Functional Safety Information

Overview STO Concept TIDA-01599

Table of Contents

Trademarks

Table 1-1. Revision History

Revision	Date	Name	Change
1.2	2018/10/25	Navaneeth Kumar N (TI), Anant Kamath (TI)	Version shared with TUEV SUED for feedback. Refer to “Review Protocol_Concept V1.0.docx”
1.3	2021/08/04	M. Staebler (TI)	Changed format to according to TUEV template, added additional references, added further info on conditions of use/assumptions and STO_1 and STO_2 subsystems. Adjusted MCU signal names on schematics to reflect input or output signal w/ MCU. Added info on reinforced isolated gate driver ISO5852S, and pin-compatible ISO5452.
1.4	2021/09/23	M. Staebler (TI)	Updated conditions of use, removed the STO latching feature, added table to explain U7 load switch QOD.
1.5	2021/09/29	M. Staebler (TI)	Updated figure 3 which shows STO_1 subsystem (added second transistor Q3 for redundant VCC clamp), added reference to IEC 615008-2 table A DC fault model. Updated figure 4 to match the schematics rev E2
1.6.	2021/11/11	M. Staebler, C. Gao (TI)	Added STO_FB channel, updated block diagram, added description of STO-FB logic and updated system FMEA and references. Modified file name to include STO.
1.6a	2022/01/31	M. Staebler (TI)	No change in content, corrected typos only.
1.6b	2022/05/18	M. Staebler (TI)	Correction to *FMEA STO Concept TIDA-01599* secure link

1 Scope

This document describes a concept implementation of the safety function safe torque off (STO) according to IEC 61800-5-2 for a three-phase IGBT inverter for industrial drives.

The STO subsystem is based on the TI **TIDA-01599** reference design and utilizes a dual-channel approach with HFT = 1 specifically for isolated IGBT gate drivers with CMOS and TTL logic input like TI's reinforced isolated gate driver ISO5852S or ISO5452.

The safety integrity level for the STO function is capable of SIL 3 according to IEC 61508 and category 3 PL e per ISO 13849, as assessed by TÜV SÜD.

2 Related Documents

Table 2-1. Collateral and Documentation References

Document	Description
Design guide	Redundant dual-channel safe torque off (STO) reference design for AC inverters and servo drives, Texas Instruments, TIDA-01599, TIDUDS9 Design files will be updated as reflected in this document.
Schematics	Updated TIDA-01599 schematic rev. E2: TIDA-01599E2.1(001)_Sch.pdf TIDRVA2
Design guide	Wide-Input Isolated IGBT Gate-Drive Fly-Buck Power Supply for Three-Phase Inverters Reference Design, Texas Instruments, TIDA-00199, TIDU670
Data sheet	ISO1211, Single-channel Isolated 24-V to 60-V digital input receiver for digital input modules, Texas Instruments, https://www.ti.com/product/ISO1211
Data sheet	ISO5452, 2.5-A / 5-A 5.7-kV RMS single channel isolated gate driver with split output and protection features, Texas Instruments, https://www.ti.com/product/ISO5452
Data sheet	ISO5852S, 2.5-A / 5-A, 5.7-kV RMS single channel isolated gate driver with split output and protection, Texas Instruments, https://www.ti.com/product/ISO5852S
Data sheet	TPS22919, 5.5-V, 1.5-A, 90-mΩ load switch with adj. output discharge, Texas Instruments, https://www.ti.com/product/TPS22919
Data sheet	TPS27S100, 40-V, 80-mΩ, 4-A, 1-ch, Industrial high-side switch with adjustable current limiting and current, Texas Instruments, https://www.ti.com/product/TPS27S100
Data sheet	TIOS101, TIOS101x Digital Sensor Output Drivers with Integrated Surge Protection, https://www.ti.com/lit/ds/symlink/tios1013.pdf
Data sheet	ISO7710 High Speed, Robust EMC Reinforced Single-Channel Digital Isolator, https://www.ti.com/lit/ds/symlink/iso7710.pdf
Concept FMEA	For access to *FMEA STO Concept TIDA-01599*, use this secure link
Functional safety information	TPS22919-Q1 Functional Safety FIT Rate, FMD and Pin FMA: TPS22919-Q1 FMD_FIT_FMA Document.pdf

3 Related Standards and Acronyms

Table 3-1. Standards References

Standard	Title
IEC 61800-5-2	Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional
IEC 61508	Functional safety of electrical/electronic/programmable electronic safety-related systems
ISO13849-1/2	Safety of machinery -- Safety-related parts of control systems -- Part 1: General principles for design, --- Part 2: Validation
IEC 60204-1	Safety of machinery - Electrical equipment of machines - Part 1: General requirements
IEC 62061	Safety of machinery - Functional safety of safety-related electrical, electronic and programmable electronic control systems(1)

(1) Defines stop category 0, uncontrolled stop

Table 3-2. Acronyms

Acronym	Description
DC	Diagnostic coverage
FIT	Failure in time (1-e9/hour)
HFT	Hardware fault tolerance
MTTF	Mean time to failure (per year)
MTTFd	Mean time to failure – dangerous (per year)
PFD	Probability of dangerous failure
PFH	Average frequency of a dangerous failure of the safety function [per hour]
SFF	Safe failure fraction
PDS/SR	Power drive system, safety related
DFD	Dangerous failure detected. Acronym used on the FMEA tables
DFU	Dangerous failure not detected. Acronym used on the FMEA tables
SF	Safe failure
NEF	No effect failures, failures which don’t have an impact on the safety function. Acronym used in FMEA tables.
FRT	Fault response time
DTI	Diagnostics time interval

4 Concept Overview

4.1 System Block Diagram

Figure 4-1 shows the overall system block diagram.

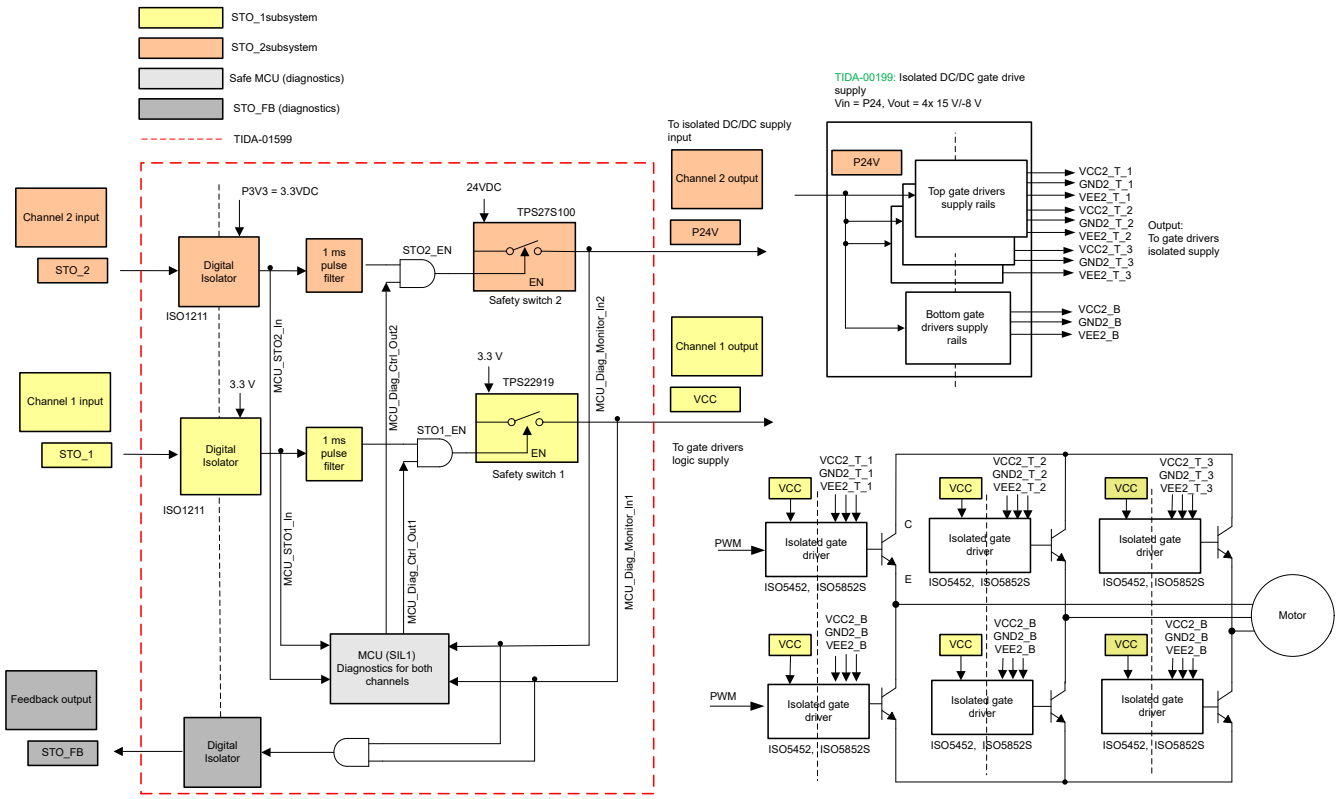

Figure 4-1. High-Level System Block Diagram of TIDA-01599 Concept

STO_1 and STO_2 control the primary and secondary side power supply to the six isolated IGBT gate driver through a power switch (VCC) and a high side switch (P24V) respectively. As long as a logic 1 (+24-V DC) is present at both STO inputs, the motor is operable. If there is a logic 0 (0 V) at one or both of the STO inputs, the power supplies to the gate drivers will be disconnected and the motor coasts down to zero. The use of 1oo2 architecture helps achieve HFT = 1 and only the occurrence of two simultaneous faults can cause failure of the safety function.

The MCU (SIL 1) implements the diagnostics coverage of the STO_1 and STO_2 safe subsystems and sets the system to a safe state, when a fault is detected.

An STO_FB signal is provided to indicate the status of the drive (safe state or normal operation) and can be used to feedback the drive's status to a safety PLC for additional diagnostics, if desired.

4.2 System Specifications

The PDS/SR is a DC-fed 3-phase inverter which supports the function STO (safe torque off) according to IEC 61800-5-2. The STO function supports IEC 60204-1 stop category 0, resulting in an uncontrolled coast stop too. It shall meet IEC61508 SIL 3 and ISO13849 category 3 PL e.

The STO function removes both supply voltages of the six isolated IGBT gate driver supplies. STO_1 removes the logic input supply (VCC) of the isolated gate drivers, STO_2 removes the input supply (P24V) to the isolated multi-output DC/DC, which therefore removes the isolated output supply rails (VCC2/VEE2) to the six isolated IGBT gate drivers, respectively. Due to that the six outputs of the isolated gate drivers are 0 V (off) and the six IGBTs turn-off respectively. In that case the 3-phase IGBT inverter cannot generate a rotating torque to the motor anymore.

The PDS/SR is operating in high demand or continuous mode, where the rate of demands for operation made on safety sub-function is greater than 1 per year.

Table 4-1. TIDA-01599 System Specifications

Parameter	Value	Comment
Safety function	STO	Safe torque off per IEC 61800-5-2
Hardware redundancy (HFT)	HFT = 1 (1oo2)	
IEC 61508 SIL level	SIL 3	
ISO 13849	Category 3, PL e	
Demand mode	Continuous	
SFF/DC	≥ 90% (HFT = 1)	Cat 3 PL e medium DC is ≥90%.
PFH	< 10-7	The quantitative analysis is not part of this concept study.
STO response time	10 ms (nominal), 200 ms (maximum)	The Time between active low STO and gate drive output (Vgs) low, which means power IGBTs are OFF. The quantitative analysis is not part of this concept study.
DTI (Diagnostics test interval)	100 ms (10 Hz)	The quantitative analysis is not part of this concept study. Diagnostics runs at least 10 Hz (load switch STO_1 and load switch for STO_2).
FRT (Fault response time)	< 200 ms	
Mission time (TM)	20 years	
STO input voltage range	24-V DC ±15% (nominal) +/-60-V DC absolute maximum	
STO input logic level, valid > 2 ms	15- to 30-V DC: STO function not engaged <10-V DC: STO function engaged	STO is active low logic input. Input is low-pass filtered to remove OSSD pulses. Valid STO is > 2 ms.
Support of OSSD test pulses	Test pulse duration < 1 ms, maximum repetition frequency 500 Hz	Added low-pass filter to remove (filter-out) the test pulses to avoid trigger STO. Diagnostics for OSSD pulses run at 250 Hz (4-ms rate).
DC supply voltage	24-V DC ±15% (nominal)	
Isolated gate driver supply voltages	Logic supply: 3V3 to 5 V (nominal) Output supply: +15 V, –8 V (nominal)	It is expected that the supply rails are protected to remain below the recommended maximum operating voltage of the selected isolated gate drivers.
Operating ambient temperature	–40°C to 85°C	

4.3 Conditions of use: Assumptions

Refer to Figure 4-1 for a high-level system block diagram of the safety elements, which are the STO_1 and STO_2 safety subsystems and the diagnostics software running on a safety MCU.

The following sections outline the assumptions, which are out of scope with this concept analysis.

4.3.1 Generic Assumptions

- PCB design: The analysis is based on concept and does not include the PCB layout design. The PCB design is out of scope for this analysis
- Over- and undervoltage protection circuits must be assessed in the implementation of this concept design. Out of the scope of this activity.
- Diagnostic and any firmware must be assessed in the implementation of this concept design. Out of the scope of this activity.
- Common cause factors and determination of beta-factor and CCF must be assessed in the implementation of this concept design. Out of the scope of this activity.
- Quantitative analysis (PFH, MTTFd, and so forth) must be assessed in the implementation of this concept design. Out of the scope of this activity

4.3.2 Specific Assumptions

1. Input signals STO_1 and STO_2
   - Input voltage is between 0- and 24-V nominal with worst case of 3.6 V as logic low and 20.4 V as logic high. No intermediate voltage is expected.
   - The logic low (diagnostic pulse) in the STO signal is assumed either to be less than 1 ms or greater than 2 ms. No intermediate values are allowed.
2. Diagnostic coverage of STO_1 and STO_2 and STO_FB subsystems
   - The MCU and the related diagnostic software is excluded in the analysis and is assumed to be developed in accordance with functional safety requirements. The MCU is assumed SIL1 certified and the software implemented accordingly to meet at least SIL1.
3. Output signal STO_FB
   - The output voltage is assumed to be between 0- and 24-V nominal with worst case of 3.6 V as logic low and 20.4 V as logic high. The external supply voltage to the 24-V STO_FB is assumed to be protected against overvoltage and is required to remain within 24 V ±20% tolerance.
4. Power supply rails of STO_1 and STO_2 subsystem
   - P3V3 supply: Assumed to be protected against fault, remains within –20% tolerance (3.9 V max., 2.7 V min. If out of spec, it will be shut down to 0V. When a single protected power supply is used for both STO_1 and STO_2 subsystems, it shall employ two independent protection circuits (HFT = 1).
   - 24-V supply: The 24-V input supply for the P24V is assumed to be protected against fault and remains within ±20% tolerance. If out of spec, it will be shut down to 0 V.
5. Isolated gate drive supply TIDA-00199
   - It is assumed that the quad output rails (VCC2 = +15, VEE2 = –8 V) decay to 0 V within less than 10 ms, after the P24V DC input voltage was disconnected.
   - It is assumed that all faults with TIDA-00199 are safe and yield to a 0-V output voltage for all quad output rails VCC2 and VEE2.
6. Temperature
   - It is assumed the components operate within the recommended operating temperature range. A temperature sensor is required to be added and if the ambient temperature is outside the recommended operating range all safety relevant supplies will be shutdown. This circuit is not part of concept.

4.4 Safe Torque Off Implementation

The *safety function* safe torque off (STO) is implemented by blocking the PWM pulses to the 6 isolated gate drivers ISO5852S (or ISO5452) as well as disable the isolated gate drive supply for all 6 isolated gate drivers ISO5452.

4.4.1 Subsystem Elements

The elements used to implement safe torque off include:

- STO_1 safe subsystem: Set VCC = 0 V, on demand
  - Input: STO_1
  - Output: VCC

  On demand, the VCC input supply of all 6 isolated gate drivers ISO5852S (or ISO5452) is set to 0 V, which set the output of the six ISO5852S (or ISO5452) gate driver to 0 V, hence all six IGBTs turn off. Refer to Section 4.4.3.
- STO_2 safe subsystem: Set P24V = 0 V, on demand
  - Input: STO_2
  - Output: P24V

  On demand, the 24-V input supply P24V to the TIDA-00199 fly-buck converter is disabled. Then the isolated supply voltages of TIDA-00199 (VCC2, VEE2) of all 6 isolated gate drivers ISO5852S (or ISO5452) will decay to 0 V, which set the output of the ISO5852S (or ISO5452) gate driver to 0 V or high-impedance. With the external pull-down resistors, the six IGBTs will turn off. Refer to Section 4.4.4.
- Diagnostic coverage: MCU (SIL 1) software periodically disable the two load switches TPS22919 and TPS27S100 through logic low diagnostic pulse and check if the output of corresponding switches goes low. If a single fault is detected by the diagnostics software, the MCU will continuously drive the diagnostic signals MCU_Diag_Cntrl_Out1 and MCU_Diag_Cntrl_Out2 low, which will move the system to the safe state, where no force producing power is available at the motor. Refer to Section 4.4.5.
- STO_FB: The STO_1 and STO_2 safe subsystem outputs are combined into a single logic feedback STO_FB. STO_FB is active low and indicates the drive state, either normal operation or safe state. The STO_FB signal can be used as monitor to validate the drive status. Refer to Section 4.4.6.

4.4.2 STO Safe Subsystem States and Timing Diagram

Table 4-2 shows the logic table of the safety subsystem. STO_1 and STO_2 are *active low signals*. Logic levels valid for state changes > 1 ms.

Table 4-2. Safety Subsystem Logic Table

Input 1: STO_1	Input 2: STO_2	Output 1: VCC	Output 2: P24V	IGBT Gate Driver Output	State
1	1	1	1	Normal operation	Normal operation
1	0	1	0	0 (off)	STO
0	1	0	1	0 (off)	STO
0	0	0	0	0 (off)	STO

The timing diagram of the STO_1 and STO_2 subsystems are shown in Figure 4-2 and Figure 4-3 respectively. The STO_1 and STO_2 safe subsystems cut the power of the primary and secondary supply of the gate drivers. Due to that, the output voltage OUTH/OUTL of each of the six gate drivers ISO5452 (or ISO5852S) become 0 V.

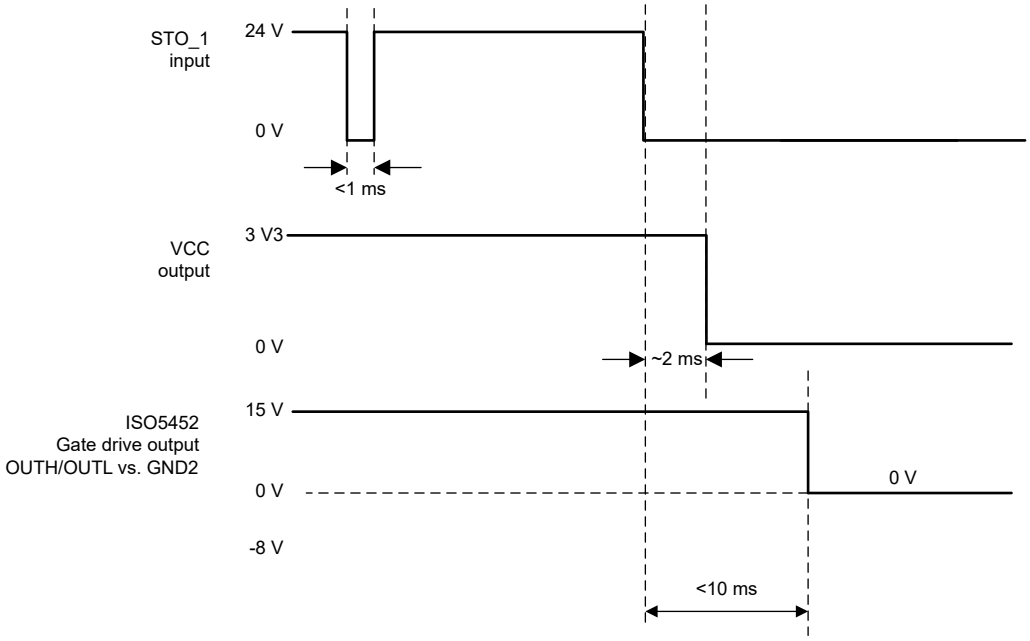

Figure 4-2. Timing Diagram Example ST0_1

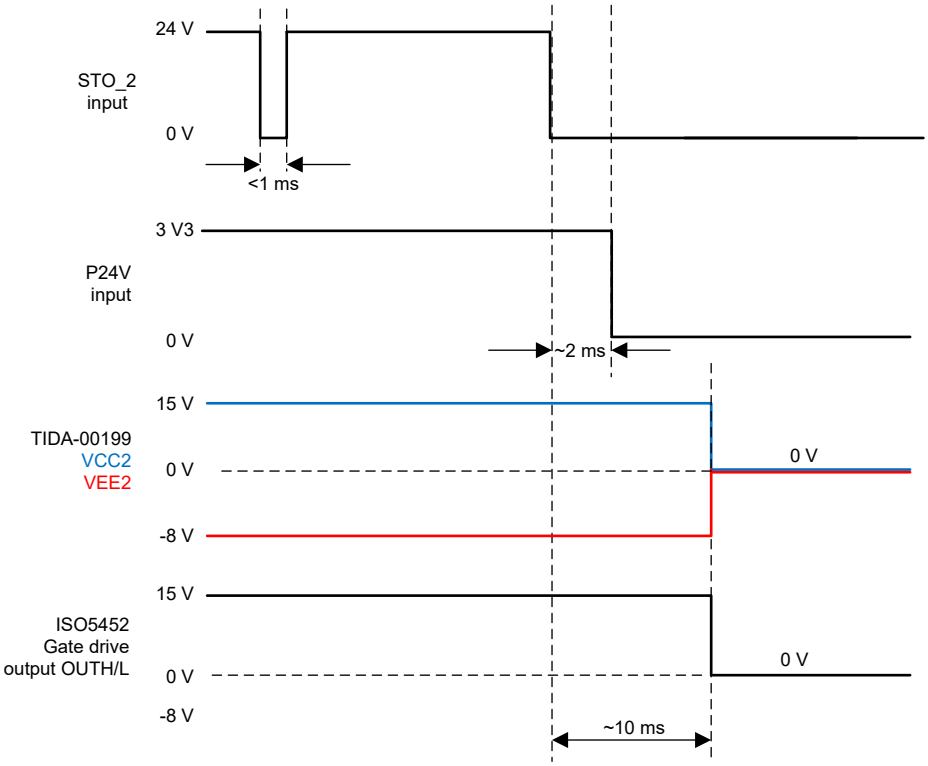

Figure 4-3. Timing Diagram Example ST0_2

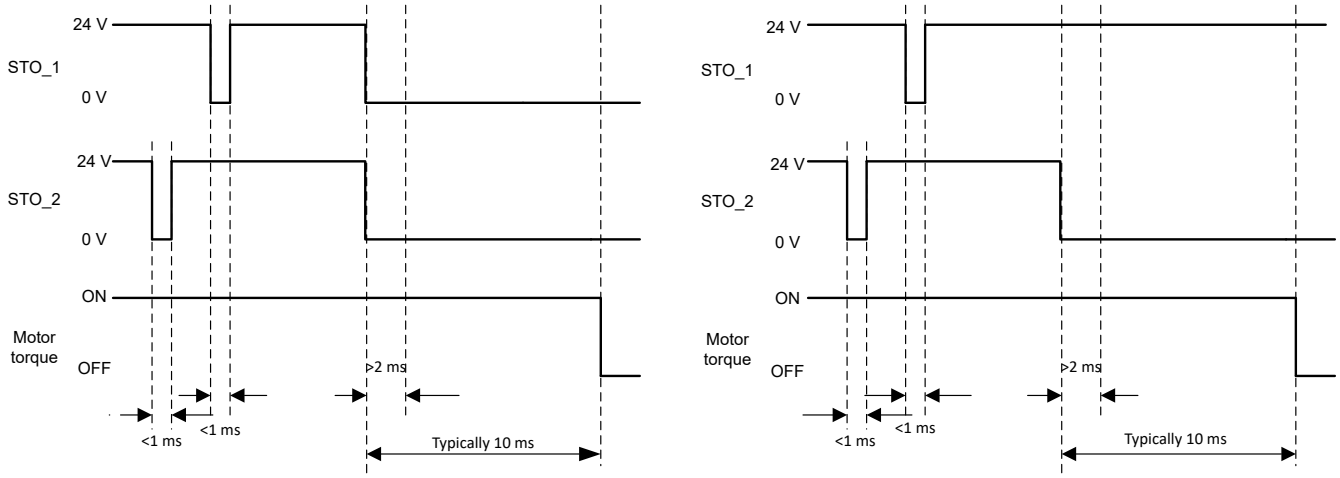

Figure 4-4. STO Timing Diagram Example for Turning Off the Six IGBTs, Which Results in Torque Off

4.4.3 STO_1 Subsystem

Figure 4-5 shows the logic table of the safety subsystem. STO_1 and STO_2 are *active low signals*. Logic levels valid for state changes > 1 ms.

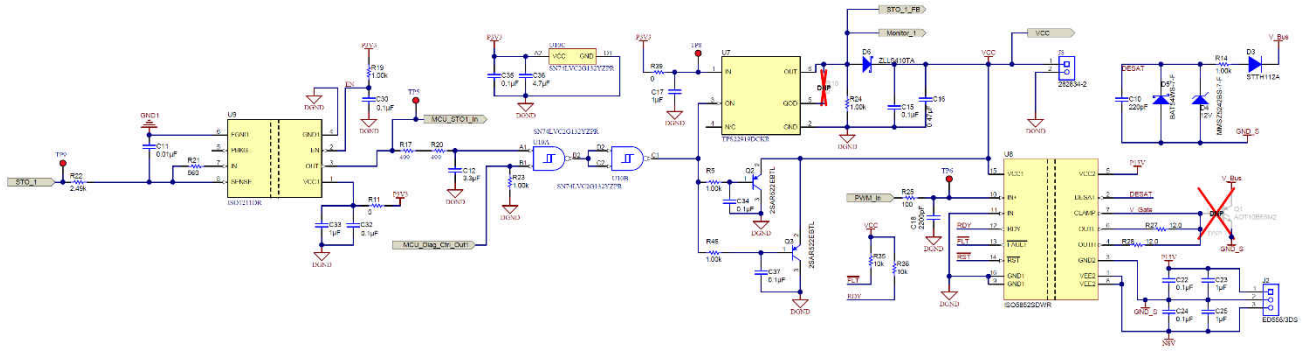

Figure 4-5. STO_1 Subsystem (1oo1d)

The 24-V isolated digital input receiver ISO1211 converts the STO_1 input signal to a 3V3 CMOS level signal. The STO_1 signal from the output of the ISO1211 then pass through low pass RC filter to remove 1ms diagnostics pulses present on STO_1 signal. The output of ISO1211 (MCU_STO_1_In) is also monitored by the MCU (SIL 1) for stuck high faults. The low-pass filtered STO_1 signal is ANDed with MCU diagnostic signal (MCU_Diag_Cntrl_Out1) to generate load switch STO1_EN signal. The STO1_EN signal is used to enable (logic high) and disable (logic low) the load switch, which in turn control the supply voltage VCC of the isolated gate driver ISO5852S (or ISO5452) logic input supply VCC1. Dual redundant PNP bipolar junction transistors Q2 and Q3, actively clamp the logic side gate drive supply VCC to GND when STO_1 is activated. This prevents reverse bias of the VCC supply through the CMOS input gate driver ISO5852S (or ISO5452) in case the PWM signals are still active high (3V3). The STO_1_FB signal used by the STO_FB logic to monitor the state of the drive.

4.4.4 STO_2 Subsystem

Figure 4-6 shows the STO_2 subsystem.

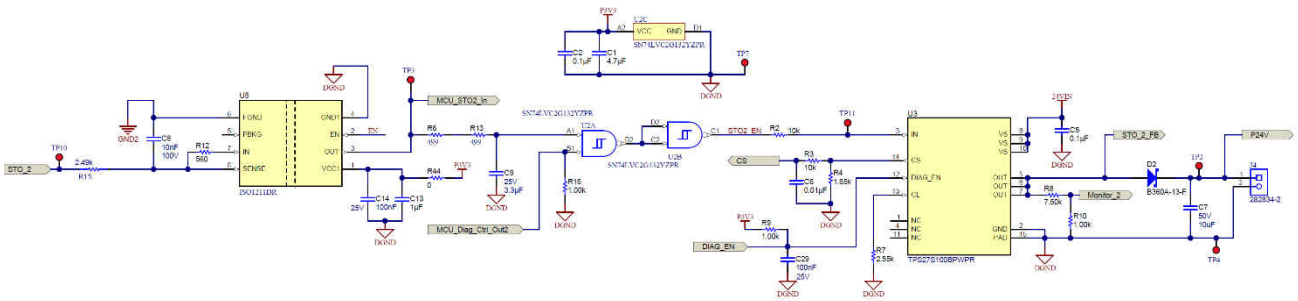

Figure 4-6. STO_2 subsystem (1oo1d)

The 24-V isolated digital input receiver ISO1211 converts the STO_2 input signal to a 3V3 CMOS level signal. The STO_1 signal from the output of the ISO1211 then pass through low pass RC filter to remove 1ms diagnostics pulses present on STO_2 signal. The output of ISO1211 (MCU_STO_2_In) is also monitored by the MCU (SIL 1) for stuck high faults. The low-pass filtered STO_2 signal is ANDed with MCU diagnostic signal (MCU_Diag_Cntrl_Out2) to generate load switch STO2_EN signal. The STO_2_EN signal is used to enable (logic high) and disable (logic low) the high-side load switch, which in turn control the input voltage P24V of the isolated gate supply TIDA-00199. The output of the TIDA-00199 provides 4 bipolar rails (+15 V, 8 V) to supply the six IGBT gate drivers ISO5852S (or ISO5452) VCC2 and VEE2. When the P24V input to TIDA-00199 is disconnected, the VCC2 and VEE2 supplies to the six gate drivers decay to 0V. All 6 isolated gate drivers ISO5852S (or ISO5452) will be disabled, which set the output of the ISO5852S (or ISO5452) gate driver to 0V or high-impedance. With the external pull-down resistors, the six IGBTs will turn off. The STO_2_FB signal used by the STO_FB logic to monitor the state of the drive.

4.4.5 MCU (SIL 1) Diagnostic Coverage

In the TIDA-01599 STO concept an MCU (SIL 1) is assumed to do the diagnostics coverage. The MCU is not part of the analysis. A hardware based diagnostic coverage is possible too.

MCU diagnostic coverage tasks:

- **Task 1**: Periodically monitors STO_1 and STO_2 inputs for OSSD test pulses with 1ms logic low signal present on STO_1_In1 and STO_2_In2 from the corresponding ISO1211 outputs. If no logic low is detected for more than 4ms, the MCU concludes the corresponding ISO1211 output is stuck high or shorted to VCC and puts the 3-phase IGBT inverter into a safe state by driving both diagnostic pulses MCU_Diag_Cntrl_Out1 and MCU_Diag_Cntrl_Out2 continuously low. This in turns will disable the six gate drivers, the six IGBT will be turned off and the drive will enter the safe state.
- **Task 2**: MCU periodically generates short low pulses on the MCU_Diag_Cntrl_Out1 and MCU_Diag_Cntrl_Out2 signals disables the output of the AND gates, which in turn turns off the corresponding load switches. The MCU reads back the output of the load switches through the signals MCU_Diag_Monitor_In1 and MCU_Diag_Monitor_In2. If a short or stuck high was found, the MCU puts the 3-phase IGBT inverter into a safe state by driving both diagnostic pulses MCU_Diag_Cntrl_Out1 and MCU_Diag_Cntrl_Out2 continuously low. This in turns will disable the six gate drivers, the six IGBT will be turned off and the drive will enter the safe state.
- **Task 3**: MCU periodically monitors STO_1 and STO_2 signals from the corresponding ISO1211 output. If either STO_1 or STO_2 or both are active low, the MCU also continuously drives MCU_Diag_Cntrl_Out1 and MCU_Diag_Cntrl_Out2 signal low.

Table 4-3 shows the logic table. Note that STO related signals are active low.

Table 4-3. MCU Diagnostics Logic Table

STO_1 | STO_2	MCU_STO_1_in | MCU_STO_2_in	MCU Diagnostics: Fault Detected	MCU_Diag_Cntrl_Out1 | MCU_Diag_Cntrl_Out2	IGBT Gate Driver Output	State
1 | 1	1 | 1	no	normal operation	normal operation	normal operation
1 | 1	1 | 1	Yes (for example, load switch stuck on)	0	0	Safe state
1 | 1	1 | 1	Yes (for example, no OSSD pulse)	0	0	Safe state
0 | 0	0 | 1	Yes (for example, ISO1211 stuck high)	0	0	Safe state
0 | 0	1 | 0	Yes (for example, ISO1211 stuck high)	0	0	Safe state
0 | 0	0 | 0	no	0	0	STO

4.4.6 STO_FB Subsystem

The STO_FB signal is an active low signal and indicates the drive state. A high signal (logic level 1) indicates normal drive operation, while a low signal (logic state 0) indicates the drive is in the safe state. The schematic is shown in Figure 4-7. The output signals STO_1_FB and STO_2_FB of the corresponding STO_1 and STO_2 safe subsystems are logically combined to a single active low feedback signal STO_FB through an isolated 24-V digital output. The corresponding logic states are shown in Table 4-4.

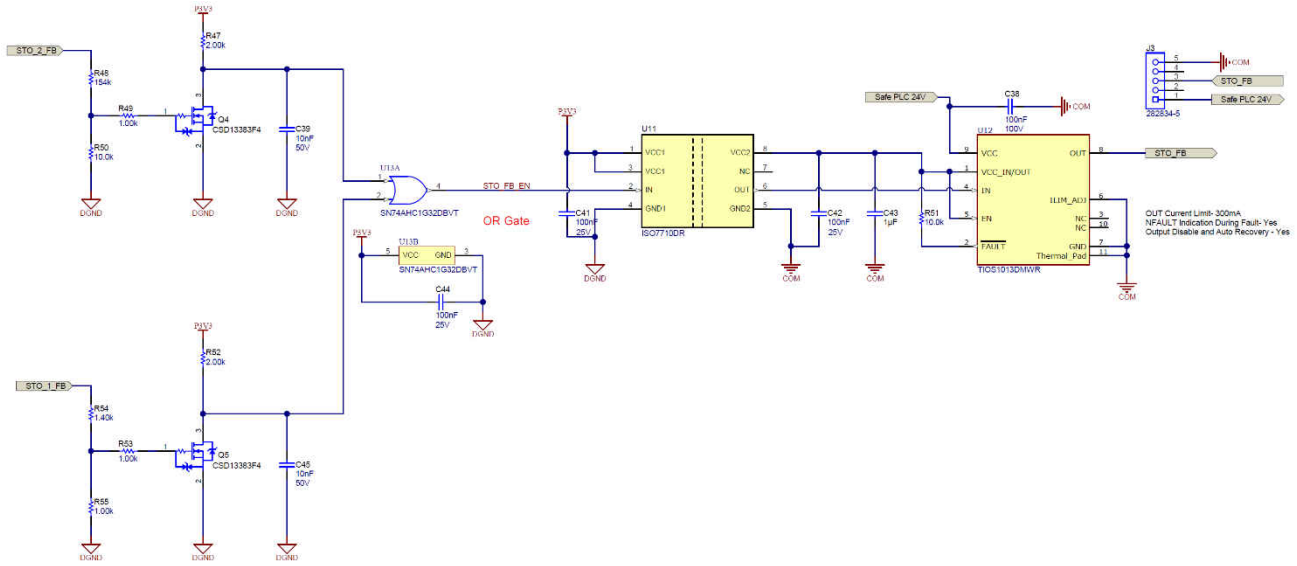

Figure 4-7. STO_FB Feedback Monitor Subsystem

Table 4-4. STO_FB Diagnostics Logic Table

Input 1: STO_1	Input 2: STO_2	Output_1: STO_1_FB (Monitor_1)	Output_2: STO_2_FB (Monitor_2)	Drive State	STO_FB	Comment
1	1	1	1	Normal operation	1	
0	0	0	0	Safe state (off)	0	
1	1	0	1 (stuck high fault)	Safe state (off)	0	(1) The MCU has detected a single dangerous fault (stuck high) in subsystem STO_2 and has triggered the safe state through STO_1 subsystem.
1	1	1 (stuck high fault)	0	Safe state (off)	0	(2) The MCU has detected a single dangerous fault (stuck high) in subsystem STO_1 and has triggered the safe state through STO_2 subsystem.
0	0	0	1 (stuck high fault)	Safe state (off)	0	Single detected fault could be detected earlier already, see (1) in above row.
0	0	1 (stuck high fault)	0	Safe state (off)	0	Single detected fault could be detected earlier already, see (2) in above row.
0	0	1 (stuck high fault)	1 (stuck high fault)	Normal operation	1	Dangerous state, due to two dangerous faults, one in each safe subsystem STO_1 and STO_2.

The STO_FB signal can be active low (logic state 0), while both STO_1 and STO_2 are inactive high (logic state 1). This state occurs when the diagnostics MCU (SIL 1) detects a single dangerous fault in one of the STO_1 or STO_2 subsystems. If a short or stuck high was found, the MCU puts the 3-phase IGBT inverter into a safe state by driving both diagnostic pulses MCU_Diag_Cntrl_Out1 and MCU_Diag_Cntrl_Out2 continuously low. This state can be used for example by an external safety PLC to recognize a single fault in either STO_1 or STO_2 systems and take appropriate actions. The safety PLC and related action are out of scope for this concept analysis.

4.4.7 Information on ICs

4.4.7.1 Isolated 24-V Input Receiver

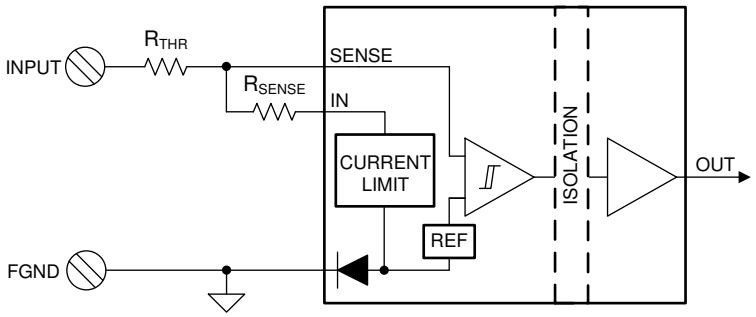

Figure 4-8. ISO1211 Functional Diagram

4.4.7.2 Load Switch: TPS22919

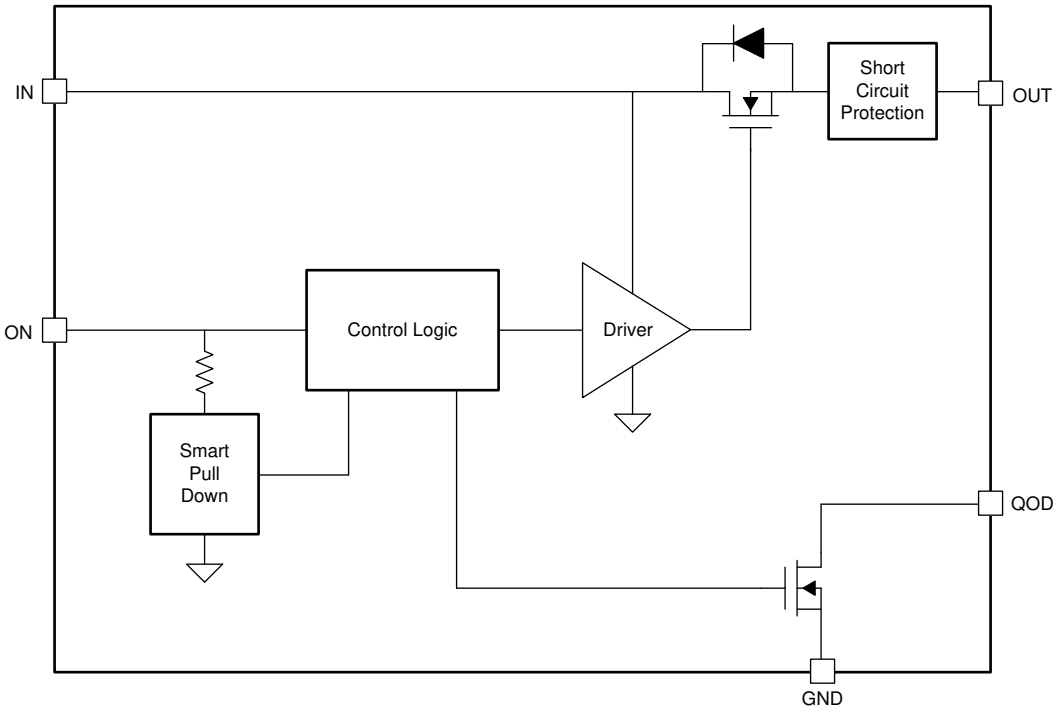

Figure 4-9. TPS22919 Block Diagram

Table 4-5 describes the connection of the VOUT pin depending on the state of the ON pin as well as the various QOD pin configurations.

Table 4-5. TPS22919 Functional Modes vs QOD

On	QOD Configuration	TPS22919 V_{OUT}
L	QOD pin connected to V_{OUT} with R_{QOD}	GND ($R_{PD,\ QOD}$ + R_{QOD})
L	QOD pin tied to V_{OUT} directly	GND ($R_{PD,\ QOD}$)
L	QOD pin left open	Floating
H	N/A	V_{IN}

4.4.7.3 High-Side Switch: TPS27S100

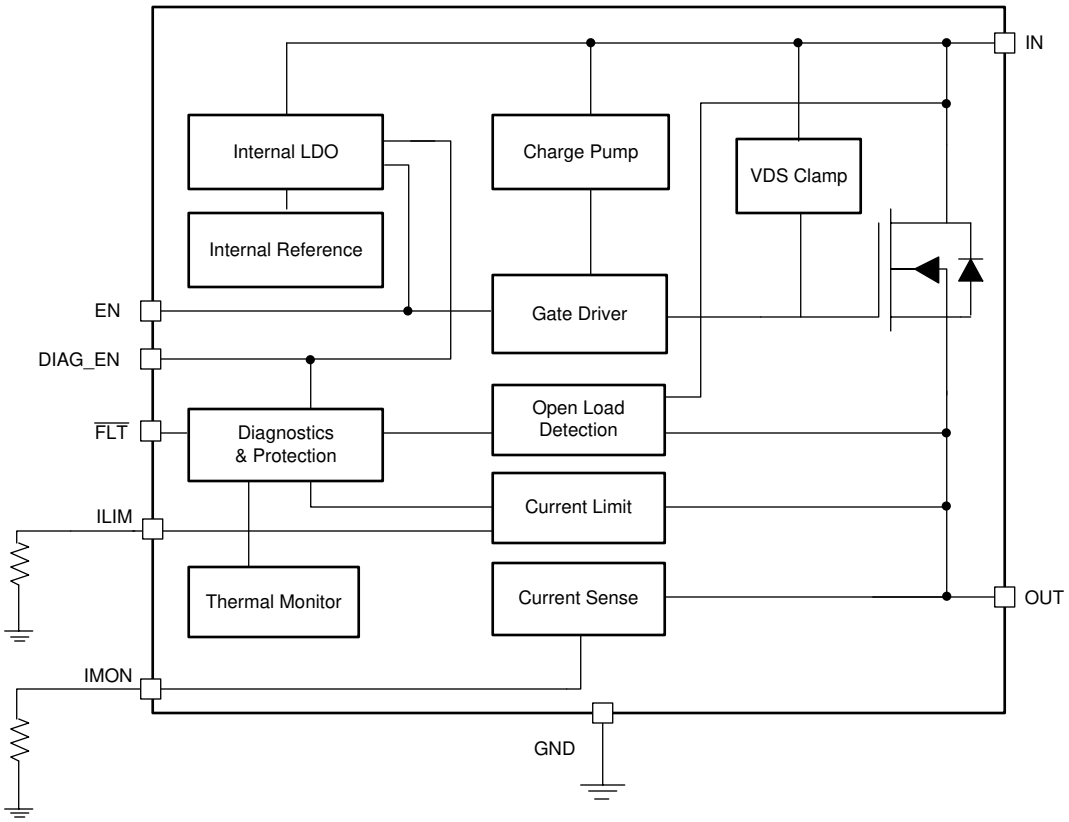

Figure 4-10. TPS27S100 Functional Diagram

4.4.7.4 Isolated Gate Driver: ISO5852S (ISO5452)

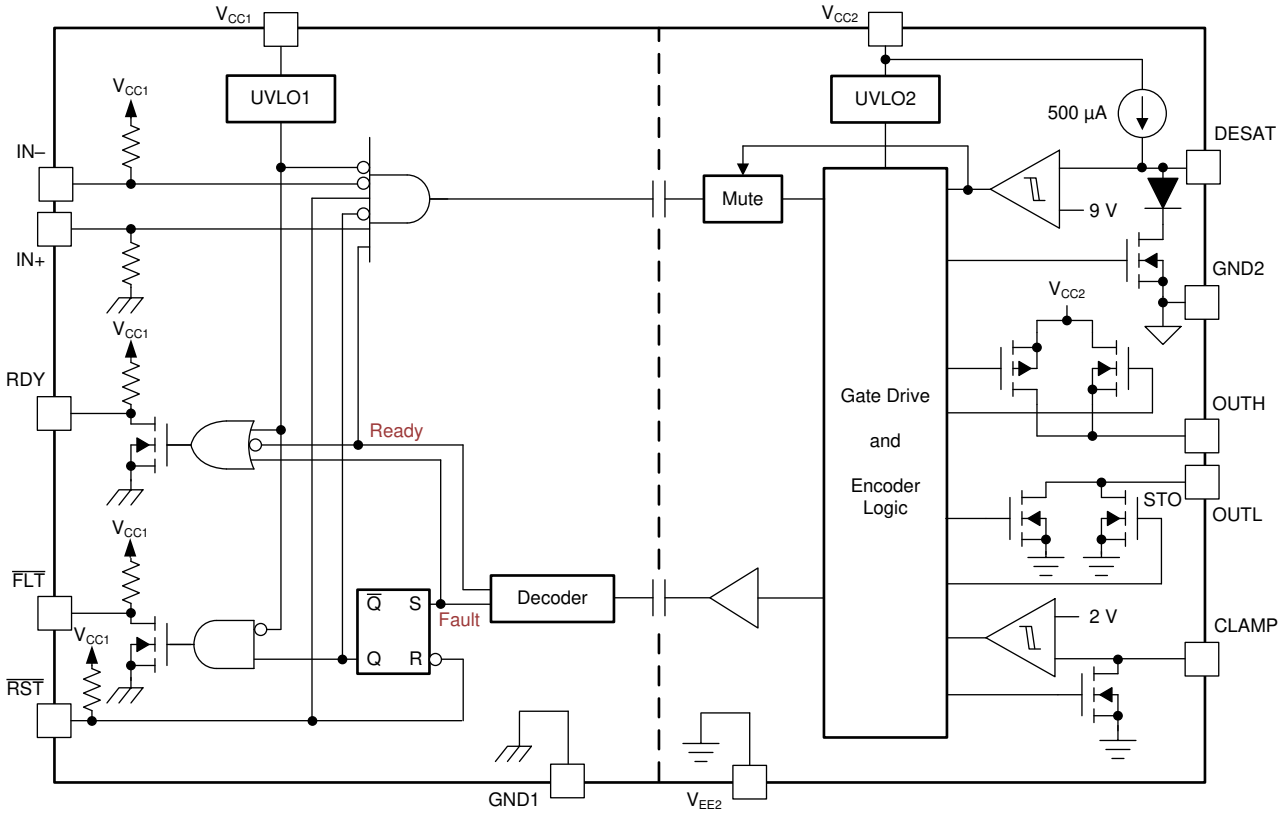

Figure 4-11. ISO5852S (ISO5452) Block Diagram

Table 4-6 shows the ISO5852S (ISO5452) isolated gate driver output voltage depending on the logic supply voltage VCC1 and the isolated supply voltage VCC2. If any of these supply voltages is off (see threshold values under footnote 1), the output OUTH/L of the gate driver is low. Table 4-6 is copied from the ISO5852S (ISO5452) data sheet, reference number SLLSEQ0 and SLLSEQ4.

Table 4-6. ISO5852S (ISO5452) Functional Table VCC1 and VCC2/VEE2 vs Output Voltage

Function Table(1)

V_{CC1}	V_{CC2}	IN+	IN–	$\overline{RST}$	RDY	OUTH/L
PU	PD	X	X	X	Low	Low
PD	PU	X	X	X	Low	Low
PU	PU	X	X	Low	High	Low
PU	Open	X	X	X	Low	Low
PU	PU	Low	X	X	High	Low
PU	PU	X	High	X	High	Low
PU	PU	High	Low	High	High	High

(1) PU: Power Up (V_{CC1} ≥ 2.25-V, V_{CC2} ≥ 13-V), PD: Power Down (V_{CC1} ≤ 1.7-V, V_{CC2} ≤ 9.5-V), X: Irrelevant

4.5 Safe State

The safe-state is triggered by the following events:

1. Active low STO_1 input signal requesting safe torque off
2. Active low STO_2 input signal requesting safe torque off
3. Diagnostic coverage of STO_1 or STO_2 subsystems (ISO1211 and corresponding load switches) detects a dangerous fault
4. Safe power supply voltages P24V, P3V3 or the corresponding logic supply voltages of the STO_1 and STO_2 subsystem are cut-off

5 Concept FMEA

The concept FMEA was based on IEC 61800-5-2: 2016 paragraph D.3 Fault Models shown in the following list. The concept GMEA also considers 61508-2 table A1, discrete hardware DC fault models for drift and oscillation.

- **D.3.8 Resistors**: The requirements of ISO 13849-2:2012, **Table D.14 apply**.
- **D.3.11 Capacitors**: The requirements of ISO 13849-2:2012, **Table D.17 apply**.
- **D.3.12 Discrete semiconductors**: For example diodes, Zener diodes, transistors, triacs, GTO thyristors, IGBTs, voltage regulators, quartz crystal, phototransistors, light-emitting diodes [LEDs]. The requirements of ISO 13849-2:2012, **Table D.18 apply**.
- **D.3.13 Signal Isolation components**: The requirements of IEC 61800-5-2 **Table D.5 apply**.
- **D.3.14 Non-programmable integrated circuits (IC)**: The requirements of IEC 61800-5-2: 2016 **Table D.6 applies**. In this standard, ICs with less than 1 000 gates, less than 24 pins, or both, operational amplifiers, shift registers and hybrid modules are considered to be non-complex. This definition is arbitrary.
- **D.3.15 Programmable ICs, complex ICs, or ICs that are both programmable and complex**: The requirements of **Table D.7 apply**. In this standard, an IC is considered to be complex if it consists of more than 1 000 gates, more than 24 pins, or both 1 000 gates and more than 24 pins. This definition is arbitrary. The analysis should identify additional faults which should be considered if they influence the operation of the safety sub-function.

This FMEA considers comparators, logic gates, and load switches (less than 24-pins) type A per IEC 61800-5-2 D3.14, ISO1211 and ISO5852S (or ISO5452) are part of D3.13 and D.3.14.

5.1 System FMEA

For access to *FMEA STO Concept TIDA-01599*, use this secure link.

6 References

See Section 2 for a list of related documentation.

The following materials are offered for additional reference:

1. Texas Instruments, *TIOS1013 and TIOS1015 Functional Safety FIT Rate, FMD and Pin FMA* Application Note
2. Texas Instruments, *ISO7710/ISO7710-Q1 Functional Safety FIT Rate, FMD and Pin FMA* Application Note
3. Texas Instruments, *ISO5x Functional Safety FIT Rate, FMD and Pin FMA* Application Note, *not currently released*
4. Texas Instruments, *TPS22919-Q1 Functional Safety, FIT Rate, Failure Mode Distribution and Pin FMA* Functional Safety Information, *not currently released*

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