Technical White Paper

Simplifying Robotics Motor Drive Safety Assessments

Ester Vicario, Kristen Mogensen *Systems Engineering and Marketing*

ABSTRACT

With the increasing use of robotic systems in industrial environments, industry safety requirements and national and international safety regulations need to continually be updated to make sure that humans have a secure environment when working in close proximity to machines. Functional safety assessments are required to demonstrate that devices meet safety requirements and can responsibly be 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 to select the right devices, meeting the safety requirements and reducing the overall bill of materials (BOM) size and cost. By describing the steps to follow to meet the safety requirements, this white paper shows how to speed up safety assessments and achieve lower design cost.

Table of Contents

List of Figures

List of Tables

Trademarks

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 need to be regulated to provide personal safety.

To show that robots meet the 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 and regulated safety requirements. Making sure that the product is safety-compliant is usually a long and complex procedure, increasing the overall design cost, robot size, and time-to market.

This white paper offers a simplified explanation of the process needed to follow to safety assess a motor drive. The main standards used, the types of architecture, and selection of devices is described, helping to accelerate the system design process.

For this specific document, a new safety concept of a single-channel motor drive design is used as baseline. This safety concept provides a block level concept of how to achieve Category 2, Performance Level 2 (Cat 2, PLd) per ISO 13849 or Safety Integrity Level 2 and Hardware Fault Tolerance = 0 (SIL 2, HFT = 0) per IEC 61508 standard and it is intended to help the reader meet the safety requirements in a cost-effective manner. As an example, this white paper refers to the standard ISO 3691-4 which focuses on industrial trucks such as autonomous mobile robots (AMRs); however, the same procedure can be used with any other machine that requires Cat 2, PLd.

This concept uses TI's latest high-performance motor control C2000™ real-time controllers and PMICs which both include on-chip safety functionality. By using this product family, design concepts, and additional TI available safety resources, designs can achieve a lower BOM implementation of the overall system and reduce the time to market.

2 Understanding Cat 2, PLd Safety Requirements

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

2.1 Safety Requirements per ISO 3691-4

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; therefore, it is the responsibility of the designer to decide where the safety functions are placed within the industrial truck modules as Figure 2-1 shows.

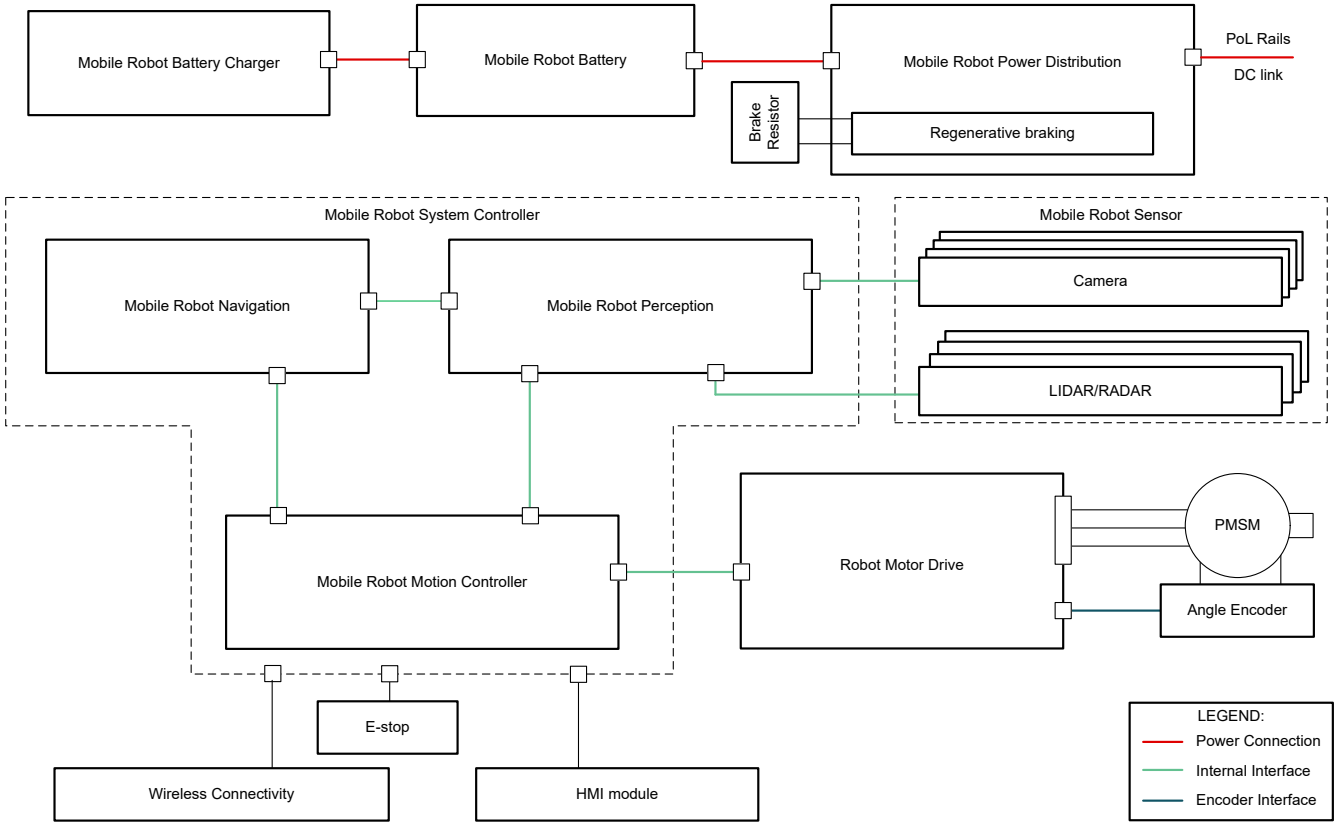


Figure 2-1. Simplified Mobile Robot Block Diagram

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

Similarly to PL, several standards measure the system safety performance by using the safety integrity level (SIL) parameter defined in IEC 61508. The relation between PL and SIL levels is found in Table 2-1.

Table 2-1. IEC 61508 and ISO 13849 SIL and PL Relation

Hardware Fault Tolerance (HFT)								Category			
IEC 61508							ISO 13849				
0	1	2	0	1	2	SFF	DC	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								

Both SIL and PL are discrete levels for safety performance and these levels quantify the diagnostic capabilities by using different parameters. SIL uses Safety Failure Fraction (SFF) as a parameter to quantify the ratio between safe faults and total faults of the system. Similarly, PL refers to the DC parameter as a measure of effectiveness of the diagnostics implemented in the system. However, both SIL and PL are related through two main parameters which are inversely proportional: MTTF (Mean Time to Dangerous Failure) – used in the ISO standards – and PFH (Probability of dangerous failure per hour) – used in IEC standards. By using this relation, it is possible to use both PL and SIL levels when assessing a system for safety.

Table 2-2. PL and SIL Relation Through PFH and MTTF Parameters

PL (ISO 13849)	PFH target values [PFH = 1/MTTF]	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 PL or SIL applies to the complete safety function, typically formed by sensors, data processing and actuators, each one of those function subsystems need to meet a minimum PL or SIL. Per subsystem, different standards exist to describe how the safety level is met. As an example, for motor drives and actuators implementations, the subsystem specific standard, IEC 61800-5-2 is used to specify the safety requirements.

IEC 61800-5-2 defines the requirements for the design and development of motor drives by describing designated safety subfunctions such 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 ISO 13849-1 and describes the requirements needed 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, it is important to understand the key relationship between the safety requirements per application, the safety subfunctions needing to be implemented, and the level of risk reduction (SIL or PL) required per subfunction.

For this specific case, as summarized in Table 1 of ISO 3691-4, a minimum PLd level is required. Focusing on the motor drive subsystem, the safety subfunctions defined in IEC 61800-5-2 are used so as to meet the PLd requirements. Table 2-3 summarizes the main relationship between those three standards.

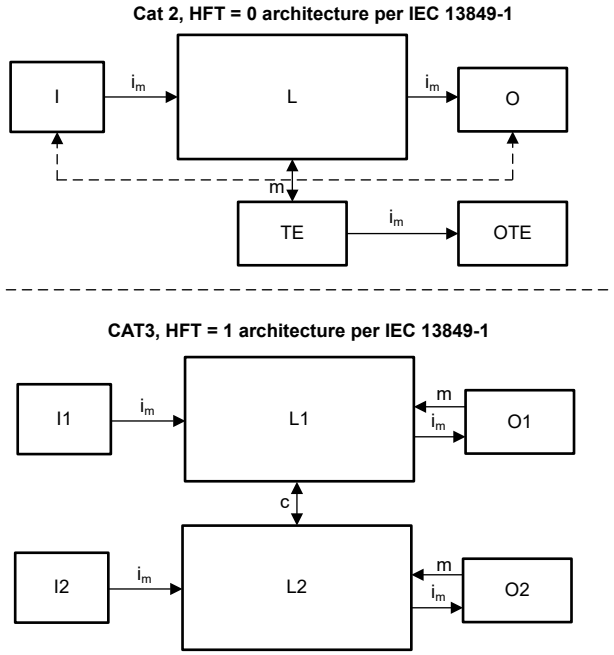
Table 2-3. Safety Requirements per ISO 3691-4

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
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 either using Category 2, HFT = 0 or Category 3, HFT=1 architecture as defined in the IEC 13849-1 standard. This choice impacts the amount of redundancy and diagnostics 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 Cat 2, HFT = 0, system implementations require less redundancy in exchange of a higher diagnostics coverage of 90% (DCavg = 90%). To meet the required DCavg, the diagnostics functions need to be executed within a defined timing interval to make sure that the safe state is reached on time. Contrarily, Category 3 architectures require dual-channel designs in exchange of lower diagnostic coverage and more relaxed timing constrains.

In the case of AMRs, one of the key constraining factors is the overall size and weight of the system. Therefore, more compact Cat 2 architectures are appropriate for these types of applications. However, in cases where a Cat 3 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.

2.3 Device Selection Based on Process Safety Time

Once the initial safety requirements are known, as well as the architecture that is to be implemented, it is time to select the devices. As a common starting point, the MCU or processor is selected prior the rest of the devices and aspects such as safety features or processing capabilities are a key result during the selection process.

Within the safety standard, ISO 13849-1 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.

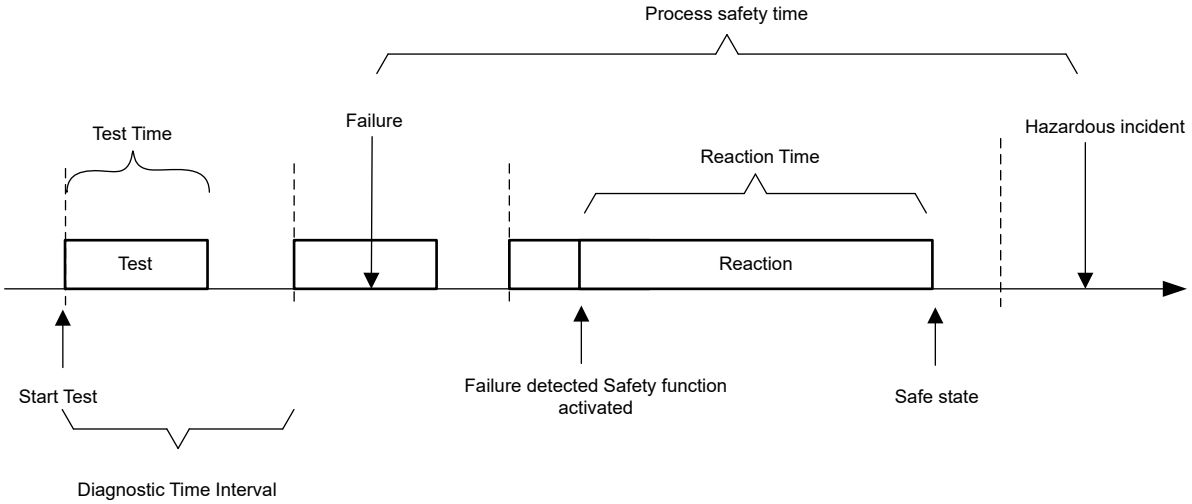


Figure 2-3. Functional Safety Related Timing Considerations

The diagnostic time interval comprises the amount of time available to execute the diagnostic functions and process the inputs received from them. Given a defined diagnostic time interval, higher diagnostic coverage implies a more powerful processor is required.

Due to the unpredictability of the hazards, in AMRs the diagnostics need to be run continuously. By running continuously, a fault can be instantaneously detected and the device can be brought to the safe state within the required process safety time.

Moreover, ISO 3691-4 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 needed to avoid the risk and make sure that the safety state is reached prior to collision of the object.

Based on the maximum speeds and distances to objects stated in ISO 3691-4 table A.1, it is estimated that the safety process time needs to be less than 415 ms. Within this timing, the diagnostics functions of the MCU must be completed and if a fault is detected, the safe state must be reached. To allow enough leeway for the reaction time, the diagnostics time interval must be less than 10% of the overall process safety time. This means a maximum of 41.5 ms is allowed for a full diagnostic sweep during operation of the system function.

Due to these timing constraints and the Cat 2 architecture selection, it is important to have a powerful real-time MCU with integrated safety mechanisms that can both fulfill the motor control and the safety requirements. TI C2000 real-time controllers and PMIC devices are an excellent choice to make sure that both the process safety time and the diagnostic coverage can be met, achieving PLd.

3 Implementing Mobile Robot Motor Drive Safety Requirements

Once the safety requirements and architecture category of the system are understood, the designer must select the remaining devices and implement the complete motor drive to make sure that the safety requirements are met.

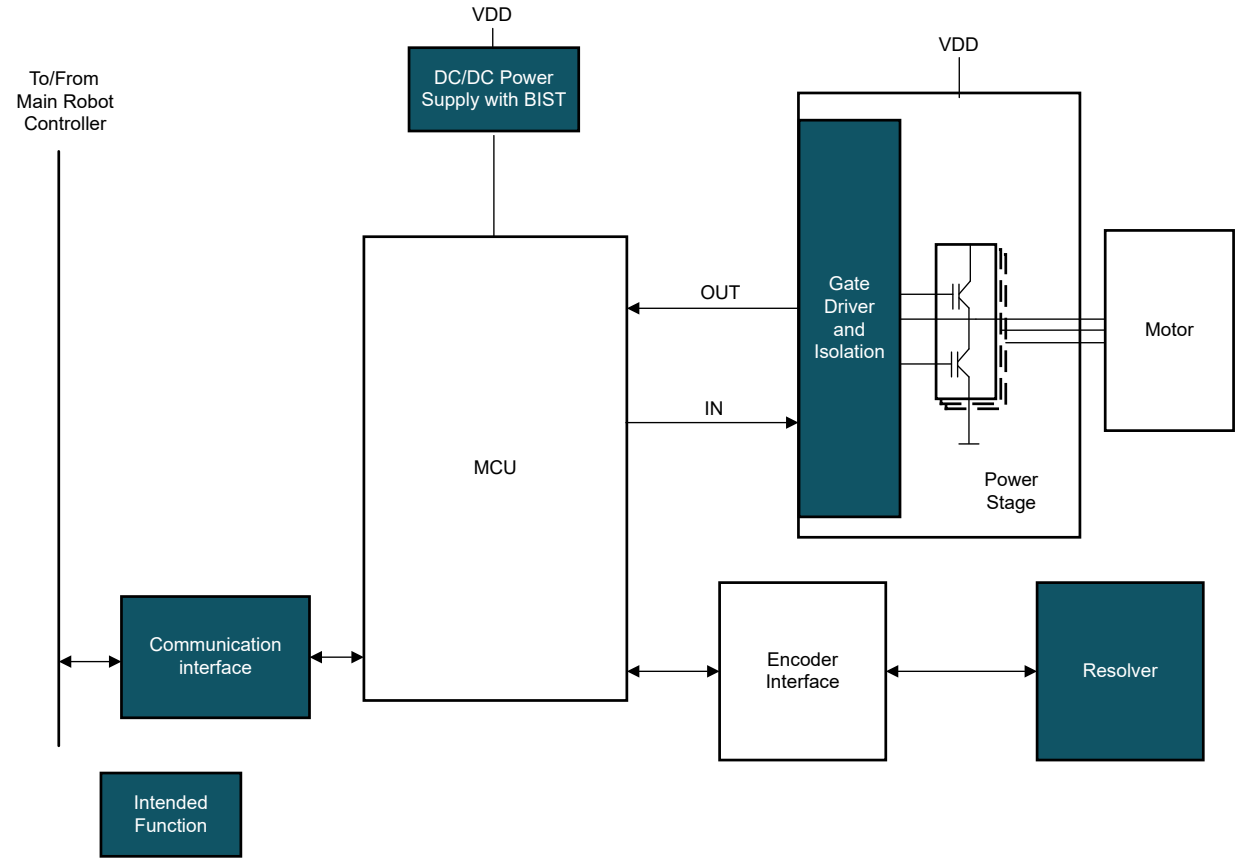


Figure 3-1. Motor Drive System Block Diagram

As Figure 3-1 shows, 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, the required safe failure fraction (SFF) depends on the type of device which can be Type A or Type B. Per IEC 61508, type A subsystems have the failure modes well defined, 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 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 diagnostics subsystems only need to achieve a safety level below the required system SIL level to achieve the minimum safety level. Although this amendment is part of the IEC61508 standard, it is state-of-art to use it with the ISO 13849-2 machinery standard when analyzing diagnostic subsystems.

Therefore, for this specific case, because an SIL 2 system is required, diagnostic related modules must fulfill at least SIL 1 and a minimum SFF = 0% to meet the SIL 2 system requirements. However; safety and non-diagnostic functions still must fulfill SIL 2 and have a minimum SFF of 60%.

By understanding which sub-systems are Type A and Type B, it is possible to easily select the device itself based on features such as available safety documentation or diagnostic features.

Because the MCU is a type B device and is used to implement safety functions, the MCU needs a minimum SFF = 60%. This means that each one of the subsystems used by the device must be monitored with diagnostic functions to achieve the required 60% coverage.

As a first step it is needed to select which device functions need to be used and the diagnostic coverage required for each. Once defined, safety documentation is key to demonstrate if there are enough diagnostics available for each one of the intended functions or if external diagnostic devices are needed.

TI's latest C2000™ real-time controllers are designed considering functional safety. By taking advantage of the safety features and documentation provided, it is possible to simplify and accelerate the safety assessment. Some of the key C2000™ safety features and devices are documented in the Industrial Functional Safety for C2000™ Real-Time Microcontrollers product overview.

Moreover, for less complex devices, it is also important to have safety documentation available. As previously mentioned, one of the conditions of a device type A to consider is that the device functionalities and failure modes must be well defined. For that, TI safety documentation results are beneficial to justify the type of device and therefore the minimum SFF required.

TI Multi-channel ICs (PMICs) devices greatly help reduce the overall BOM and size of the motor control module while making sure that the safety requirements are met. With integrated functionalities such as built-in LDOs, supervisors, BISTs, Watchdog, and DC/DC regulators, these ICs help simplify the design while providing the diagnostic functions needed to supervise both MCU and the required power rails.

Per ISO 13849 section 6.1, given that the safety functions cannot be periodically performed, the diagnostics and the safety functions cannot be within the same IC to achieve this 60% diagnostic coverage. ISO 13849 considers that a single fault in the IC results in the complete loss of function of this IC and for Category 2, that loss of function should be detected by the diagnostics features. Therefore, to make sure that the loss of function does not result in a loss of the diagnostics function, it is not possible to use voltage supervision and watchdog Q&A within the same IC. For this example, external voltage supervisors are used and the internal question and answer (Q&A) Watchdog of the PMIC device. The Supervisor and reset ICs power management folder details the extensive TI portfolio of voltage supervisors supporting functional safety.

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

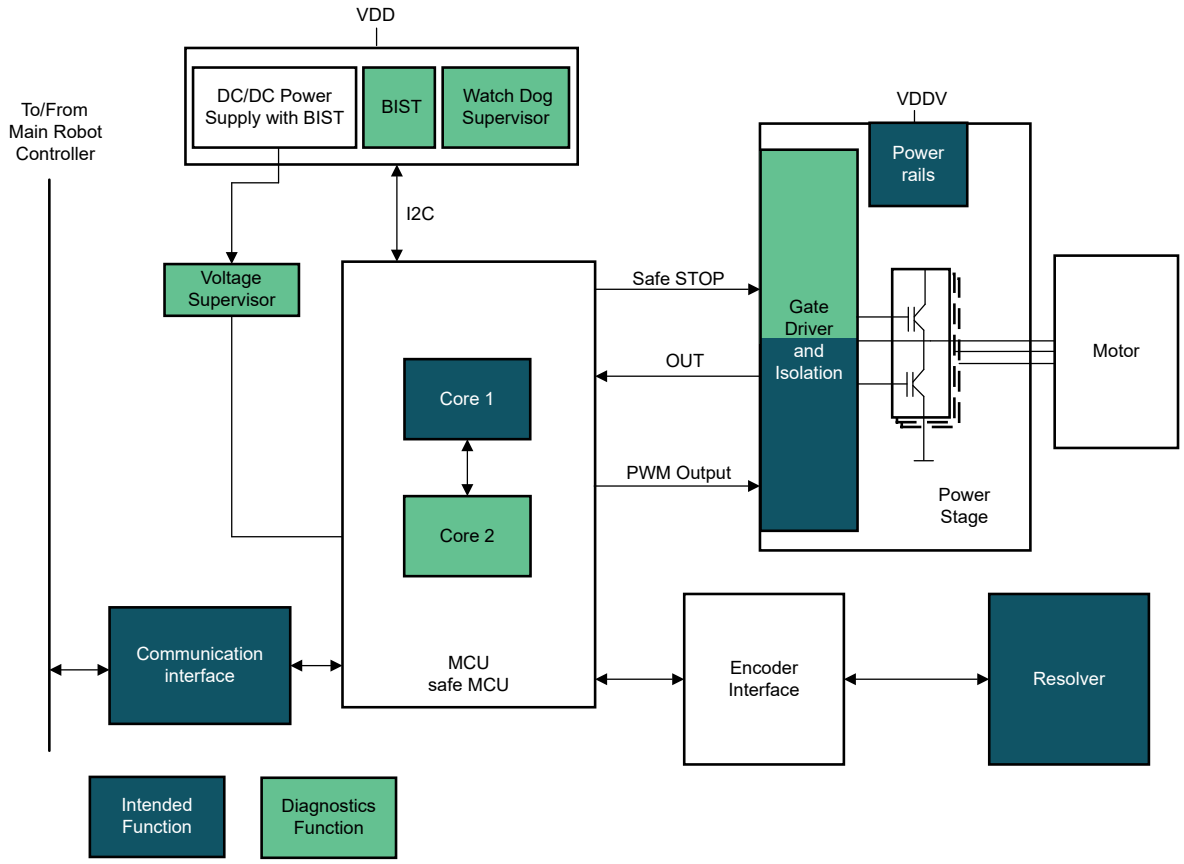


Figure 3-2. Simplified Motor Drive System Including Safety Features

Once the safety functions are defined on a system level, a block level analysis is needed to demonstrate that each one of the subsystems meets the needed safety requirements.

In this case, safety subsystems are split between safety and diagnostic functions. The diagnostic functions are used to make sure that the safety functions meet the minimum SFF 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
Safety function (S), Diagnostic function (D)	S	D	S	D
SIL	2	1	2	1
HFT	0	0	0	0
Minimum required SFF | DC	60%	0%	90%	60%

By properly defining and demonstrating that each of the intended functions achieves the required minimum diagnostic coverage, this 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 requirements needed to make sure that the safety level is met, it is possible to reduce the total BOM by maximizing the use of internal features of the devices. Therefore, the expertise TI has on functional safety can be leveraged to a great advantage during product development.

TI offers an extensive portfolio of functional safety focused devices and resources. The TI functional safety page provides information on collateral and products to choose the best devices and increase safety-related knowledge.

Request the complete safety concept for the examples in this document from the TI sales team. The overall concept greatly simplifies the safety certification process of mobile robots and can also be used for any type of motor drives which require HFT = 0, PLd.

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