EAI Endorsed Transactions
on Cloud Systems
Research Article EAI.EU

Integrating functional safety in motor drives with redundancy and diagnostic coverage

Aishwarya Bhatnagar[1,*], Vaibhavi Shanbhag[1] and Navaneeth Kumar N[1]

[1]Texas Instruments, Bangalore India

Abstract

Functional safety has become an integral part of motor drives. The main objective of functional safety is to bring the machine to a safe state quickly. A fail-safe system is fault-tolerant and inherently responds in a way that causes no or minimal harm to the machinery and operator. This paper presents the method of implementing safety functions defined in IEC-61800-5-2 like Safe torque off and Safe brake control. It also shows implementation of Safe power supply and Safe digital I/O to be integrated in the power converter for achieving high safety standards. These implementations not only add redundancy but also facilitate diagnostic coverage. The solutions proposed in this paper are validated under different test conditions.

Keywords: Functional Safety, Safe Torque Off, Safe Brake Control

Received on 01 August 2019, accepted on 07 October 2019, published on 05 November 2019

doi: 10.4108/_____

* Email:a-bhatnagar@ti.com

1. Introduction

Motor drives are an integral part of the industrial and automation processes. These operations often involve the control of machinery, for which safety is always a concern. Functional safety in drives not only ensures avoiding accidents but also reduces unplanned downtimes and enables smoother production workflows.

Safety integrated drives have to comply with certain standards. IEC 61800-5-2 is a product standard which specifies requirements and makes recommendations for the design and development, integration and validation of safety related power drive systems (PDS (SR)) in terms of their functional safety considerations. This standard defines different safety sub-functions with specified safety performance, to be implemented for preventing hazardous conditions. The two most basic and common sub- functions are Safe torque off (STO) and Safe brake control (SBC). STO is a stopping function that prevents torque-producing power from being provided to the motor. SBC provides safe output signal to control an external brake, thereby preventing suspended loads from falling. The term Safety integrity level (SIL) is used to specify a target level of risk reduction by a safety function. Drives offer STO and SBC from SIL1 till SIL3 depending upon the end application. Higher SIL levels for more stringent conditions can be realized by adding redundancy and diagnostic features to the hardware design. There can be a situation where the wire carrying signal from the emergency stop button is broken. In that case the motor will not stop rotating which can cause injury to the operator. This paper ensures diagnostic coverage to detect such faults and ensures a safer environment.

In case of suspended loads, stopping the motor is not enough. The motor has an electromagnetic brake that is locked when the grid voltage is cut off and released when voltage is applied to the coil. This brake should be latched when the motor comes to standstill to prevent the load from falling. Since the brake needs continuous power for normal operation, efficiency becomes crucial. The proposed solution uses solenoid current controller to reduce power

		continuously to generate a signal when temperature increases.
3.	Failure to generate 3.3V rails.	3.3V output of LDOs monitored by MCU continuously.
4.	Input wire break	Periodic checking for wire break condition on the input using digital isolator and an isolated switch.
5.	Digital input receiver stuck at high or low due to power or signal loss.	Check if IN1 and IN2 complimentary outputs.
6.	Output of High side smart switch short to ground	Output feedback from High side smart switch monitored by MCU.
7.	Output wire break	Digital Output is monitored by MCU through isolator.
8.	Overload or short circuit at high side smart switch output or under voltage detected at input of the switch	High side smart switch generates a fault signal to be fed back to MCU.

2.4 Implementation of Safe Power Supply

The proposed method implements a single fault tolerant safe power supply using two redundant channels to generate 3.3V power supply for the MCU as shown in Figure 8. The redundant channels are designed with different architectures to avoid common cause failures. The DC-DC converters are rated for 60V input as stated by IEC-61800-5-2. The independent voltage monitoring circuits ensure protection against under voltage and overvoltage.

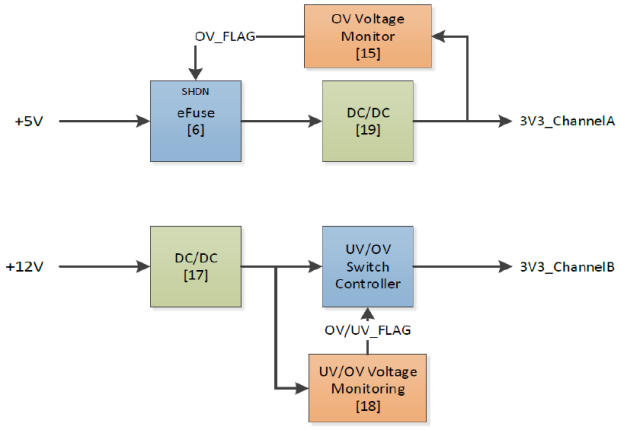

Figure 8. Block diagram of Safe power supply

3.3V Generation on Channel A

5V is down converted to 3.3V using a synchronous step down converter which is rated up to 65V at the input. The 3.3V output of the DC/DC is continuously monitored using voltage monitors for under voltage and overvoltage detection.

When the voltage monitoring circuit detects an overvoltage condition it generates a shutdown signal to switch off the e-Fuse at the input, thereby disconnecting the input supply. The e-Fuse employs protection features like reverse input polarity protection in case of a miswiring fault, under voltage lockout, overvoltage protection, overload and short circuit protection. The e-Fuse enables a controlled start-up thereby regulating the inrush current.

3.3V Generation on Channel B

12V is down converted to 3.3V using a synchronous step down converter which can handle a typical voltage of 66V. The 3.3V output of the converter is continuously monitored using a voltage monitor which generates a reset signal in case of under voltage or overvoltage detection. The reset signal is used to switch off the UV/OV switch which disconnects the DC/DC output from the 3.3V output.

The 3.3V_ChannelA and 3.3_ChannelB power supplies are multiplexed using a priority power MUX where the priority is given to the highest input voltage.

3. Conclusion

This proposal implements safety functions like STO and SBC. STO is implemented through two redundant channels which are controlled independently by switches. These switches provide diagnostic coverage to detect different fault conditions. This paper also highlights implementation of SBC using dual switches. It uses solenoid current controller to regulate peak and hold currents of the electromagnetic brake coil thereby improving efficiency. This paper also highlights a method of implementing safe power supply and safe digital I/Os incorporating extensive self-diagnostic and protection features with redundant channels to increase the fault tolerance of the fail-safe system.

References

[1] Texas Instruments, “ISO1211 - Isolated 24-V to 60-V Digital Input Receivers for Digital Input Modules (Rev. E) (SLLSEY7E),” ISO121x Datasheet, Aug 2018

[2] Texas Instruments, “TPS27S100 - 40-V, 80-mÙ Single-Channel High-Side Switch (Rev. A) (SLVSE42A),” TPS27S100x Datasheet, Mar 2018

[3] Texas Instruments, “TPS22919-5.5 V, 1.5 A, 90-mÙ Self-Protected Load Switch with Controlled Rise Time (Rev. B) (SLVSEN5B),” TPS22919 Datasheet, May 2019

[4] Texas Instruments, “ISO5852S- High-CMTI 2.5-A and 5-A Reinforced Isolated IGBT, MOSFET Gate Driver With Split Outputs and Active Protection Features (Rev. B) (SLLSEQ0B),” ISO5852S Datasheet, Jan 2017

[5] Texas Instruments, “ISO7142CC- 4242-VPK Small-Footprint and Low-Power Quad Channel Digital Isolator (Rev. B) (SLLSEF1B),” ISO7142CC Datasheet, Aug 2015
[6] Texas Instruments, “TPS2660 - 60-V, 2-A Industrial e-Fuse With Integrated Reverse Input Polarity Protection (Rev. E) (SLVSDG2E),” TPS2660 Datasheet, Jan 2017
[7] Texas Instruments, “DRV110 - Power saving solenoid controller with integrated supply regulation (Rev. A) (SLVSBA8A),” DRV110 Datasheet, Jan 2013
[8] Texas Instruments, “Redundant Dual-Channel Reference Design for Safe Torque Off in Variable Speed Drives (TIDUDS9),” Reference Design, Dec 2017
[9] Texas Instruments, “Smart Holding-Brake Control and Diagnostics Reference Design for Servo Drives and Robotics (TIDUE38),” Reference Design, May 2018
[10] Texas Instruments, “LMT86 - 2.2-V, SC70/TO-92/TO-92S, Analog Temperature Sensors (Rev. E) (SNIS169E),” LMT86 Datasheet, March 2013
[11] Texas Instruments, “TMP302 - Easy-to-Use, Low-Power, Low-Supply Temperature Switch in Micro package (Rev. E) (SBOS488E),” TMP302 Datasheet, Dec 2018
[12] Texas Instruments, “ISO776x -High-speed, robust EMC, reinforced six-channel digital isolators (Rev. E) (SLLSER1E),” ISO776x Datasheet, Aug 2017
[13] “IEC 61800-5-2”, International Standard, “Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional”
[14] Texas Instruments, “TPL7407L - 40-V 7-Channel Low Side Driver (Rev. D) (SLRS066D),” TPL7407L Datasheet, Mar 2016
[15] Texas Instruments, “TPS3703-Q1 - Overvoltage and Undervoltage Reset IC With Time Delay and Manual Reset (Rev. A) (SBVS344A),” TPS3703-Q1 Datasheet, Nov 2018
[16] Texas Instruments, “LMR36015 4.2-V to 60-V, 1.5-A ultra-small synchronous step-down converter (Rev. B) (SNVSB49B),” LMR36015 Datasheet, Feb 2019
[17] Texas Instruments, “TPS3702 High-Accuracy, Overvoltage and Under voltage Monitor (SBVS251),” TPS3702 Datasheet, Jan 2015
[18] Texas Instruments, “LMR36006 4.2-V to 60-V, 0.6A ultra-small synchronous step-down converter (Rev. B) (SNVSB48B)”, LMR36006 Datasheet, Feb 2019.
[19] Texas Instruments, “TMS570LS0432 16/32 Bit RISC Flash MCU, Arm Cortex-R4 (Rev. C) (SPNS186C),” TMS570LS0432 Datasheet, May 2018