Technical White Paper

Simplifying Robotics Motor Drive Safety Assessments to Reduce System BOM

Kristen Mogensen, Martin Staebler (Stäbler), Ester Vicario
Systems Engineering and Marketing

Abstract

As the use of robotic systems in industrial environments increases, the industry safety requirements and national and international safety regulations are continually updated to maintain a safe and secure environment for when humans are working in close proximity to machines. Functional safety assessments are required to demonstrate that products meet certain safety requirement standards, so products can be responsibly released to market.

Safety assessments can be a long process, delaying the time-to-market and increasing the overall design cost of the product. This document explains how to simplify the assessment process using a motor drive for an autonomous mobile robot (AMR) as an example. The document describes the aspects to consider for selecting the right semiconductor devices, meeting the safety requirements, and reducing the overall bill of materials (BOM) size and potential costs. This white paper shows how to speed up safety assessments by describing the steps to follow to meet the safety requirements and potentially achieve lower design cost.

Table of Contents

1 Introduction 2
2 Understanding CAT2, PLd Safety Requirements 2
2.1 Safety Requirements per the ISO 3691-4 Standard 3
2.2 System Architecture Selection 5
2.3 Device Selection Based on Process Safety Time 6
3 Implementing Mobile Robot Motor Drive Safety Requirements 6
4 Conclusion 9

List of Figures

Figure 1-1. Hierarchy of A, B, C Standards Typically Used in Robotic Applications 2
Figure 2-1. Simplified Mobile Robot Block Diagram 3
Figure 2-2. Designated Architectures for Categories 2 and 3 per IEC 13849-1 5
Figure 2-3. Functional Safety Related Timing Considerations 6
Figure 3-1. Motor Drive System Block Diagram 7
Figure 3-2. Simplified Motor Drive System Including Safety Features 9

List of Tables

Table 2-1. The Relationship Between the IEC 61508 Standard SIL and the ISO 13849 Standard PL 4
Table 2-2. PL and SIL Relationship Through PFH and $MTTF_d$ Parameters 4
Table 2-3. Safety Requirements per the ISO 3691-4 Standard 4
Table 3-1. Example of Diagnostic Coverage Required per Device Type 9

Trademarks

C2000™ is a trademark of Texas Instruments.
All trademarks are the property of their respective owners.

Copyright © 2026 Texas Instruments Incorporated

1 Introduction

Industries rely on automation to increase production rates and overall efficiencies. To raise the productivity, companies are deploying robots in factories and humans continue to work alongside these machines. As a result, employees are exposed to new types of hazards that require regulation to provide personal safety. To show that robots meet safety requirements, prior to being released to the market, each product must go through a safety assessment. Assessments must show that machines meet the minimum safety requirements based on the necessary Type C product safety standard. Figure 1-1 shows some typical standards used for robotic applications and shows how these standards connect with each other. Different standards can be used for arguing a robotic implementation which is integrated for different purposes.

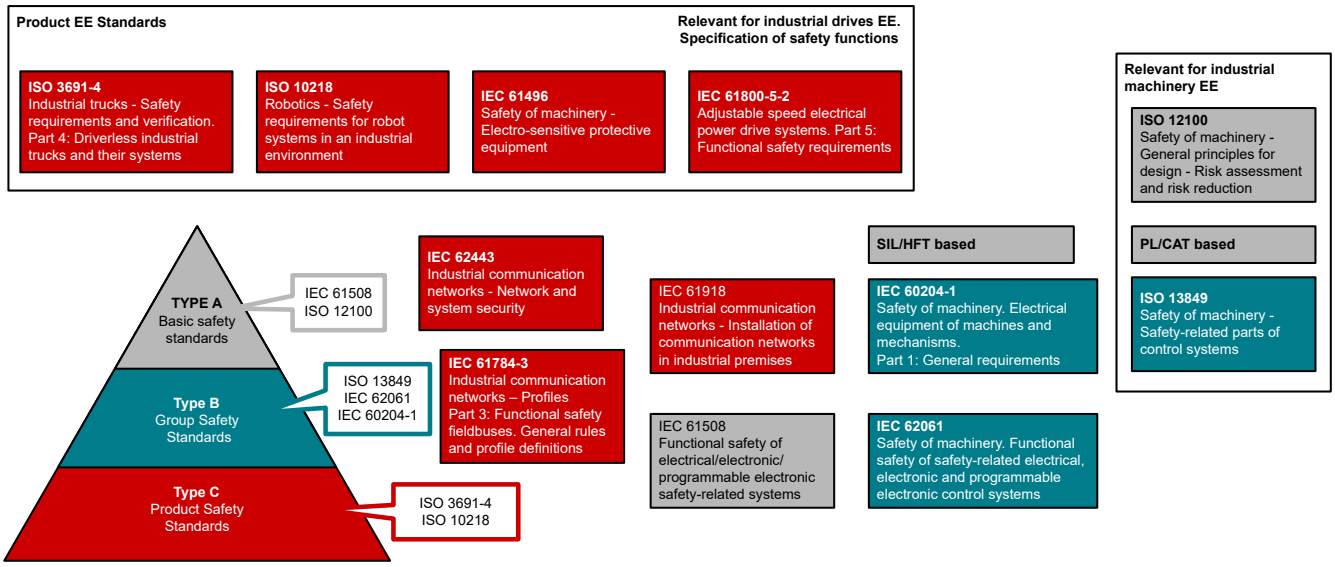


Figure 1-1. Hierarchy of A, B, C Standards Typically Used in Robotic Applications

Demonstrating that the product is safety-compliant is typically a long and complex procedure, which increases the overall design cost, robot size, and time-to-market. This white paper offers a simplified explanation of the process to follow for conducting a safety assessment of a motor drive. The assessment uses the Type C standard of the ISO 3691-4 standard. The Type C standard defines the type of safety architecture and performance level that is required for the assessment. In this use-case, the ISO 3691-4 standard refers to the ISO 13849 standard and the safety performance level d (PLd). The implementer must determine whether to design a category 3 (CAT3) PLd system or a category 2 (CAT2) PLd system. In this use-case, cost and size are critical; therefore, an analysis was included for a block-level concept of how to achieve CAT2 using a safety rated component by TI. In this use-case, the block-level system was shown to achieve a PLd of CAT2, according to the ISO 13849 standard, or a safety integrity level 2 (SIL 2) and hardware fault tolerance (HFT) equal to zero, according to the IEC 60204-1 standard. This use-case is intended to help readers effectively meet the safety requirements of ISO 3691-4 while maintaining a smaller BOM size, potentially at a lower cost. The ISO 3691-4 (section 4) standard is the standard for industrial trucks; however, section four of the standard also covers autonomous trucks, which are used as the *state-of-the art* standard when developing autonomous mobile robots (AMRs) for warehouse environments. The procedure used in this use-case can be used with any other machinery that requires a PLd of Cat 2 for safety.

This concept uses TI's latest high-performance, motor control, C2000™ real-time microcontroller and PMICs which both include on-chip safety functionality. Designers can potentially achieve lower costs of the overall system, associated with a smaller BOM size implementation, and reduce the time-to-market for this solution by using the C2000 product family, these design concepts, and additional TI Functional Safety resources.

2 Understanding CAT2, PLd Safety Requirements

Understanding the required safety standards of a product is crucial during the first step of the product design process. Since this white paper uses a mobile robot motor drive as an example, the requirements of the ISO 3691-4 safety standard must be applied for the product.

Copyright © 2026 Texas Instruments Incorporated

2.1 Safety Requirements per the ISO 3691-4 Standard

The ISO 3691-4 standard defines the safety requirements and verifications for driverless industrial trucks, including industrial mobile robots (IMRs), such as autonomous mobile robots (AMRs). The standard describes the safety requirements of the overall machine; however, the designer is responsible for determining where the safety functions are placed within the industrial truck modules, as seen in Figure 2-1.

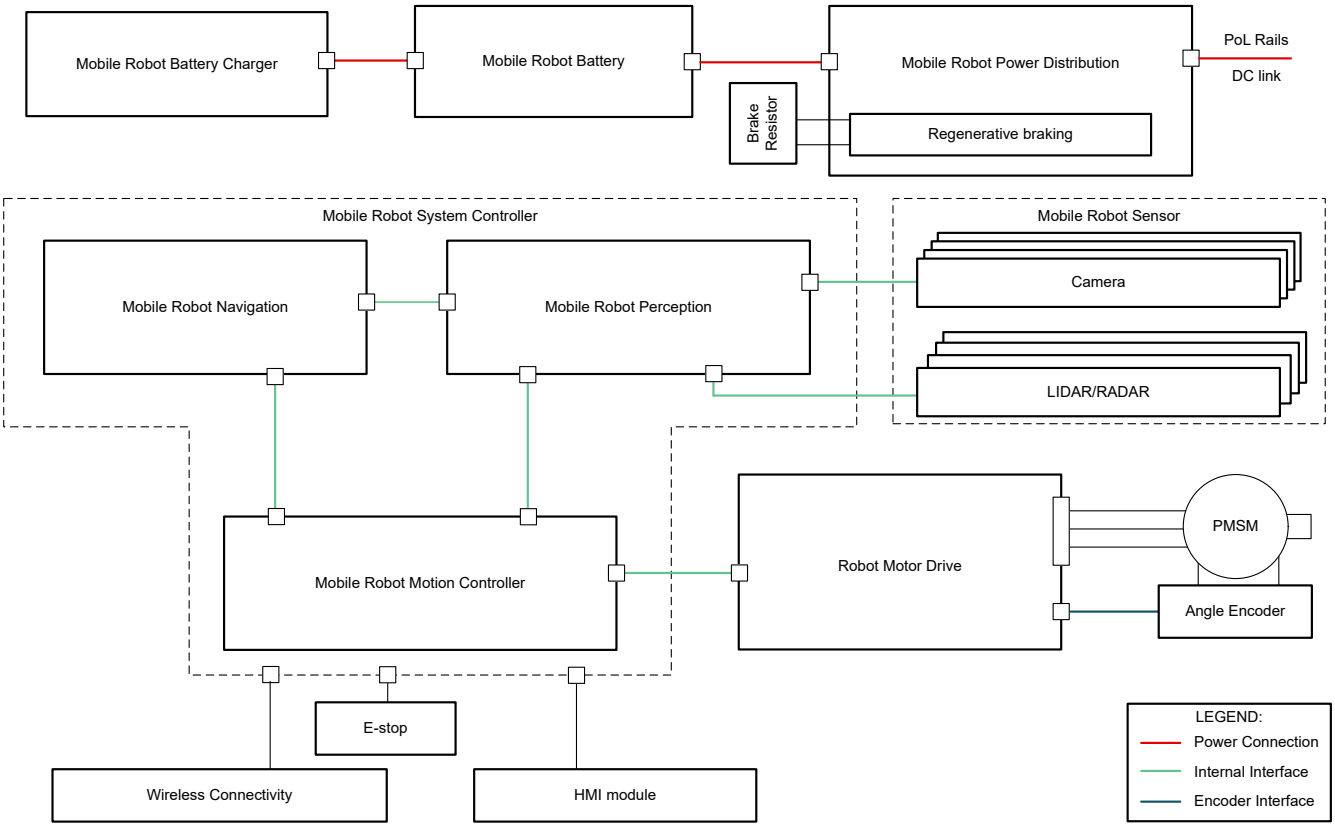


Figure 2-1. Simplified Mobile Robot Block Diagram

The ISO 3691-4 safety standard describes the safety considerations that must be implemented to meet necessary risk reductions when a hazardous situation exists. For each of the described risk situations, the ISO 3691-4 standard assigns a minimum required performance level (PL) according to the ISO 13849-1 standard. The PL is a value commonly used to achieve the required risk reduction for each safety function and is defined in the machinery standard of ISO 13849-1 (Section one).

Similar to the PL, several standards use the safety integrity level (SIL) to measure the system safety performance. The parameters of the SILs are defined in the IEC 61508 standard. The relationship between the PL and SIL is found in Table 2-1.

Copyright © 2026 Texas Instruments Incorporated

Table 2-1. The Relationship Between the IEC 61508 Standard SIL and the ISO 13849 Standard PL

Hardware Fault Tolerance (HFT)							Category				
IEC 61508							ISO 13849				
0	1	2	0	1	2	SFF	DC(1)	1	2	3	4
-	SIL 1	SIL 2	SIL 1	SIL 2	SIL 3	< 60%	None				
SIL 1	SIL 2	SIL 3	SIL 2	SIL 3	SIL 4	60% to < 90%	Low	c	c	d	
SIL 2	SIL 3	SIL 4	SIL 3	SIL 4	SIL 4	90% to < 99%	Medium		d	e	
	SIL 4	SIL 4	SIL 4	SIL 4	SIL 4	≤ 99%	High				e
Type B			Type A								

(1) Diagnostic coverage (DC).

The SIL and PL both define the safety levels of performance according to the standards used for evaluation (IEC61508 or ISO13849). These levels quantify diagnostic coverage by using different parameters. The SIL uses the safety failure fraction (SFF) as the parameter to quantify the ratio between the safe faults of the system and the total faults of the system. Similarly, the PL refers to the DC parameter as a measure of the effectiveness of the diagnostics implemented in the system. However, DC is the ratio of detected dangerous faults versus all dangerous faults. The SIL and PL are related through two main parameters which are inversely proportional: $MTTF_d$ (mean time to dangerous failure)—used in the ISO standards—and PFH (probability of dangerous failure per hour)—used in IEC standards for high demand systems. By using this relationship, using both levels (PL and SIL) is possible when assessing a system for safety.

Table 2-2. PL and SIL Relationship Through PFH and $MTTF_d$ Parameters

PL (ISO 13849)	PFH Target Values [PFH = 1/$MTTF_d$]	SIL (IEC 61508, IEC 62061)
a	≥ 10^{-5} to < 10^{-4}	No correspondence
b	≥ 3 x 10^{-6} to <10^{-5}	1
c	≥ 10^{-6} to < 3 x 10^{-6}	1
d	≥ 10^{-7} to < 10^{-6}	2
e	≥ 10^{-8} to < 10^{-7}	3

Although the PL or SIL applies to the complete safety function typically formed by sensors, data processing, and actuators, each one of these function subsystems must meet a minimum PL or SIL. For each subsystem, a different standard exists to describe how the safety level is met. As an example, for motor drive and actuator implementations, the specific subsystem standard (IEC 61800-5-2) is used to specify the safety requirements. The IEC 61800-5-2 standard defines the requirements for the design and development of variable speed drives by describing the designated safety subfunctions, for example as safe torque off (STO), safe limited speed (SLS), safe brake control (SBC), and so forth. Within the standard, IEC 61800-5-2 refers to the ISO 13849-1 standard and describes the requirements necessary for each subfunction to achieve a minimum PL. Moreover, aspects such as independence between systems, redundancy, and the processing time are discussed on both previously-mentioned standards and must be considered when implementing the system. Therefore, prior to starting the system implementation, understanding the key relationships between the safety requirements is important for each application, for each safety subfunctions that must be implemented, and for each level of required risk reduction (SIL or PL) for each subfunction. For this specific use-case (as summarized in Table 1 of the ISO 3691-4 standard), a minimum PLd safety level is required. Focusing on the motor drive subsystem, the safety subfunctions defined in the IEC 61800-5-2 standard are used to meet the PLd requirements.

Table 2-3 summarizes the main relationships between the three standards.

Table 2-3. Safety Requirements per the ISO 3691-4 Standard

Safety Function per EN ISO 3691-4	Minimum Required PL per EN ISO 3691-4	Related Safety Subfunction per IEC 61800-5-2
Breaking System	d/b	SBC, SS1, STO
Speed control	d/c	SLS, SOS, STO

Copyright © 2026 Texas Instruments Incorporated

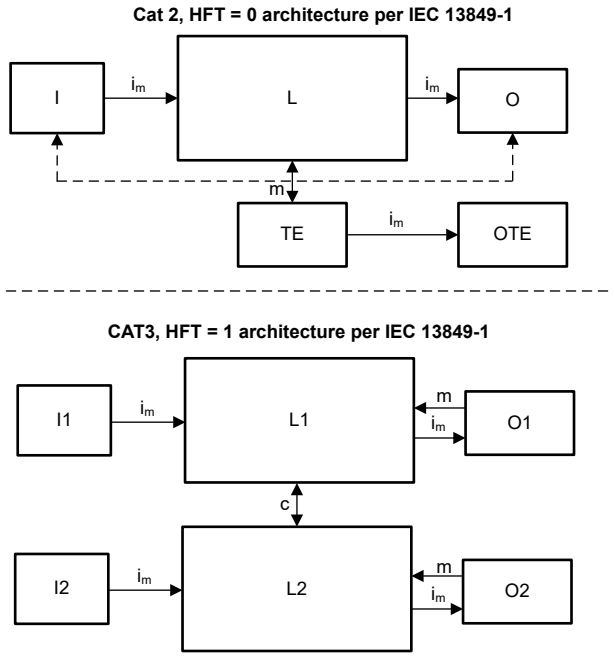
Table 2-3. Safety Requirements per the ISO 3691-4 Standard (continued)

Safety Function per EN ISO 3691-4	Minimum Required PL per EN ISO 3691-4	Related Safety Subfunction per IEC 61800-5-2
Automatic Battery Charging	b	NR(1)
Load Handling	b	NR(1)
Steering	–	SLS
Stability	c	NR(1)
Emergency Stop Function	d	STO
Personnel Detection Systems	d/c	SLS, SOS, SS1, STO SDI
Automatic, Manual, and Maintenance Modes	d/c	SLS, SOS, STO
Warning Systems	a	NR(1)
Access Into the Confined Zone	d	SOS, STO

(1) NR: Implementation not related with the robot motor drive

2.2 System Architecture Selection

The ISO 13849-1 standard defines the relationship between the required diagnostic coverage and the architectural category which correlates to the amount of redundancy of the system. As previously stated, the ISO 3691-4 standard requires a minimum PLd safety level that can be achieved by using either a CAT2, HFT = 0 architecture or a CAT3, HFT=1 architecture, as defined in the IEC 13849-1 standard. This choice impacts the amount of redundancy and diagnostic coverage required in the system, as shown in Figure 2-2.



I = input, L = logic, O = Output, TE = Test Equipment, OTE = Output Test Equipment, m = monitoring, c = compare

Figure 2-2. Designated Architectures for Categories 2 and 3 per IEC 13849-1

As shown in Table 2-1, CAT2, HFT = 0 system implementations require less redundancy in exchange for a higher diagnostic coverage of 90% (DCavg = 90%). To meet the required DCavg, the diagnostic functions must be executed within a defined timing interval to reach the safe state on time. Contrarily, CAT3 architectures require dual-channel designs in exchange for lower diagnostic coverage and more relaxed timing constraints. In the case of AMRs, one of the key constraining factors is the overall size and weight of the system. Therefore, the more compact CAT2 architectures are appropriate for these types of applications. However, in cases where a CAT3 implementation is preferred, TI also provides the *Industrial Functional Safety for C2000™ Real-Time Microcontrollers* product overview and guidance on how to implement such systems.

Copyright © 2026 Texas Instruments Incorporated

2.3 Device Selection Based on Process Safety Time

Once the initial safety requirements are known, as well as the architecture to implement, the system integrator can select the appropriate devices. As a common starting point, the MCU or processor is typically selected prior to the rest of the devices, and aspects such as safety features or processing capabilities are the key result during this selection process. Within the safety standard, ISO 13849-1 (section 1) describes different timing requirements to make sure that the system is able to detect a fault and reach a safe state within a defined process safety time

Figure 2-3 shows the typical nomenclature used to defined the time intervals.

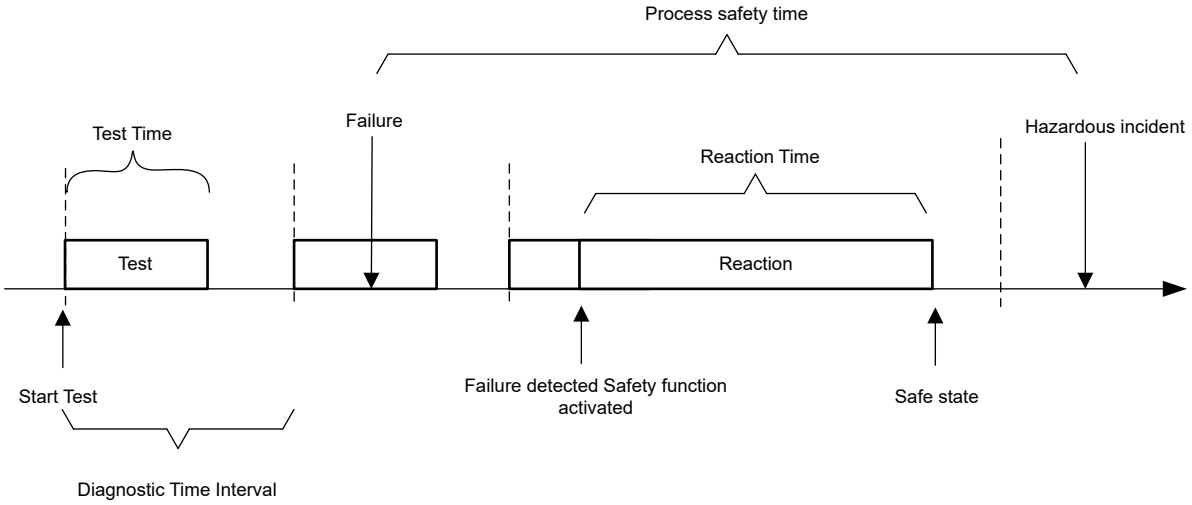


Figure 2-3. Functional Safety Related Timing Considerations

The diagnostic time interval comprises the amount of time available to execute the diagnostic functions and the process the inputs received from these diagnostics. Given a defined diagnostic time interval, higher diagnostic coverage implies a more powerful processor. Due to the unpredictability of hazards, the diagnostics in AMRs must run continuously, 24 hours a day and seven days a week. By running continuously, a fault can be instantly detected, and the device can be brought to the safe state within the required process safety time. Moreover, the ISO 3691-4 standard further restricts this testing time interval by defining the maximum speed of the AMR depending on the distance to an object. By considering the worst-case scenario, the designer must calculate the process safety time necessary to avoid the risk and make sure that the safe state is reached prior to a collision of the object. The safety process time is estimated to be less than 415ms as determined by the maximum speeds and distances to objects in Table A.1 of the ISO 3691-4 standard. The diagnostic functions of the MCU must be completed within this time, and if a fault is detected, the safe state must be reached within this time. To allow enough leeway for the reaction time, the diagnostic time interval must be less than 10% of the overall process safety time. This means a maximum of 41.5ms is allowed for a full diagnostic sweep during operation of the system function. Due to these timing constraints, and that the architecture selection is CAT2, Having a powerful real-time MCU with integrated safety mechanisms that can both fulfill the motor control requirements and the safety requirements is important. The TI C2000™ real-time microcontrollers and PMIC devices are an excellent choice for meeting both the process safety time and diagnostic coverage that achieves PLd.

3 Implementing Mobile Robot Motor Drive Safety Requirements

Once the designer understands the safety requirements and architecture category of the system, the designer must select the remaining devices and implement the complete motor drive to meet the safety requirements.

Copyright © 2026 Texas Instruments Incorporated

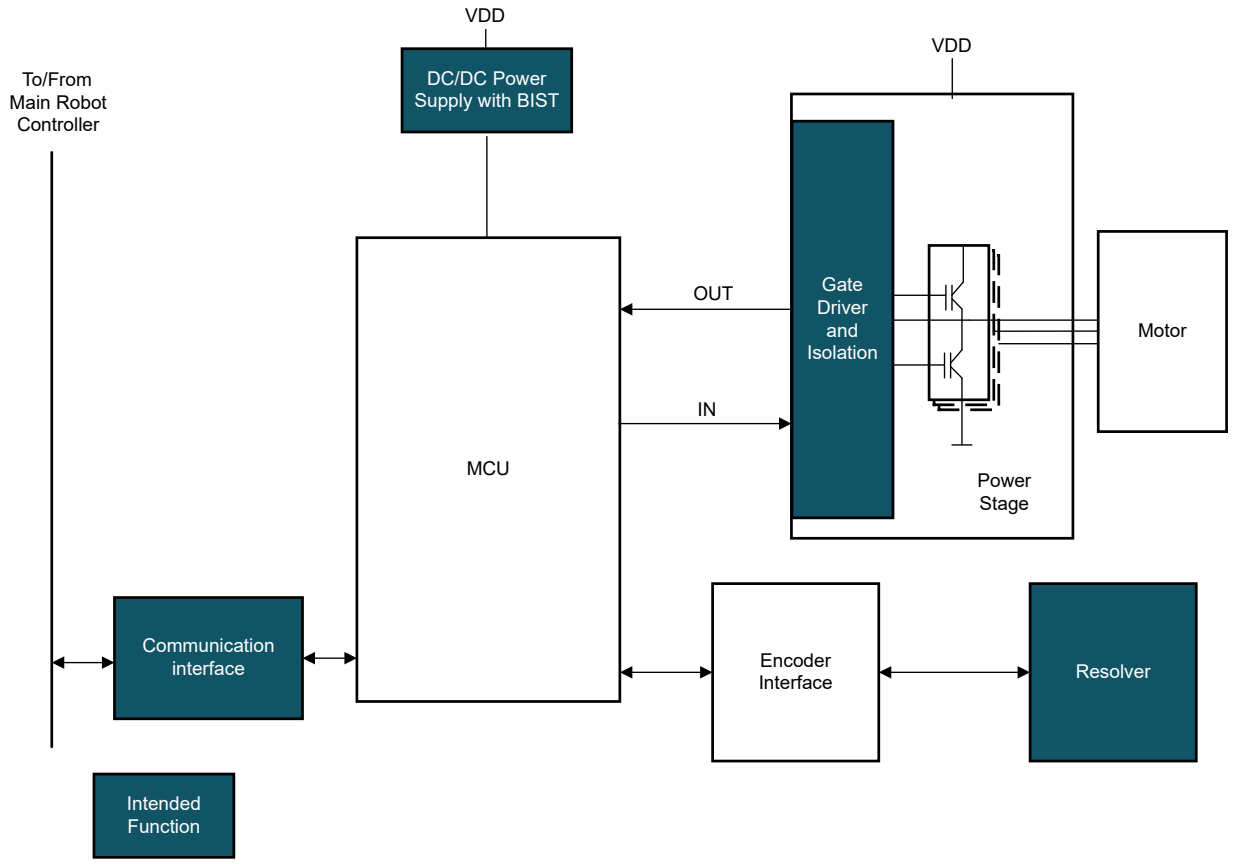


Figure 3-1. Motor Drive System Block Diagram

Figure 3-1 shows that a motor drive system is typically formed by an MCU, a power stage (which can integrate the analog front end), the encoder, and the power supply. In the IEC 61508 standard, the required safe failure fraction (SFF) depends on the type of integrated circuit (IC). The subsystem can be Type A or Type B. According to the IEC 61508 standard, Type A subsystems have well-defined failure modes, where the behavior under fault conditions is determined and there is enough failure data to claim that the failure rates are met.

Conversely, Type B subsystems are more complex subsystems, where the failure modes are not fully defined. The fault conditions cannot be completely determined, and there is not enough data to support the claim that the failure rates are met.

The complete definition of both types of subsystems is found in section 7.4.4 of the IEC61508 standard. Moreover, the CNB-M-11.059 amendment of the IEC61508 standard states that diagnostic subsystems must only achieve a safety level below the required system SIL level to achieve the minimum safety level. Although this amendment is specified as part of the IEC61508 standard, using the IEC61508 standard in combination with the ISO 13849-2 machinery standard when analyzing diagnostic subsystems is considered a *state-of-art* practice when analyzing diagnostic subsystem for safety circuits.

Therefore, for this specific use-case, since a SIL 2 system is required, modules related to diagnostics must fulfill at least SIL 1 and a minimum SFF = 0% (Type A) to meet the SIL 2 system requirements. However, safety functions not related to diagnostics must still fulfill SIL 2 requirements and have a minimum SFF of 60%. By understanding which subsystems are Type A and Type B, the designer can easily select the individual device based on the features of the device, for example, the availability of safety documentation or diagnostic features.

Since MCUs and PMICs are complex devices, these devices are considered Type B devices. As MCUs and PMICs are part of the implemented safety function, MCUs and PMICs require a diagnostic coverage of 90%, see Table 3-1 for details. Meaning, each one of the subsystems used by the device for a safety function must be monitored with diagnostic functions to achieve the required coverage of 60%.

Copyright © 2026 Texas Instruments Incorporated

The first step in this process is to select the device functions that must be used to implement the safety function and define the diagnostic coverage that is required for each function.

The second step, once the diagnostic coverage is defined, is to create the safety documentation. The safety documentation demonstrates that the correct diagnostic coverage is available for each of the intended safety functions and safety diagnostic functions. The safety documentation also details if external diagnostic devices are required.

TI's latest C2000™ real-time microcontrollers are designed considering functional safety. Designers can simplify and accelerate the safety assessment process by taking advantage of the safety features and safety documents provided by TI. Many of the key safety features of the C2000™ real-time microcontrollers and devices are documented in the *Industrial Functional Safety for C2000™ Real-Time Microcontrollers* product overview.

As previously mentioned, the device functions and failure modes must also be well defined for Type A devices. Therefore, having safety documentation available for less complex devices is also important. For these type of devices, the results of the safety documentation from TI are beneficial for justifying the type of device and the minimum SFF that is required.

TI's multichannel IC (PMIC) devices help greatly reduce the overall BOM and the size of the motor control module while meeting the safety requirements. These ICs help simplify the design with integrated functions such as built-in low dropout regulators (LDOs), supervisors, built-in self-tests (BISTs), watchdog timers, and DC/DC regulators, while providing the diagnostic functions necessary to supervise both the MCU and the required power rails.

According to the ISO 13849 standard (section 6.1), the diagnostic function and safety function cannot be within the same IC to achieve diagnostic coverage of 60% since the safety functions cannot be periodically performed. The ISO 13849 standard considers that a single fault in the IC results in the complete loss of the functions of this IC. For a CAT2 device, that function loss must be detected by the diagnostic features. Therefore, to prevent a loss of function from resulting in a loss of diagnostic function, using a voltage supervision and watchdog Q&A function within the same IC is not permissible. This example uses external voltage supervisors and the internal question and answer (Q&A) watchdog of the PMIC device. The power management folder of *Supervisor and Reset ICs* details TI's extensive portfolio of voltage supervisors that support functional safety.

Figure 3-2 shows a highly simplified example of some of the diagnostic features that can be used to achieve SIL 2.

Copyright © 2026 Texas Instruments Incorporated

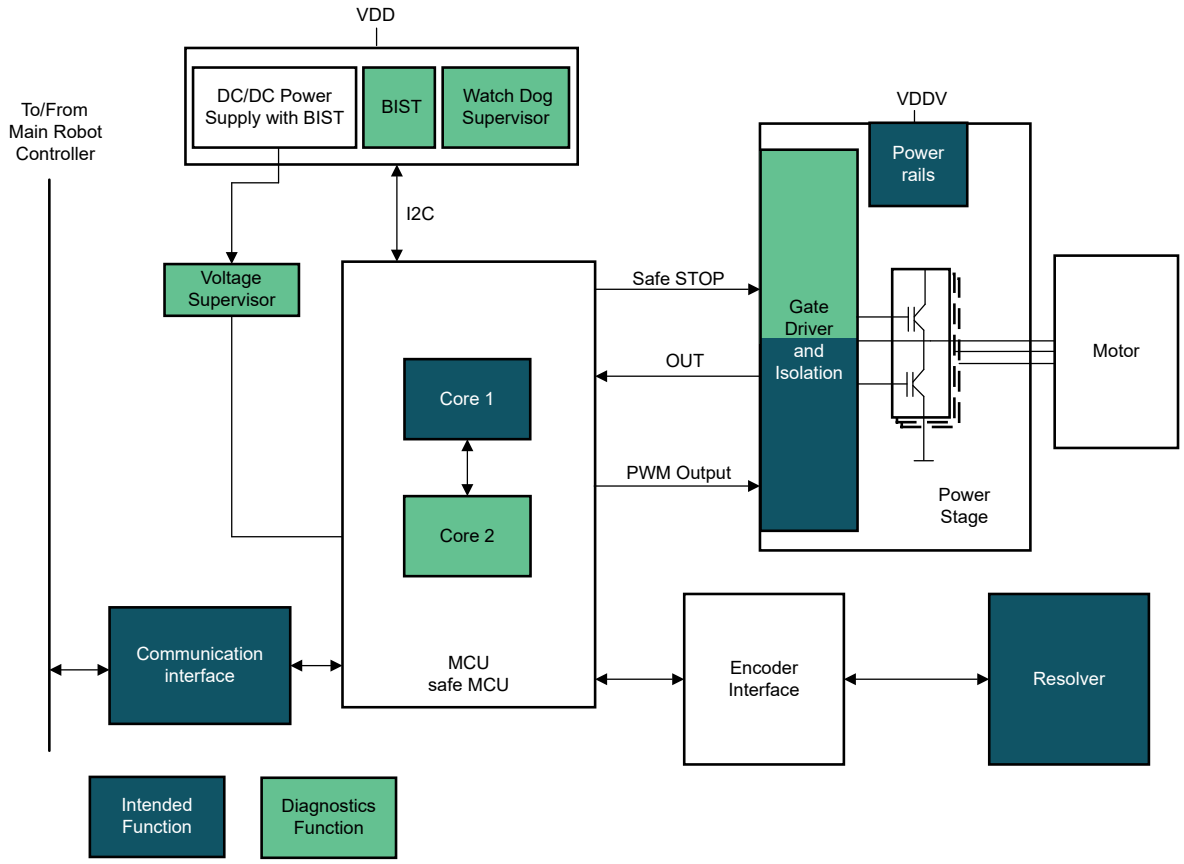


Figure 3-2. Simplified Motor Drive System Including Safety Features

Once the safety functions are defined at a system level, an analysis at a block level is necessary to demonstrate that each one of the subsystems meets the safety requirements. In this use-case, the safety subsystems are split between the safety and diagnostic functions. The diagnostic functions are used to make sure that the safety functions meet the minimum SFF/DV_{avg} defined per subsystem type.

Table 3-1 summarizes the details.

Table 3-1. Example of Diagnostic Coverage Required per Device Type

Parameter	Type A	Type A	Type B	Type B	N/A	N/A
Safety function (S), Diagnostic function (D)	S	D	S	D	S	D
SIL	2	1	2	1	PLd	PLc
HFT	0	0	0	0	CAT2	CAT2
Minimum required SFF | DC	60%	0%	90%	60%	90%	60%

By properly defining and demonstrating that each of the intended functions achieves the required minimum diagnostic coverage, this action demonstrates that the system is able to achieve the required PL and SIL and can be safety certified.

4 Conclusion

This document showed the procedures to follow to achieve a safety-certified system. A clear product design and development strategy further reduces the time to market. Moreover, by properly understanding the necessary requirements to meet the appropriate safety level, a designer can reduce the total BOM by maximizing the use of the internal safety features of devices. An example of this type of reduction is using the second core of the C2000™ microprocessor device as the test equipment (TE) of the CAT2 system, which has been documented and certified by TÜV SÜD with the report number TF103287T. This core is otherwise typically used as a

Copyright © 2026 Texas Instruments Incorporated

second processor or as logic circuits. TI has the expertise on functional safety and can be leveraged to provide designers with a great advantage during product development phase.

TI offers an extensive portfolio of devices and resources focused for functional safety. TI Functional Safety provides information on collateral and products to help designers select devices and increase their safety-related knowledge.

The complete safety concept report is available with an NDA and can be requested through the TI sales team. The overall concept greatly simplifies the safety certification process of mobile robots used for warehouse operations and can be used for any type of safety processor subsystem which requires HFT = 0, PLd. For more details on the process, see the *Industrial Functional Safety for C2000™ Real-Time Microcontrollers* product overview.

Copyright © 2026 Texas Instruments Incorporated

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATASHEETS), 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 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, TI’s General Quality Guidelines, 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. Unless TI explicitly designates a product as custom or customer-specified, TI products are standard, catalog, general purpose devices.

TI objects to and rejects any additional or different terms you may propose.

Copyright © 2026, Texas Instruments Incorporated

Last updated 10/2025