

デザイン・ガイド: TIDA-010049

IEC 61508 (SIL-2) 用、TUV 評価済みのデジタル入力のリファレンス・デザイン



概要

この 8 チャンネル、グループ絶縁型デジタル入力モジュールのリファレンス・デザインは、産業用機能安全を必要とするアプリケーションに特化したものです。このリファレンス・デザインには診断機能が実装されており、恒久的なハードウェア障害と過渡的でランダムなハードウェア障害の両方を検出するのに役立ちます。この入力モジュールのコンセプトは、TUEV SÜED (TÜV ⁽¹⁾SÜD) 社により評価済みであり、IEC61508-2:2010 (SIL2) と EN13849-1:2015 (Cat2 PLd) の要件を満たしています。また、このリファレンス・デザインは、ハードウェア・フォルト・トレランス (HFT) = 0 (1oo1D アーキテクチャ) を実現し、IEC61131-2 (type 1) 勧告に準拠して設計されたデジタル入力を搭載しています。

リソース

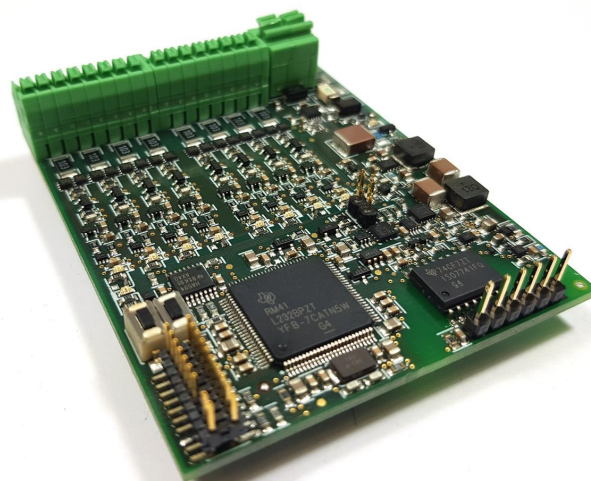
TIDA-010049		デザイン・フォルダ
RM41L232		プロダクト・フォルダ
LMR36006	TPS3852	プロダクト・フォルダ
TPS62230	LM5166	プロダクト・フォルダ
TPS22917	TPS2662	プロダクト・フォルダ
REF3030	ISO7741	プロダクト・フォルダ
TLV9001	TPS3700	プロダクト・フォルダ
TL431LI	TVS0500	プロダクト・フォルダ
SN74LVC1G11	TMP302	プロダクト・フォルダ
SN74LVC2G132	SN74LVC1G125	プロダクト・フォルダ
CSD18541F5	SN74AHC594	プロダクト・フォルダ

特長

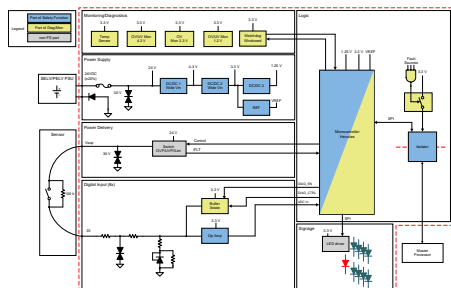
- IEC61131-2 (type 1) に準拠したグループ絶縁型 8 チャンネル・デジタル入力
- IEC61508-2:2010 (SIL2) と EN13849-1:2015 (Cat2 PLd) の要件を満たすコンセプト (TÜV SÜD により評価済み)
- 診断および監視機能
- 誤配線保護 (逆極性、デジタル入力の短絡、開放、クロス配線)
- 小フットプリント

アプリケーション

- 機能安全を備えたデジタル入力モジュール
- 産業用ロボットの I/O モジュール
- サーボ・ドライブ制御モジュール
- 列車制御/管理システム



E2E™ エキスパートに質問



(1) Technischer Überwachungsverein



使用許可、知的財産、その他免責事項は、最終ページにあるIMPORTANT NOTICE (重要な注意事項)をご参照くださいますようお願いいたします。

1 System Description

The digital input module is a widely used I/O module in the programmable logic controllers (PLC) space. The use-cases are very flexible. A sensor connected to an input can vary from a switch monitoring a door to a digital encoder for motors.

Digital inputs can be current-sinking or current-sourcing. This design supports the current-sinking type of digital input. This means that the sensor is connected between the field supply rail (typically 24 V) and the digital input. The current flows through the digital input to the ground.

Standard input modules may fail without being recognized by the system, for example, an input channel may indicate that the sensor switch is closed (logical 1) high while the sensor switch is essentially open (logical 0). Where this might be acceptable in a standard application, a functional safety application cannot tolerate this behavior. This design focuses on the functional safety aspect to detect random faults and to act accordingly.

An input channel count of 8 was chosen to comply with commonly used channel counts, such as 4, 8, 16, and 32 with respect to the number of available MCU analog inputs and digital input and output pins. No additional logic, such as general purpose input and output (GPIO) expanders, is required to drive the diagnostic signals. This avoids additional fault sources and does not unnecessarily complicate the design.

1.1 Key System Specifications

表 1. Key System Specifications

PARAMETER	SPECIFICATIONS	DETAILS
Input power source	24 V ($\pm 20\%$)	2.4.3.1
Average active-state current consumption at $V_{in} = 24$ V (no power delivery load)	23.5 mA	3.2.2.1
Average power consumption at $V_{in} = 24$ V (no power delivery load)	0.57 W	3.2.2.1
Number of input channel	8	1
Reverse polarity protection	yes	2.4.3.1
Overvoltage protection	yes	2.4.3.1
Output voltage (power delivery)	24 V ($\pm 20\%$)	2.4.3.2
Maximum output current (total of all sensor supplies)	800 mA	2.4.3.2
Power delivery short-circuit protection	yes	2.4.3.2
Sinking-current input	yes	2.4.3.3
Input according to IEC61131-2	yes; type 1	2.4.3.3
Type of input voltage	DC	2.4.3.3
Signal range	-30 V to +30 V	2.4.3.3
0-state voltage range	-30 V to +10 V	2.4.3.3
1-state voltage range	+15 V to +30 V	2.4.3.3
Input current for 1-state (24-V DC)	3.5 mA	2.4.3.3
Global ALARM indicator	yes; red LED	2.4.3.6
Channel state indicator	yes; green LED per channel	2.4.3.6
Input power indicator	yes, green LED	2.4.3.6
ADC conversion (all channels, including diagnostics)	15 μ s (no external cap) / 550 μ s (external cap)	2.4.3.3
Potential separation between input channels	no	2.4

表 1. Key System Specifications (continued)

PARAMETER	SPECIFICATIONS	DETAILS
Potential separation between input channels and back-end	yes	2.4
Potential separation between input channels and power supply	no	2.4
Operating temperature	-40°C to +105°C	3.2.2.1
Dimension L x B x H	75 x 60 x 15 mm (2.95" x 2.36" x 0.59")	4.3

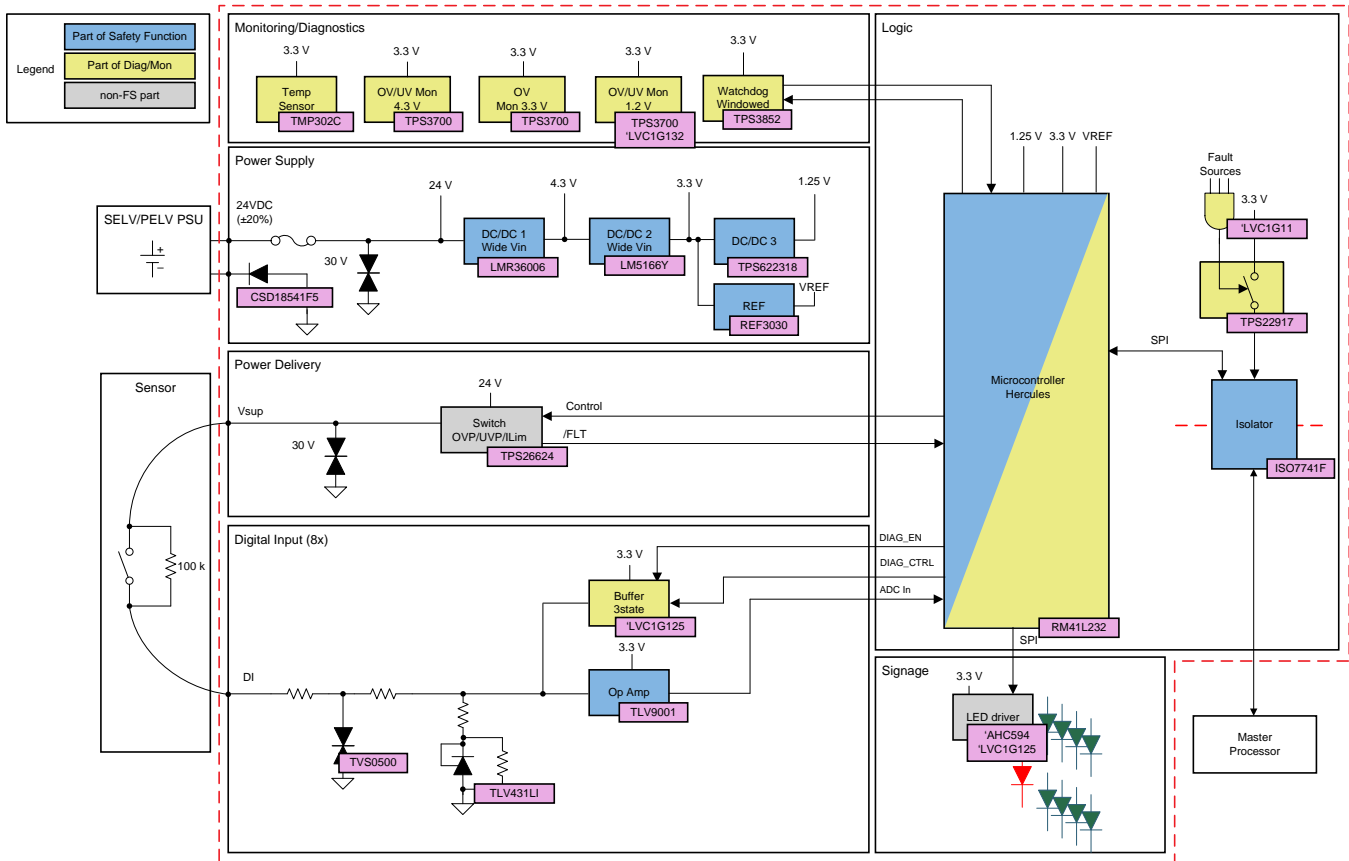
1.2 Definitions and Abbreviations

ABBREVIATION	DEFINITION
0-state	logical '0' read by a digital input channel
1-state	logical '0' read by a digital input channel
SELV	Safety Extra Low Voltage
PELV	Protective Extra Low Voltage
module, design, board, circuit	TIDA-010049 hardware as shown in the first-page images
UV	undervoltage
OV	overvoltage
RPP	Reverse Polarity Protection
ADC	Analog-to-Digital Converter
SIL	Safety Integrity Level
HFT	Hardware Fault Tolerance
DTI	Diagnostics Test Interval
WWDT	Window Watchdog Timer
MCU	Microcontroller Unit
POR	Power-on reset
Monitoring	permanent observation of a system variable, such as a supply rail or temperature
Diagnostics	Injection of an (error) signal to an element to verify its correct function and to test its behavior during a fault
IDE	Integrated Development Environment

2 System Overview

2.1 Block Diagram

図 1. TIDA-010049 Block Diagram



2.2 Design Considerations

Functional safety is important in the industrial space. This digital input module design addresses this need by adding the functional safety aspect with diagnostics and a monitoring function. These features help to detect permanent and transient random faults to avoid harm to humans, the environment, and assets.

The concept of this design has been assessed by TÜV SÜD. The concept meets requirements according to IEC61508-2:2010 (SIL2) and EN13849-1:2015 (Cat2 PLd).

注: This design itself is an interpretation of the systems engineer. This design was not reviewed by TÜV SÜD and, therefore, does not claim to be in accordance of IEC61508 or EN13849.

The goal of the concept is to develop an SIL2 digital input with a hardware fault tolerance (HFT) equal to zero. The Hercules™ processor used here is certified up to SIL3 and has a HFT of zero, helping to reach this goal. An external window watchdog is required. The power tree is implemented with three buck converters. All voltage rails are monitored against undervoltage (UV) and overvoltage (OV).

There are multiple ways to implement the digital input front end. This design uses a discrete approach, which offers the most flexibility. The diagnostics portion is integrated seamlessly. Furthermore, a discrete design with simple components can lower the effort of the failure analysis.

The power for the external sensors is provided from the digital input module. This current-limited power supply can be turned off to run certain wiring faults detection algorithms. The power can be supplied from an auxiliary source but with the penalty of limited wiring fault detection.

This design distinguishes between faults, which may lead to a fault of the Hercules MCU and faults, which are not influencing the Hercules MCU. If the Hercules MCU might be impacted, an independent safestate logic is triggered. The safestate function is reached by putting the communication to a condition, which is forbidden in normal operation. A feature of the digital data isolator helps to achieve this goal.

2.3 Highlighted Products

2.3.1 RM41L232

The RM41L232 device is a high-performance microcontroller for safety systems. The safety architecture includes dual CPUs in lockstep, CPU and Memory BIST logic, ECC on both the flash and the data SRAM, parity on peripheral memories, and loopback capability on peripheral I/Os.

The RM41L232 device integrates the Arm® Cortex®-R4 CPU. The CPU offers an efficient 1.66 DMIPS/MHz, and has configurations that can run up to 80 MHz, providing up to 132 DMIPS.

2.3.2 TPS3852H33

The TPS3852 is a precision voltage supervisor with an integrated window watchdog timer. The TPS3852 includes a precision undervoltage supervisor with an undervoltage threshold (VITN) that achieves 0.8% accuracy over the specified temperature range of -40°C to $+125^{\circ}\text{C}$. In addition, the TPS3852 includes accurate hysteresis making the device ideal for use with tight tolerance systems. The supervisor RESET delay features a 15% accuracy, high-precision delay timer.

The TPS3852 includes a programmable window watchdog timer for a wide variety of applications. The dedicated watchdog output (WDO) enables increased resolution to help determine the nature of fault conditions.

2.3.3 LMR36006

The LMR36006 regulator is an easy-to-use, synchronous, step-down DC/DC converter. With integrated high-side and low-side power MOSFETs, up to 0.6 A of output current is delivered over a wide input voltage range of 4.2 V to 60 V. Tolerance goes up to 66 V. The transient tolerance reduces the necessary design effort to protect against overvoltages and meets the surge immunity requirements of IEC 61000-4-5.

The LMR36006 uses peak-current-mode control to provide optimal efficiency and output voltage accuracy.

2.3.4 LM5166Y

The LM5166 is a compact, easy-to-use, 3-V to 65-V, ultra-low IQ synchronous buck converter with high efficiency over wide input voltage and load current ranges. With integrated high-side and low-side power MOSFETs, up to 500 mA of output current can be delivered at fixed output voltages of 3.3 V. The converter is designed to simplify implementation while providing options to optimize the performance for the target application. Pulse frequency modulation (PFM) mode is selected for optimal light-load efficiency or constant on-time (COT) control for nearly constant operating frequency.

The high-side P-channel MOSFET can operate at 100% duty cycle for lowest dropout voltage. The current limit setpoint is adjustable to optimize inductor selection for a particular load current requirement.

2.3.5 TPS622318

The TPS622318 is a high-frequency, synchronous, step-down DC/DC converter optimized for battery-powered portable applications. It supports up to 500-mA output current at an output voltage of 1.25 V and allows the use of tiny and low-cost chip inductors and capacitors.

The TPS622318 features a switching frequency of 3 MHz. At medium to heavy loads, the converter operates in pulse width modulation (PWM) mode and automatically enters power-save mode operation at light-load currents to maintain high efficiency over the entire load current range.

2.3.6 TPS26624

The TPS26624 is a compact, feature-rich, high-voltage eFuse with a full suite of protection features. The wide supply input range of 4.5 V to 57 V allows control of many popular DC bus voltages. The device can withstand and protect the loads from positive and negative supply voltages up to ± 60 V. The TPS26624 supports both input as well as output reverse polarity protection feature. Integrated back-to-back FETs provide a reverse current-blocking feature, making the device suitable for systems with output voltage holdup requirements during power fail and brownout conditions. Load, source, and device protection are provided with many adjustable features including overcurrent, output slew rate and overvoltage, and undervoltage thresholds.

The TPS26624 features latch-off functionality over-temperature and over-current fault events.

2.3.7 TPS22917

The TPS22917 device is a small, single-channel load switch using a low leakage P-Channel MOSFET for minimum power loss. Advanced gate control design supports operating voltages as low as 1 V with minimal increase in ON-Resistance and power loss.

The switch ON state is controlled by a digital input that can interface directly with low-voltage control signals.

2.3.8 ISO7741F

The ISO7741F is a high-performance, quad-channel digital isolators with 5000 V_{RMS} (DW package) and 3000 V_{RMS} (DBQ package) isolation ratings per UL 1577. This family of devices has reinforced insulation ratings according to VDE, CSA, TUV and CQC.

The ISO7741 device has three forward and one reverse-direction channels. If the input power or signal is lost, default output is low for devices with suffix F.

2.3.9 REF3030

The REF3030 is a 3.0-V precision, low-power, low-dropout voltage reference offering excellent temperature drift and initial accuracy.

2.3.10 TPS3700

The TPS3700 wide-supply voltage window supervisor operates over a 1.8-V to 18-V range. The device has two high-accuracy comparators with an internal 400-mV reference and two open-drain outputs rated to 18 V for over- and undervoltage detection.

2.3.11 TLV9001

The TLV9001 is a single low-voltage (1.8 V to 5.5 V) operational amplifier (op amp) with rail-to-rail input and output swing capabilities. These op amps provide a cost-effective solution for space-constrained applications.

2.3.12 TVS0500

The TVS0500 robustly shunts up to 43 A of IEC 61000-4-5 fault current to protect systems from high-power transients or lightning strikes. The device offers a solution to the common industrial signal line EMC requirement to survive up to 2 kV IEC 61000-4-5 open circuit voltage coupled through a 42- Ω impedance. The TVS0500 uses a unique feedback mechanism to ensure precise flat clamping during a fault.

2.3.13 TL431LI

The TL431LI device is a three-terminal adjustable shunt regulator, with specified thermal stability. The output voltage can be set to any value between V_{ref} (approximately 2.495 V) and 36 V. These devices have a typical output impedance of 0.3 Ω .

The TL431LI device is offered in two grades with initial tolerances (at 25°C) of 0.5% and 1%, for the B and A grade, respectively. In addition, low-output drift versus temperature ensures good stability over the entire temperature range.

2.3.14 TMP302C

The TMP302 device is a temperature switch in a micropackage (SOT563). The TMP302 offers low power (15- μ A maximum) and ease-of-use through pin-selectable trip points and hysteresis.

2.3.15 SN74LVC1G11

The SN74LVC1G11 is a single 3-input positive-AND gate supporting 5-V V_{cc} operation.

2.3.16 SN74LVC1G125

The SN74LVC1G11 is a single bus buffer gate with 3-state output supporting 5-V V_{cc} operation.

2.3.17 SN74LVC2G132

The SN74LVC1G11 is a dual 2-input NAND gate with schmitt-trigger inputs supporting 5-V V_{cc} operation.

2.3.18 SN74AHC594

The SNx4AHC594 devices contain an 8-bit serial-in, parallel-out shift register that feeds an 8-bit D-type storage register.

2.3.19 CSD18541F5

This 54-m Ω , 60-V, N-Channel FemtoFET™ MOSFET technology is designed and optimized to minimize the footprint in many space-constrained industrial load switch applications.

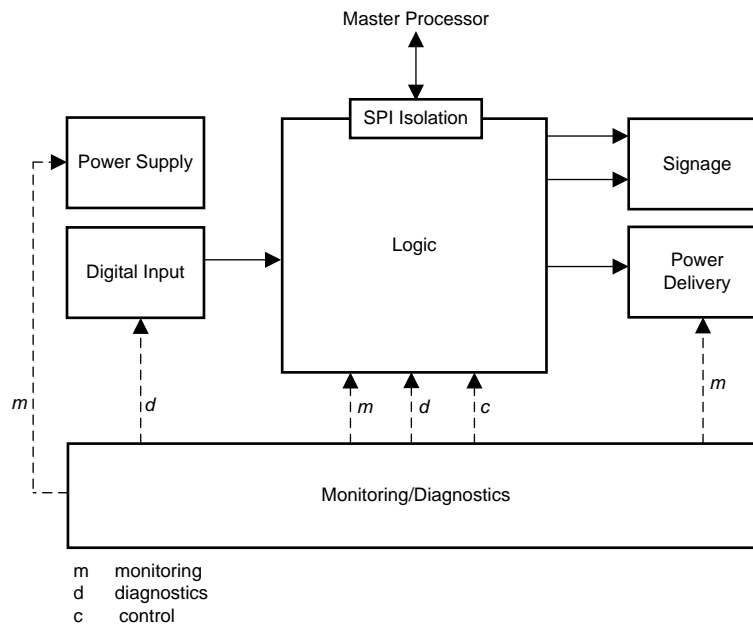
2.4 System Design Theory

The system is designed in a group-isolated manner, as in, all digital input channels share the same ground. The isolation to the back end is performed at the SPI to the master processor, as in, the entire circuit is implemented at the field side.

2.4.1 Concept

Figure 2 shows the concept of this design. This concept is assessed by TÜV SÜD for a digital input module meeting requirements for IEC61508-2:2010 (SIL2) and EN13849-1:2015 (Cat2 PLd).

Figure 2. TIDA-010049 Concept



2.4.2 Safety Function

The safety function of this design is the reliable conversion of the eight IEC61131-2 compatible digital inputs represented by defined current and voltage levels to its digital representation including the error-free forwarding of this information to the master processor. The maximum delay between any input state change to the corresponding output bit must not exceed a diagnostics test interval (DTI) of less than 1 second.

Parts of the safety function are:

1. *Power Supply* element
2. *Digital Input* element
3. *Logic* element

The *Monitoring/Diagnostics* element is a supporting function for the elements part of the safety function and monitors/tests power supply outputs, the digital input channels and external circuit like the watchdog.

The *Power Delivery* and *Signage* elements are considered non-safe. Interference-freeness to the safety-related parts is taken into account.

2.4.3 Element Description

The following sections describe the elements. For a better understanding, the individual signals are shown in 表 2. A signal starting with / is low active.

表 2. Signal Description

SIGNAL NAME	SIGNAL TYPE	DESCRIPTION
/COLD_RST	Control	Cold reset of Hercules MCU
/WARM_RST	Control	Warm reset of Hercules MCU
MASK_COLD_RST	Diagnostics	Prevents Hercules MCU cold reset during diagnostics
MASK_WARM_RST	Diagnostics	Prevents Hercules MCU warm reset during diagnostics
/DIAG_ENx	Diagnostics	Enables diagnostics for digital input channel x
DIAG_CTRLx	Control/diagnostics	Controls logical level of digital input diagnostics
/ERROR	Flag	Hercules MCU error signal
/SAFE_STATE	Feedback	Read-back of safestate
/TST_RST	Diagnostics	Triggers WDT diagnostics
SENSSUP_CTRL	Control	Power delivery on/off control
/FLT_1.25V_UV	Flag	V_{core} (1.25 V) UV detected
/FLT_1.25V_OV	Flag	V_{core} (1.25 V) OV detected
/FLT_3.3V_OV	Flag	V_{io} (3.3 V) OV detected
/FLT_4.3V	Flag	V_{int} (4.3 V) UV/OV detected
/FLT_SESSUP	Flag	Power delivery fault detected
/FLT_TEMP	Flag	Board high temperature detected

2.4.3.1 Power Supply

The *Power Supply* element generates all voltage rails required to power the design. This design is powered from a safety extra low voltage (SELV) or protective extra low voltage (PELV) power supply. The nominal input voltage is $V_{in} = 24$ V with an accepted variation of $\pm 20\%$ (from 19.2 V to 28.8 V). If V_{in} is greater than 33 V, or the current drawn exceeds 1.5 A, the design is permanently de-energized by triggering a burnable fuse (F1). Wrong polarity protection is realized by MOSFET Q1 in the ground path. The resistor divider R35, R36 generates a gate voltage of 5.3 V at 19.2 V, which is sufficient to fully turn-on Q1.

The first stage accepts an input voltage of up to 60 V (66 V absolute maximum). The buck-converter LMR36006 (U14) generates a constant intermediate voltage $V_{int} = 4.3$ V and does not supply any other circuit than the following DC/DC converter during normal operation.

When V_{int} is settled to the nominal value, the power good signal from the LMR36006 enables the second stage. The buck-converter LM5166Y (U15) generates a constant voltage $V_{io} = 3.3$ V, which powers all active components. The switching frequency of this converter is 600 kHz. The built-in current limiter limits the output current to 300 mA in the event of a load short-circuit. The voltage reference $V_{ref} = 3.0$ V is generated from V_{io} by the voltage reference circuit REF3030 (U9) and a preceding low pass with a corner frequency of less than 40 dB at 600 kHz. Together with the rejection of the REF3030, the voltage ripple is within one half LSB of the Hercules MCU 12-bit converter.

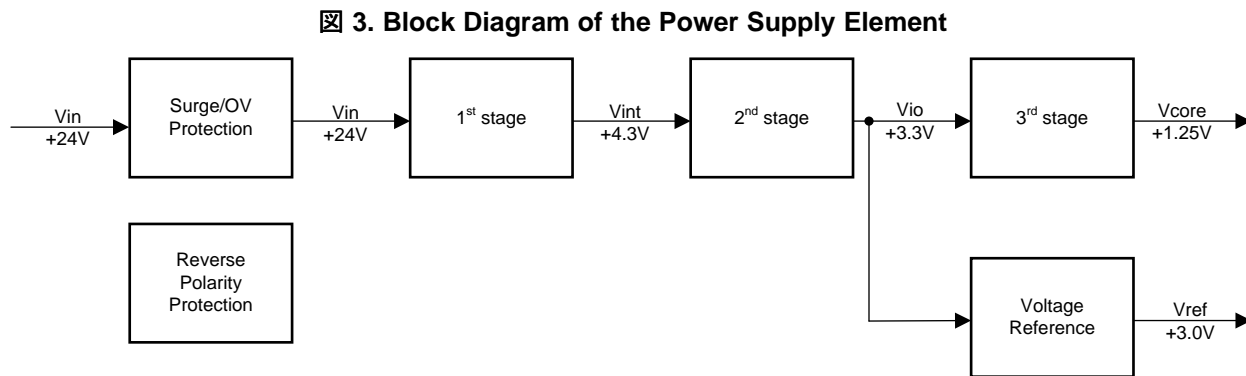
When V_{io} is settled to the nominal value, the power good signal from the LM5166Y enables the third stage. The buck-converter TPS622318 (U16) generates a voltage $V_{core} = 1.25$ V solely for the MCU core.

The power tree is set up in a way that it can tolerate an input-to-output short of the first stage or second stage without affecting operation of the circuit. If the first stage fails, the second stage works with V_{in} . As V_{int} is not connected to any component, the increased voltage will have no effect. If the second stage fails, the design is powered by V_{int} . All components in the system tolerate a maximum voltage of at least 4.6 V at the V_{io} rail, which allows to continue operation and to report the fault.

An UV or OV of any voltage rail is reported. If the Hercules MCU is impacted by voltage violations, the design is put into the safestate, and the Hercules MCU is held in reset until the fault disappears. An OV condition of V_{core} is not intercepted, and the design is put in permanent safe state in this fault event. Only a power cycle can restart the hardware.

If a fault does not impact the Hercules MCU, operation is continued and it is the responsibility of the Hercules MCU application to report this fault to the next instance (master processor).

Figure 3 shows the block diagram of the *Power Supply* element.



2.4.3.2 Power Delivery

The *Power Delivery* element provides power to the external sensors up to 800 mA in total. An external sensor can be a displacement sensor with digital output, a traditional relay, or a solid-state relay. The power to the external sensors can be turned on and off by the Hercules MCU.

The core part of this element is the eFuse TPS26624 (U21). This device is powered from V_{in} and provides V_{sup} to the external sensors if the eFuse is enabled and no fault is detected. V_{sup} is nearly V_{in} as the eFuse connects V_{in} to V_{sup} using an internal MOSFET with low R_{ds_on} .

The eFuse notifies the MCU with signal /FLT_SENSSUP if at least one of the following faults or conditions occur:

- Overcurrent detection
- V_{in} UV/OV
- Reverse current
- Thermal condition
- eFuse turned off

The TPS26624 latches off during overcurrent and thermal fault condition. A power cycle is required to get back to normal operation. TI recommends the TPS26625 if an auto-retry is preferred instead.

The UV threshold is 19 V and the OV threshold is 29 V, which is ± 200 mV outside the limit of V_{in} . This feature is used to monitor V_{in} . As the signal /FLT_SENSSUP is shared with other fault sources, a UV or OV fault may not be clearly identified. A dedicated window comparator may be added to overcome this limitation.

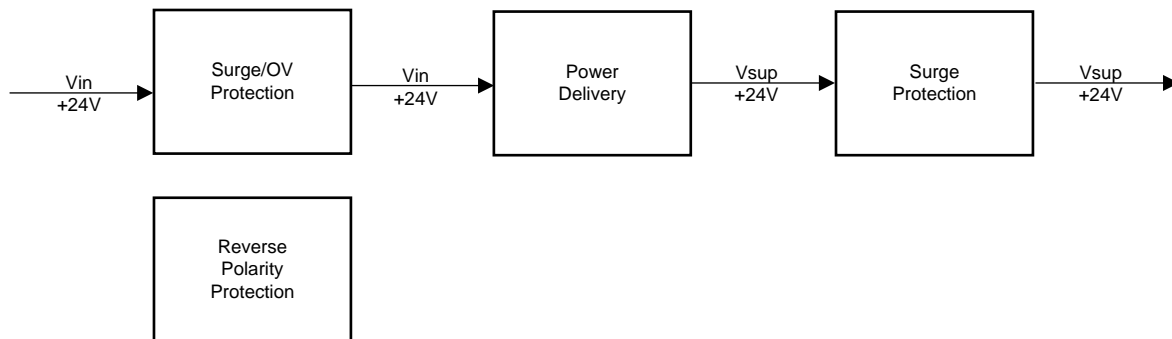
The TPS26624 features a full input and output reverse polarity protection (RPP). This RPP is not required as a discrete RPP is already added at the system level to protect the LMR36006 (U14). The RPP for the TPS26624 can be disabled by connecting pins RTN and GND. This design leaves the RPP feature enabled.

The in-rush feature allows safe hot-plugging of loads and power up with load connected.

The *Power Delivery* element is protected against surges by the TVS diode D7.

Figure 4 shows the block diagram of the *Power Delivery* element.

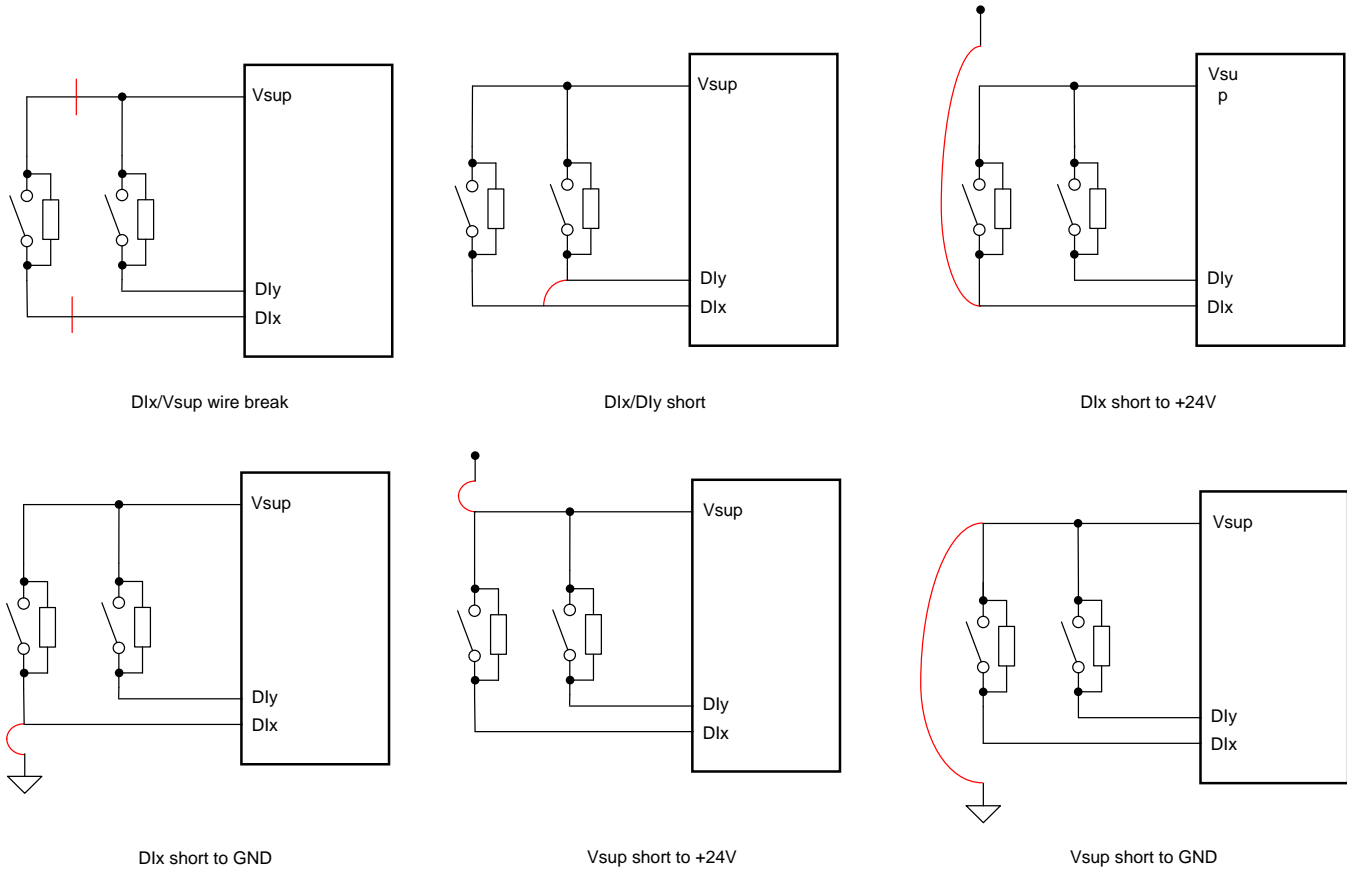
Figure 4. Block Diagram of the Power Delivery Element



Powering the external sensors straight from a 24-V DC field power supply source is possible, but wire diagnostics is limited in this case as the module does not control the power for the external sensors.

Figure 5 shows the detectable miss wiring conditions using the *Power Delivery* supply.

図 5. Detectable Digital Input Wiring Faults



注: A resistor of 100 kΩ bypassing the switching element of the external sensor is required to detect all shown wiring faults including wire-break detection.

2.4.3.3 Digital Input Front-End

The *Digital Input Front-End* element follows the IEC61131-2 standard (type 1) and translates the incoming DC voltage of up to 30 V to a voltage compatible with the input range of the ADC. 表 3 shows the input current for multiple signal input voltages (V_{signal}).

表 3. Digital Input Currents

V_{signal}	0-STATE CURRENT	1-STATE CURRENT
15 V	138 μ A	2.02 mA
24 V	220 μ A	3.5 mA
30 V	276 μ A	4.5 mA

注: The current in the 0-state requires a 100-kΩ resistor bypassing the external sensor.

The input current for the 0-state is dominated by the external bypass resistor of typically 100 kΩ. The input resistance of the digital input of about 8.676 kΩ is added.

When the bypass resistor is shorted (1-state), the input resistance is about 7.4 kΩ at $V_{\text{signal}} = 15$ V and 6.6 kΩ at $V_{\text{signal}} = 30$ V.

Each input stage consists of two TVS0500 (U3 and U4) in parallel. If one TVS0500 fails, opening the other component still protects the input in case of a surge event.

The input signal is attenuated by a resistor divider. The shunt regulator TL431LI (U5) clamps the voltage at 2.5 V over a wide input range. An additional voltage of maximal 300 mV is built up by R5 on top of the shunt regulator voltage. Therefore, the maximal voltage at the op-amp input is 2.8 V. The op amp TLV9001 (U2) acts as a buffer providing a signal with low impedance to the ADC input. The maximal input voltage of 2.8 V is chosen as the leakage input current of the ADC input increases toward the maximum input voltage of $V_{ref} = 3 \text{ V}$.

The need for the RC combination between the op amp and the ADC input is dependent on the application. See the [ADC source impedance for Hercules™ Arm® safety MCUs application report](#) for more information. The capacitor shortens the settling time but adds a significant recovery time of about 68 μs . The 3-dB corner frequency of the input signal for $R4 = 200 \Omega$ and $C1 = 560 \text{ nF}$ is 417 Hz. The ADC round-trip time is about 550 μs . Removing the capacitor C1 increases the round-trip time to about 15 μs .

Diagnostics is accomplished by injecting and drawing current to and from the signal chain. A simple way to do this is to use a tri-state digital buffer. The buffer remains in tri-state during normal operation.

If diagnostics is desired and the channel is in 0-state, the signal DIAG_CTRL is set high and the diagnostics are enabled by asserting signal /DIAG_EN. As a result, the input channel will switch to 1-state.

If the channel is in 1-state, the signal DIAG_CTRL is set low, and the diagnostics are enabled by asserting signal /DIAG_EN. As a result, the input channel will switch to 0-state.

2.4.3.4 Logic

The *Logic* element mainly includes the Hercules MCU, the windowed watchdog and the data isolator. A power switch and several logic gates trigger and provide the safe state in case a fault, which may influence the correct operation of the Hercules MCU, is detected.

2.4.3.4.1 Hercules MCU

The following integrated blocks of the RM41L232 are used:

- Processing: dual lock-step Arm Cortex -R4 CPU
- ADC: sampling of the digital input channels
- SPI3: communication with master processor
- SPI2: control of signage (LEDs)
- N2HET: timing for ADC
- GIO: interrupts for incoming fault signals, control of diagnostic features

The RM41L232 is designed to help develop functionally safe applications. Internal faults are detected and indicated by the fault signal /ERROR, which triggers the safe state in this design. Functional safety designs up to SIL3 (HFT = 0) can be achieved. The [Safety Manual for RM42x and RM41x Hercules™ ARM™-Based Safety Critical Microcontrollers User's Guide](#) provides information regarding system-level integration of the Hercules MCU.

2.4.3.4.2 Safe State

The design distinguishes between two fault classes.

- Faults not influencing the Hercules MCU

- Faults influencing the Hercules MCU

Faults of the first category will not enter the safe state, but the Hercules MCU gets notified. It is the responsibility of the Hercules MCU application software to report these faults to the master processor. The second category of faults may lead to a undetermined function of the Hercules MCU. The safe state is triggered in this case.

The Hercules MCU has two separate reset pins: cold reset (/PORRST pin) and warm reset (/RST pin). A cold reset is required when any of the supply rails of the Hercules MCU are outside of the specified range. A warm reset is triggered if the watchdog fails or an Hercules MCU internal fault is detected. The safe-state is triggered if a cold reset or a warm reset is demanded. The fault sources are:

- V_{core} UV or OV fault (cold reset)
- V_{io} UV fault (cold reset)
- MCU internal error (warm reset)
- windowed watchdog fail (warm reset)

The V_{core} UV fault condition is removed as soon as the voltage is back to normal while the V_{core} OV sticks, as this fault may have damaged the core of Hercules MCU permanently. The SN74LVC2G132 (U6) acts as a RS-flipflop and holds, together with the window comparator U19, the Hercules MCU in cold reset. The Hercules MCU can only be reset by a power cycle.

The inputs to the RS-flipflop are the signals /FLT_1.25V_UV and /FLT_1.25V_OV. These signals are inherently sequential. /FLT_1.25V_OV goes high when V_{io} is available during startup as U19 is powered from V_{io} . V_{core} is not available at this time. This means that /FLT_1.25V_UV is low and /FLT_1.25V_OV is high. /FLT_1.25V_UV will transition from low to high when V_{core} is within limits after power up. V_{core} power up is delayed as U16 is enabled when V_{io} is stable. This startup sequence leads to a logic high at pin 7 of U6. If the V_{core} OV fault occurs, the flip-flop flips and a current is injected to the resistor network of U19 forcing a permanent V_{core} OV condition, even if the fault has disappeared.

A V_{core} UV fault (/FLT_1.25V_UV asserted) has no effect to the flip-flop and triggers a cold reset including the safe state low directly as long as the fault remains.

The V_{io} UV fault is handled by the supervisor portion of the windowed watchdog. If V_{io} drops below 93% of its nominal value a cold reset (and the safe state) is triggered as long as the fault remains.

Hercules MCU internal self-tests can reveal internal errors, which then trigger the /ERROR pin resulting in a warm reset (and safe state).

A windowed watchdog timer is recommended to operate the Hercules MCU in functional safety applications. The TPS3852H33 (U8) is used in this application. The timer expects a falling edge at pin WDI in a time window of $2.2 \text{ ms} < t_w < 9.3 \text{ ms}$ relative to the prior falling edge. If this condition is met, output /WDO remains high. Otherwise, the output /WDO is asserted, a warm reset generated and the safe state triggered.

When a fault triggers the safe state, the load switch TPS22917 (U11) is turned off. The network R21, R22, R25, and D2 allow a trigger from signal /WARM_RST or the output of the 3-input AND gate SN74LVC1G11 (U10). Signal /WARM_RST is connected to pin /RST of the MCU, which is bidirectional. At the same time, it must be maskable (signal /MASK_WARM_RST) to prevent an Hercules MCU warm reset during diagnostics.

U11 powers down the field side of the isolator ISO7741F (U13). If turned off, U11 will actively discharge C29 with a resistance of 150 Ohms to GND. This is important as a current can be drawn from pin IND (if driven high), which can lead to an undefined behavior of U13. Resistor R28 limits the current into pin IND to 1 mA. The maximum voltage at pin VCC2 of U13 cannot get higher than 150 mV as the 1 mA flows through the discharge circuit (150 Ohm) of U11. U13 is designed to drive any output pin (here OUTD) on the isolated side low in case a power-down occurs. The design is then considered to be in the safe state.

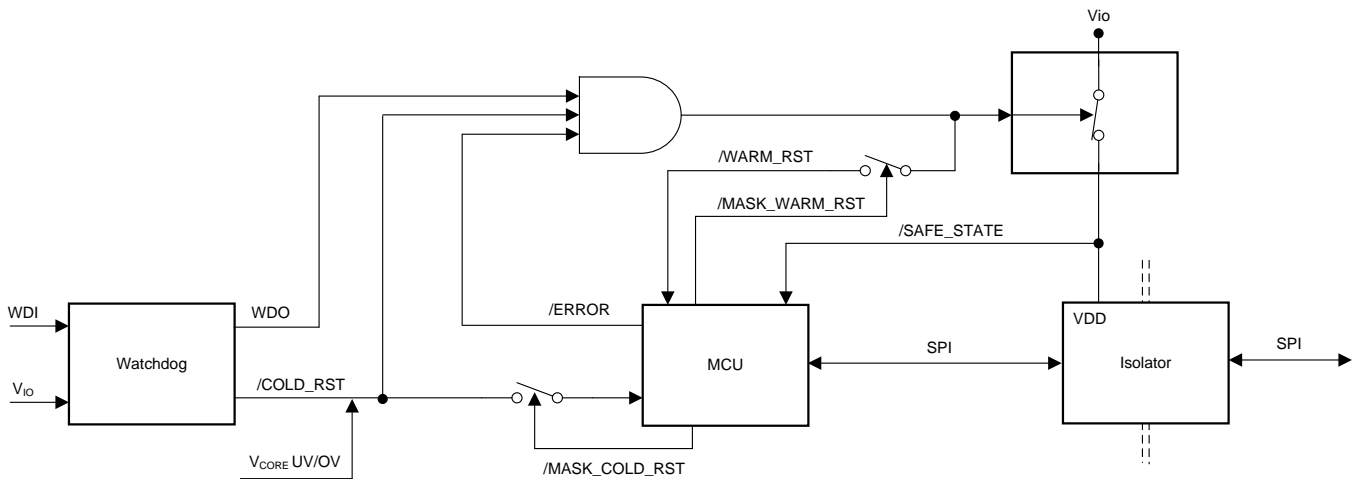
The trigger of the safe state logic itself is not maskable. It is implementation-dependent whether the MCU notifies the master processor about a imminent test or if the master processor commands a test. In any case, the master processor must be able to distinguish whether the seen safe state is a result of a test or a real safe state.

During normal operation, the signal MASTER_SPI_MISO is forced high between transfers by the pull-up resistor R26.

The maximum delay time for a safe state to be recognized by the master processor is the data frame length. This means short data frames are recommended. If longer frames are desired, forced 1bits distributed in the frame, which are checked by the master processor on-the-fly, can decrease the safe state response time.

Figure 6 shows the block diagram of the safe state logic.

Figure 6. TIDA-010049 Safe State Logic



2.4.3.5 Monitoring/Diagnostics

The *Monitoring and Diagnostics* element combines a set of diagnostics and monitoring features to test and observe the components important for the safety function. This element also includes the internal Hercules MCU monitoring and diagnostics features.

2.4.3.5.1 Voltage Monitors

In this design, all voltage rails are monitored.

V_{in} (24 V) is monitored by the *Power Delivery* element. If V_{in} is less than 19 V or greater than 29 V, the eFuse U21 generates a fault signal (/FLT_SENSSUP), which is reported to the microcontroller. See 2.4.3.2 for more information.

V_{int} (4.3 V) is monitored by a window comparator. It will generate a fault signal (/FLT_4.3V) to the microcontroller if V_{int} is out of boundaries of $\pm 5\%$.

V_{io} (3.3 V) UV is monitored by the supervisor portion of the WWDT. The fault is triggered if V_{io} falls below 93% of its nominal voltage. The V_{io} UV fault output (/RESET) is tested by pulling the /MR pin low (asserting signal /TST_RST). Asserting signal MASK_COLD_RST (high) prevents a cold reset of the MCU but triggers the safe state logic function for testing. V_{io} OV is monitored by a comparator and reported to the MCU. This fault is not critical as the voltage can only go to V_{int} at maximum, which is not critical.

V_{core} (1.25 V) is monitored by a window comparator. The UV fault signal (/FLT_UV_1.2V) is triggered at 92.5% of its nominal value. The OV fault signal (/FLT_OV_1.2V) is triggered at 105% of its nominal value. The OV fault signal is sticky, as in, it can only be removed by a power cycle. See 2.4.3.4.2 for more information.

2.4.3.5.2 Power Delivery Monitor

The *Power Delivery* element provides power to the external sensors and is sourced by V_{in} . The output turns off in UV, OV, overcurrent, or thermal condition. A fault flag (/FLT_SENSSUP) reports to the Hercules MCU that at least one of these faults has occurred. See 2.4.3.2 for more information.

2.4.3.5.3 Temperature Monitor

Ambient temperature is monitored by the temperature sensor TMP302C (U20). If the board temperature rises above 100°C, an ambient temperature fault (/FLT_TEMP asserted) is reported to the microcontroller.

2.4.3.5.4 ADC Monitor

Analog input channel ADIN5 is connected to a shunt reference, which supplies a constant voltage of 2.5-V DC. If the digital code of this channel deviates from its predefined nominal value range, it is considered a fault.

The internal multiplexer can be tested by sampling known voltages at ADIN5 (2.5V) and ADIN[0, 1, 3, 4, 6, 16, 20] (GND).

2.4.3.5.5 Window Watchdog Timer Diagnostics

The windowed watchdog timer (WWDT) portion of the TPS3852 (U8) is tested periodically as the TPS3852 is considered a complex element. The test is performed by omitting watchdog pulses generated by the MCU. As a result the TPS3852 will assert pin /WDO, which generated a warm reset to the MCU. A mask signal MASK_WARM_RST prevents the MCU from entering the warm reset. See 2.4.3.4.2 for more information.

2.4.3.5.6 Digital Input Front-End Diagnostics

The digital input signal chain can be tested if the input state remains constant for longer than DTI to ensure it can still transition to the opposite state. The logic buffer SN74LVC1G125 (U1) injects a signal opposite to the current sensed state.

If fault of a digital input is detected by the software, the application software must perform one or more of the following actions:

1. Communicate fault to the master processor
2. Passivate the channel
3. Passivate the module

The module will not enter the safe state as the functionality of the MCU is not affected by this fault.

See [2.4.3.3](#) for more information.

2.4.3.5.7 SafeState Diagnostics

Triggering the safe function is the result of a set of diagnostics and monitors:

1. /ERROR signal of the microcontroller (internal error)
2. WWDT fault
3. V_{io} UV fault
4. V_{core} UV and OV fault

Items two and three blank the communication between the Hercules MCU and the master processor for a maximum of 230 ms. This time is dominated by the windows watchdog /RESET and /WDO assertion time.

2.4.3.5.8 Hercules MCU Diagnostics

The /ERROR pin of the Hercules MCU is manually triggered within the DTI to ensure it can trigger the safe state logic in case an internal fault occurs. The signal MASK_WARM_RST prevents a warm reset of the Hercules MCU during test.

2.4.3.6 Signage

The LED signage part is not functional-safety related. The 8-bit, serial-to-parallel shift register SN74AHC594 (U22) expands the SPI port to 8 general-purpose outputs, driving one green status LED per digital input channel. When the LED is on the MCU, it reads a 1-state. Otherwise, the MCU reads a 0-state (application-programmable).

The red LED D7 is used as global fault indicator and is application-programmable. The MCU signal is buffered by the logic buffer SN74LVC1G125 (U23).

The green LED D8 is on if V_{in} is greater than 19 V to indicate the minimum operating voltage is available.

2.4.3.7 Fault Handling

2.4.3.7.1 Monitoring Faults

表 4 shows a list of detectable system faults, such as voltage and temperature, which are passively detected by monitors.

表 4. Faults Passively Detected by Monitoring Feature

ID	FAULT	FAULT EVENT TRIGGERS	FAULT EVENT CONSEQUENCE	REASON
MF1	V_{in} UV/OV	Notification to MCU	Application-programmable	Input stage or passives fault, SELV/PSELV PSU fault
MF2	V_{int} UV/OV	Notification to MCU	Application-programmable	DC/DC 1 fault
MF3	V_{io} OV	Notification to MCU	Application-programmable	DC/DC 2 fault
MF4	V_{io} UV	MCU cold reset, temporary safe-state	Reboot of system	DC/DC 2 fault
MF5	V_{core} OV	Module passivation	Permanent safe-state, (power cycle reactivates module)	DC/DC 3 fault
MF6	V_{core} UV	MCU cold reset, temporary safe-state	Reboot of system	DC/DC 3 fault

表 4. Faults Passively Detected by Monitoring Feature (continued)

ID	FAULT	FAULT EVENT TRIGGERS	FAULT EVENT CONSEQUENCE	REASON
MF7	V _{sup}	Notification to MCU	Application-programmable	Vsup output short to GND, voltage source higher than Vin connected
MF8	Ambient temperature	Notification to MCU	Application-programmable	Ambient temperature above limit

2.4.3.7.2 Diagnostics Faults

Selected hardware components are periodically tested to verify their correct operation. 表 5 shows the supported diagnostic functions.

表 5. Faults Actively Detected by Diagnostic Features

ID	FAULT	PART(S) AFFECTED	DIAGNOSTIC TRIGGER	DIAGNOSTICS FAIL	REASON(S)
DF1	Watchdog	TPS3852 (U8)	MCU skips WD pulse	Module does not enter safe-state	WD pulse not skipped, U8 does not assert pin /WDO, fault in safe function signal chain
DF2	V _{io} UV	TPS3852 (U8)	Assert /MR pin	Module does not enter safe-state	/MR pin at U8 not asserted, U8 does not assert pin /RST, fault in safe function signal chain
DF3	Digital input channel	Logic (U1), Amp (U2), Ref (U5)	Enable channel diagnostics	State does not change	Fault of components in input channel
DF4	MCU	RM41L232 (U7)	BIST	/ERROR asserted	MCU internal fault
DF5	MCU	RM41L232 (U7)	/ERROR asserted	Module does not enter safe-state	/ERROR not asserted, fault in safe function signal chain
DF6	Safe function	Logic (U10), Switch (U11), Isolator (U13)	DF1/DF2/DF4 or DF5	Master processor and MCU disagree on safe function diagnostics result	DF1/DF2/DF4 or DF5 trigger fault, fault in safe function signal chain
DF7	Analog-to-digital converter/external reference	RM41L232 (U7)	Convert analog-to-digital converter input channel ADIN[5]	Converted code deviates from expected code	External reference fault, ADIN[5] driving circuit fault, multiplexer fault

3 Hardware, Software, Testing Requirements, and Test Results

3.1 Required Hardware and Software

The TIDA-010049 is a stand-alone board. Once the application software is flashed in the MCU, the design can run on its own. In a real application, the design communicates with a master processor using header J3.

3.1.1 Hardware

A 24-V DC power supply connected to J4 is required to operate the board. The master processor communicates with the board using J3, which provides an isolated SPI. The application software is flashed with a JTAG emulator, such as the [XDS200 USB debug probe](#), using the 20-pin header J1. [図 7](#) shows the placement of the components.

3.1.1.1 Header/Connector Pinouts

This section describes all header/connector for this design.

Header J1 is a 20-pin JTAG pinout to connect emulators to the Hercules MCU. Please see the [XDS200 Quick Start Guide](#) for the CTI20 pinout used here.

Header J2 is a 2-pin header to disable (jumper removed or to enable (jumper inserted) the watchdog. This feature helps preventing the watchdog kicking in during development.

Header J3 provides the isolated SPI communication to the master processor. See [表 6](#) for the pinout.

表 6. Isolated SPI Pinout

PIN NAME	DESCRIPTION
J3.1	Isolated ground
J3.2	SPI data line from Hercules MCU to master processor (MASTER_SPI_MISO)
J3.3	SPI data line from master processor to Hercules MCU (MASTER_SPI_MOSI)
J3.4	SPI clock signal
J3.5	SPI CS signal
J3.6	Isolated 3.3 V

Connector J4 is connected to the external SELV/PELV power supply. See [表 7](#) for the assignment of the terminals.

表 7. 24V DC Power Supply Pinout (J4)

TERMINAL NAME	DESCRIPTION
J4.1	24-V DC
J4.2	GND

Connector J5/J6 provides power to the external sensors and the digital input terminals. See [表 8](#) for the assignment of the terminals.

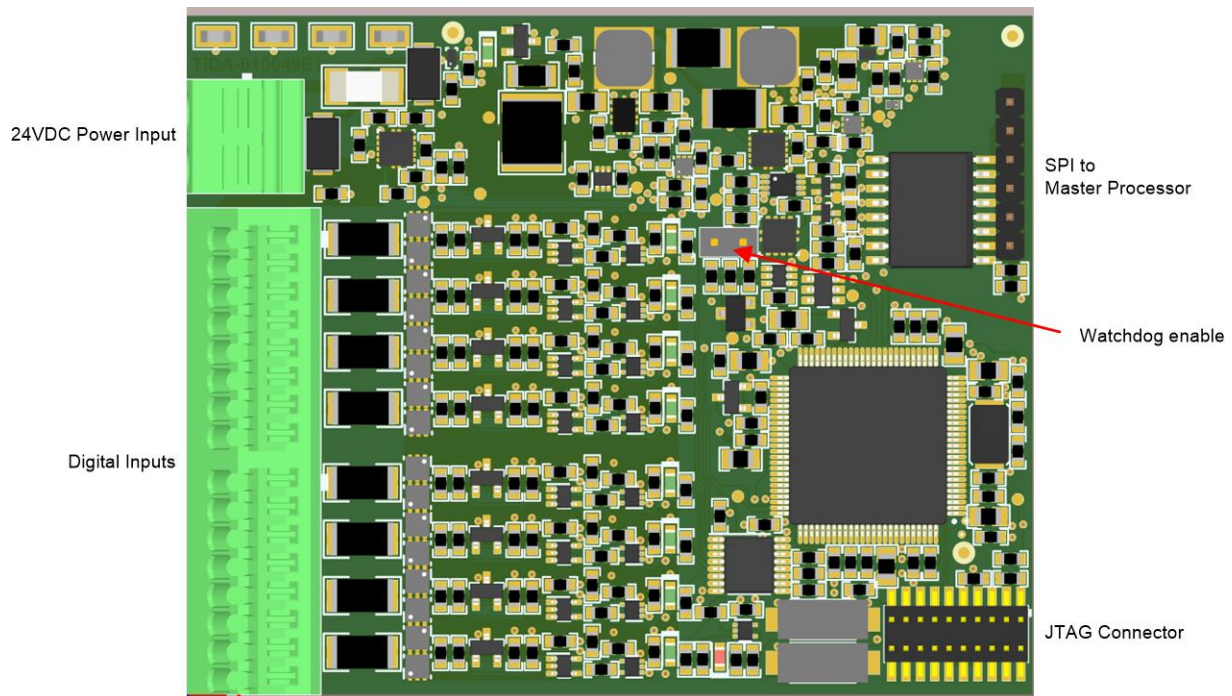
表 8. Power Delivery and Digital Inputs

TERMINAL NAME	DESCRIPTION
J5.1	Digital input channel 1
J5.2	Optional power external sensor 1
J5.3	Digital input channel 2

表 8. Power Delivery and Digital Inputs (continued)

TERMINAL NAME	DESCRIPTION
J5.4	Optional power external sensor 2
J5.5	Digital input channel 3
J5.6	Optional power external sensor 3
J5.7	Digital input channel 4
J5.8	Optional power external sensor 4
J6.1	Digital input channel 5
J6.2	Optional power external sensor 5
J6.3	Digital input channel 6
J6.4	Optional power external sensor 6
J6.5	Digital input channel 7
J6.6	Optional power external sensor 7
J6.7	Digital input channel 8
J6.8	Optional power external sensor 8

図 7. TIDA-010049 Connector Placements



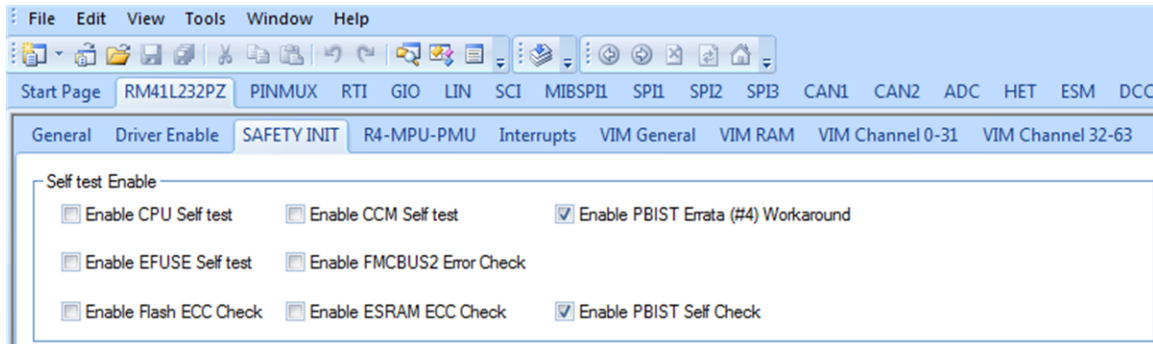
3.1.2 Software

A test program (not part of the deliverables of the TIDA-010049 reference design package) was developed to test functionality of the described features. The development platform is the [Code Composer Studio v8.0.0](#) IDE. The MCU is initialized using the [HALCOGEN](#) tool.

During software development, TI recommends disabling the watchdog timer by leaving header J2 open. This prevents unwanted MCU resets and communication loss to the IDE. If the watchdog is not served by signal WDI, the signal /WDO is asserted approximately 11 ms after signal /COLD_RST is deasserted. Asserting signal /WDO results in a warm reset preventing a boot up. Debugging or stopping the program or a not-served WDI result in missing WDI pulses, causing a reset.

When using the HALCOGEN tool, it is important to uncheck *Enable EFUSE Self test* and *Enable ESRAM ECC* in tab *RM41L232PZ / SAFETY INIT* shown in [Figure 8](#). These tests, initially enabled, cause the MCU signal /ERROR to go low, resulting in an immediate warm reset of the MCU. During normal operation, the signal MASK_WARM_RST prevents a warm reset during the application-programmable tests. However, this signal is not initialized at the time the HALCOGEN performs these tests (before main). Once the signal MASK_WARM_RST is under application control, the two remaining tests can be performed with signal MASK_WARM_RST asserted.

Figure 8. Hercules Safety Init Configuration

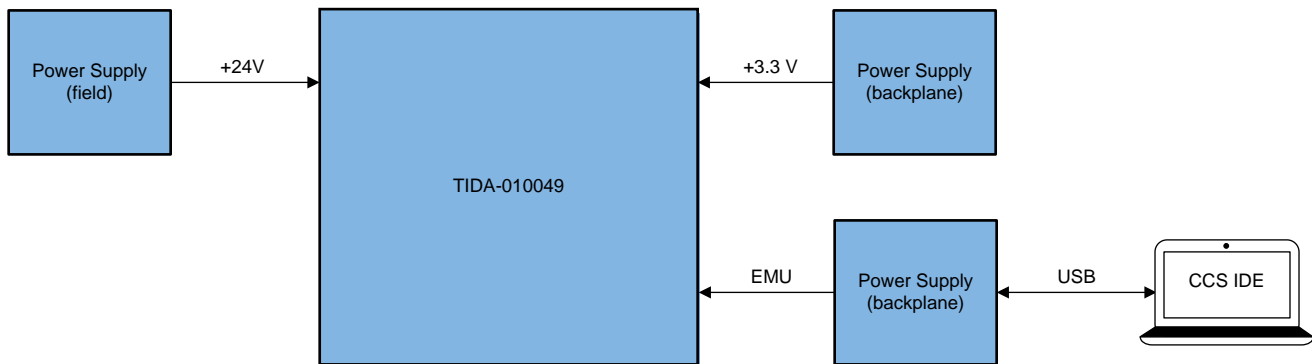


3.2 Testing and Results

3.2.1 Test Setup

The test setup is shown in [Figure 9](#). The TIDA-010049 reference design is powered from a lab power supply generating 24-V DC. The external sensors are simulated by shorting a DI to V_{sup} (switch of external sensor closed) or connecting a 100 k Ω between V_{sup} and a DI (switch open).

Figure 9. TIDA-010049 Test Setup

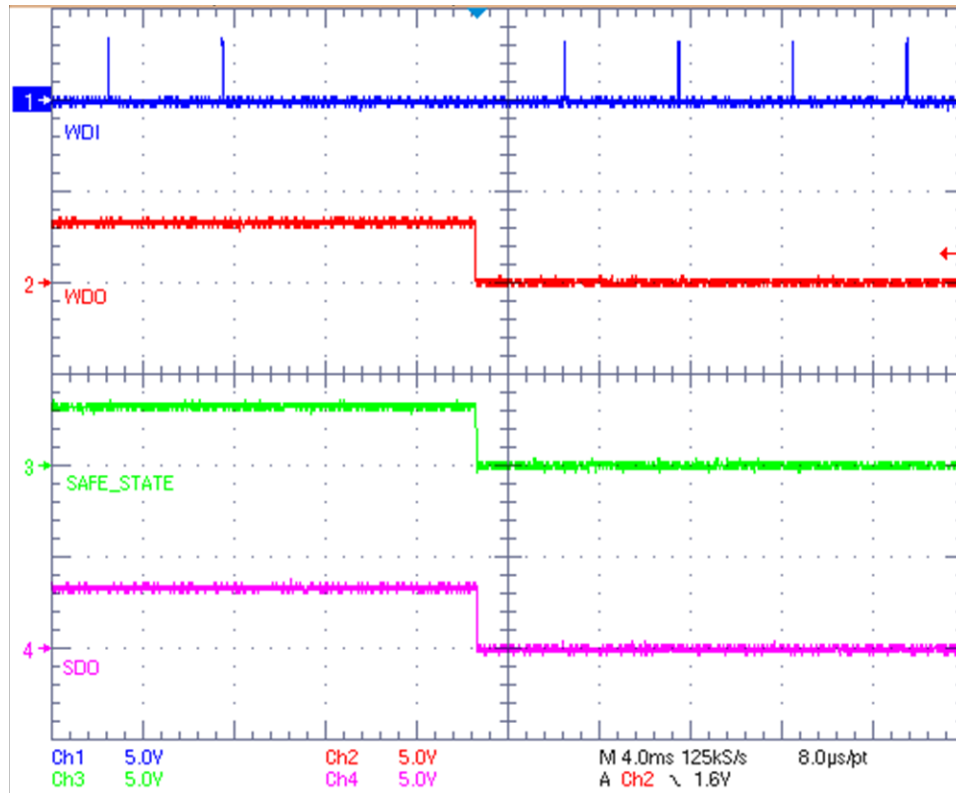


Alternatively, the external sensor switches can also be provided by the [8-channel, 2-A high-side driver reference design for digital output modules](#). This combination has been tested and works as expected. A master processor was not connected to the TIDA-010049 during hardware testing.

3.2.2 Test Results

[Figure 10](#) shows the sequence from the WDI signal fail to SDO (here signal MASTER_SPI_MISO) forced low, which is the safe state in this design.

図 10. Safe-State Triggered by Watchdog



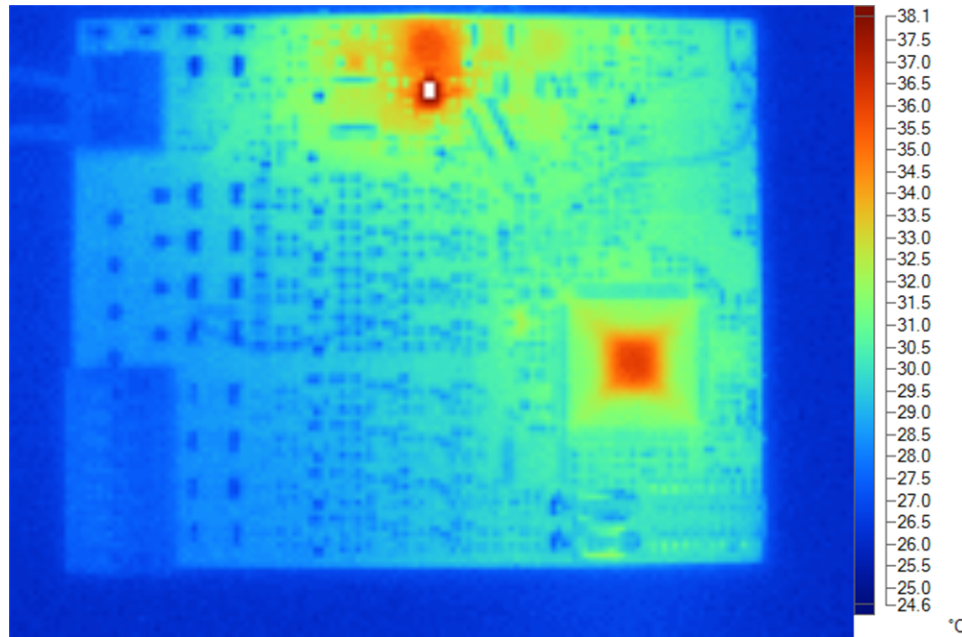
As long as the watchdog timer is served by periodic pulses at WDI (yellow trace) the signal /WDO (blue trace) is deasserted (normal operation). This condition is satisfied if the falling edge of WDI has a period of 2.2 ms to 9.3 ms. If the period is shorter or longer, signal /WDO is asserted. This event causes signal /SAFE_STATE (purple trace) to go low as the load switch U11 disconnects the isolator U13 from V_{io} and connects the power pin of the isolator to ground using the load switch discharge feature. As a result, the isolator sets the only output, signal MASTER_SPI_MISO (green signal SDO), low. The safe-state is reached within 22 μ s once a fault is detected.

The time the safe-state is reached during a WDT fault is dominated by the watchdog timeout. The pull-up resistor R16 provides the fastest reaction time possible. See the [TPS3852 precision voltage supervisor with programmable window watchdog timer data sheet](#) to learn how to increase the WDI period and, thus, the reaction time.

3.2.2.1 Power Consumption

The current consumption at $V_{in} = 24$ V under normal operation is 23.5 mA. This leads to a module power consumption of 0.57 W. 図 11 shows the heat distribution after a settling time of 10 minutes of normal operation without load connected to power delivery.

図 11. TIDA-010049 Heat Distribution



The buck converter LMR36006 (U14) of the first power stage in the top middle is the warmest spot on the board at 38.1°C, which is about 13.5°C above ambient temperature, which is inline with calculations. The Hercules MCU running at a clock speed of 80 MHz is in range of 36°C.

The maximum-allowed ambient temperature of this design is 105°C, dictated by the Hercules MCU.

3.2.2.2 Test Cases

The tests shown in 表 9 were performed to verify expected operation of the circuit during the given fault. Each test was performed isolated, as in, a full power cycle was executed between the tests.

Faults which are critical for reliable MCU operation trigger a reset of the MCU. The MCU reset is suppressed by signals MASK_*. Asserting these signals as stated below suppress a MCU reset as stated in the test cases.

Test cases starting with *M* test monitoring functions (observation of a value). Test cases starting with *D* test diagnostics functions (force a predefined state to verify correct function).

表 9. Test Plan

TEST CASE	SECTION	TEST	ACTION	EXPECTED RESULT	CONDITIONS	TEST RESULT
M1	Power supply	V _{in} UV supply	Apply 18.5 V/GND to J4.1/2	Power delivery not working (/FLT_SENSSUP asserted), LED D8 off	-	OK
M2		V _{in} OV supply 1	Apply 29.5 V/GND to J4.1/2	Power delivery not working (/FLT_SENSSUP asserted), LED D8 on	-	OK
M3		V _{in} OV supply 2	Apply 40 V/GND to J4.1/2	Fuse burned, board permanently de-energized, no input current	-	NOT TESTED
M4		V _{in} reverse polarity	Apply 24 V/GND to J4.2/1	No input current	-	OK
M5		V _{sup} reverse current	Apply 24 V/GND to J5.2/J4.2	No input current	-	OK
M6		V _{sup} reverse polarity	Apply 24 V/GND to J4.2/J5.2	No input current	-	OK
M7		Overload	Short J5.2 to J4.2	No current J5.2 to J4.2	Normal operation	OK
M8		V _{int} OV	Short R41	/FLT_4.3V asserted	V _{in} = 24 V	OK
M9		V _{int} UV	Short R47	/FLT_4.3V asserted	V _{in} = 24 V	OK
M10		V _{io} OV	Short R46	FLT_3.3V_OV asserted	V _{in} = 24 V	OK
M11		V _{core} OV	Temporarily short R40	/FLT_1.2V_OV asserted, /COLD_RST permanently asserted (until power cycle)	V _{in} = 24 V	OK
M12		V _{core} UV	Short R48	/FLT_1.2V_UV asserted, /COLD_RST asserted	V _{in} = 24 V	OK
M13	Temperature sensor	Test temperature sensor	Not performed	/FLT_TEMP asserted	V _{in} = 24 V	NOT TESTED
D1	Watchdog	V _{io} UV	Assert MASK_COLD_RST and MASK_WARM_RST, assert /TST_RST	Safety function triggered, /SAFE_STATE asserted, MASTER_SPI_MISO low	Normal operation	OK
D2	Watchdog	WDI pulse missing/bad timing	Assert MASK_WARM_RST, suppress WDI pulse	Safety function triggered, /SAFE_STATE asserted, MASTER_SPI_MISO low	Normal operation	OK
D3	MCU	Internal MCU error	Assert MASK_WARM_RST, assert /ERROR	Safety function triggered, /SAFE_STATE asserted, MASTER_SPI_MISO low	Normal operation	OK
D4	VREF	UV/OV	100-Ohm resistor between U12.1 and GND	ADC code for ADIN5 changes	Normal operation	OK

表 9. Test Plan (continued)

TEST CASE	SECTION	TEST	ACTION	EXPECTED RESULT	CONDITIONS	TEST RESULT
M14	DIN	DI reverse polarity (module not powered)	Apply 24 V/GND to J4.2/J5.1	No input current	$V_{in} = 0$ V	OK
D5		Force 0-state	Short J5.1 and J5.2, apply DIAG-0 to DI1	0-state is read while 1-state is applied to the input	Normal operation	OK
D6		Force 1-state	100-k Ω resistor between J5.1 and J5.2, apply DIAG-1 to DI1	1-state is read while 0-state is applied to the input	Normal operation	OK
D7		DI1 to DI2 short in 0-state	100-k Ω resistor between J5.1 and J5.2, 100-k Ω resistor between J5.3 and J5.4, short J5.1 and J5.3, apply DIAG-1 to DI1	DI1 changes from 0-state to 1-state, DI1 remains in 0-state, DI2 ADC input voltage raises about 300 mV	Normal operation	OK
D8		DI1 to V_{in} short	Short J4.1 to J5.1, de-assert SENSSUP_CTRL	DI1 still in 1-state	Normal operation	OK
D9		DI1 to GND short, external switch on (low impedance)	Short J5.1 to J5.2, short J5.1 to J4.2	/FLT_SENSSUP asserted (overcurrent) - latched, DI1 in WB-state	Normal operation	OK
D10		DI1 to GND short, external switch off (high impedance)	100-k Ω resistor between J5.1 to J5.2, short J5.1 to J4.2	DI1 in WB-state	Normal operation	OK
D11		V_{in} to V_{sup} short, external switch on (low impedance)	Short J5.1 to J5.2, short J5.2 to J4.1, de-assert SENSSUP_CTRL	DI1 still in 1-state	Normal operation	OK
D12		V_{in} to V_{sup} short, external switch off (high impedance)	100-k Ω resistor between J5.1 to J5.2, short J5.2 to J4.1, de-assert SENSSUP_CTRL	DI1 still in 0-state	Normal operation	OK
D13		V_{sup} to GND short	Short J5.2 to J4.2	/FLT_SENSSUP asserted (overcurrent) - latched, all DI in WB-state	Normal operation	OK
D14		DI open wire	-	DI1 in WB-state	Normal operation	OK

4 Design Files

The following sections show the collateral of this design downloadable from the product folder from <http://www.ti.com>.

4.1 Schematics

To download the schematics, see the design files at [TIDA-010049](#).

4.2 Bill of Materials

To download the bill of materials (BOM), see the design files at [TIDA-010049](#).

4.3 PCB Layout Recommendations

The size of the board is 75 mm x 60 mm (2.95" x 2.36"). All components are placed on the top side for better debugging. All field-side related signals (digital inputs, supplies) are connectable using terminal blocks on the left side of the board. The SPI bus to the master located at the backplane side is placed on the right side of the board. Visibility from the terminal side was not taken into consideration in the placement of the LEDs as expected in a I/O module mounted in a I/O slot of the PLC. This is a reference design not considered to be used as-is in a system.

4.3.1 Layout Prints

To download the layer plots, see the design files at [TIDA-010049](#).

4.4 Altium Project

To download the Altium Designer® project files, see the design files at [TIDA-010049](#).

4.5 Gerber Files

To download the Gerber files, see the design files at [TIDA-010049](#).

4.6 Assembly Drawings

To download the assembly drawings, see the design files at [TIDA-010049](#).

5 Related Documentation

1. Texas Instruments, [Safety manual for RM42x and RM41x Hercules™ Arm® -based safety critical microcontrollers user's guide](#)
2. Texas Instruments, [ADC source impedance for Hercules™ Arm® safety MCUs application report](#)
3. Texas Instruments, [Reference design of eight-channel, parallel, 1-A, high-side, digital output module for PLC design guide](#)
4. Spectrum Digital, Inc. (SDI), [XDS200 Quick Start Guide](#)

5.1 商標

E2E, Hercules, FemtoFET are trademarks of Texas Instruments.
Altium Designer is a registered trademark of Altium LLC or its affiliated companies.
Arm, Cortex are registered trademarks of Arm Limited.
すべての商標および登録商標はそれぞれの所有者に帰属します。

5.2 **Third-Party Products Disclaimer**

TI'S PUBLICATION OF INFORMATION REGARDING THIRD-PARTY PRODUCTS OR SERVICES DOES NOT CONSTITUTE AN ENDORSEMENT REGARDING THE SUITABILITY OF SUCH PRODUCTS OR SERVICES OR A WARRANTY, REPRESENTATION OR ENDORSEMENT OF SUCH PRODUCTS OR SERVICES, EITHER ALONE OR IN COMBINATION WITH ANY TI PRODUCT OR SERVICE.

6 **About the Author**

LARS LOTZENBURGER is a systems engineer at Texas Instruments, where he is responsible for developing reference design solutions for the industrial segment. Lars brings to this role his extensive experience in analog and digital circuit development, PCB design, and embedded programming. Lars earned his diploma in electrical engineering from the University of Applied Science in Mittweida, Saxony, Germany. He currently focuses on functional safety and human machine interface (HMI) applications for the industrial sector.

重要なお知らせと免責事項

TI は、技術データと信頼性データ(データシートを含みます)、設計リソース(リファレンス・デザインを含みます)、アプリケーションや設計に関する各種アドバイス、Web ツール、安全性情報、その他のリソースを、欠陥が存在する可能性のある「現状のまま」提供しており、商品性および特定目的に対する適合性の黙示保証、第三者の知的財産権の非侵害保証を含むいかなる保証も、明示的または黙示的にかかわらず拒否します。

これらのリソースは、TI 製品を使用する設計の経験を積んだ開発者への提供を意図したものです。(1) お客様のアプリケーションに適した TI 製品の選定、(2) お客様のアプリケーションの設計、検証、試験、(3) お客様のアプリケーションに該当する各種規格や、その他のあらゆる安全性、セキュリティ、規制、または他の要件への確実な適合に関する責任を、お客様のみが単独で負うものとします。

上記の各種リソースは、予告なく変更される可能性があります。これらのリソースは、リソースで説明されている TI 製品を使用するアプリケーションの開発の目的でのみ、TI はその使用をお客様に許諾します。これらのリソースに関して、他の目的で複製することや掲載することは禁止されています。TI や第三者の知的財産権のライセンスが付与されている訳ではありません。お客様は、これらのリソースを自身で使用した結果発生するあらゆる申し立て、損害、費用、損失、責任について、TI およびその代理人を完全に補償するものとし、TI は一切の責任を拒否します。

TI の製品は、[TI の販売条件](#)、または ti.com やかかる TI 製品の関連資料などのいずれかを通じて提供する適用可能な条項の下で提供されています。TI がこれらのリソースを提供することは、適用される TI の保証または他の保証の放棄の拡大や変更を意味するものではありません。

お客様がいかなる追加条項または代替条項を提案した場合でも、TI はそれらに異議を唱え、拒否します。

郵送先住所 : Texas Instruments, Post Office Box 655303, Dallas, Texas 75265

Copyright © 2022, Texas Instruments Incorporated