC MOSFET Gate Driver With Advanced Protection Features For Automotive Applications
7. Understanding failure modes in isolators
8. Industrial Functional Safety for C2000™ Real-Time Microcontrollers: https://www.ti.com/lit/ml/swab013b/swab013b.pdf
9. TMS320F2838x TUV-SUD Safety Certificate: www.ti.com/lit/cr/sszqqm2/sszqqm2.pdf
10. IEC 61800-5-2: 2016 - Adjustable speed electrical power drive systems. Part 5-2. Functional safety requirements
11. ISO 13849-2:2012 Safety of machinery — Safety-related parts of control systems — Part 2: Validation

Please join our live Q&A