Integrating functional safety in AC/servo drives with redundancy and diagnostic coverage

Aishwarya Bhatnagar[1], Vaibhavi Shanbhag[2], Navaneeth Kumar N[3]

***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. Fail-operational systems are fault-tolerant. They are expected to operate even when a failure has occurred. 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

I. INTRODUCTION

Motor drives are an integral part of the industrial and automation processes. These processes often involve the control of machinery, for which safety is always a concern. Functional safety in drives not only helps ensure 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 to 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 proposes methods to implement diagnostic coverage to detect such faults that could lead to 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 a 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 dissipation in the braking coil. Typical solutions for STO and SBC make use of optical isolators to safely isolate the electrical circuits. These optical isolators have poor thermal performance and suffer from ageing. The proposed solution uses digital isolators to attain better performance.

Signals from an emergency stop button or safety sensors like light curtains are some of the safe digital inputs to a drive. These digital inputs are further used to generate safe digital outputs which maintain the machinery in a safe state. A safe power supply is necessary for powering the safety microcontroller (MCU) and the safe digital input/output (I/O s). In this proposal, the power supply and digital I/Os are implemented with redundant channels using different architectures to ensure overcoming of common cause failures. Diagnostic features like over voltage protection, ±60V input tolerance, open cable detection, and continuous temperature monitoring haves been incorporated to help assist with safety certifications. This solution implements safe digital I/O and power supply meeting higher SIL by integrating self-diagnostic and monitoring features, hardware redundancy and fail safe outputs.

II. SYSTEM OVERVIEW

Figure 1 shows the block diagram representation of a safety integrated drive. The motor is connected to a three-phase inverter which converts the DC-link voltage to variable voltage and frequency AC output. An isolated gate driver controls the switching device of the inverter.

The STO signal can be triggered by the emergency switch, light curtain OR safety programmable logic controller (PLC). This signal prohibits supplying torque producing rotating magnetic field to the motor by disconnecting power to the gate drivers. Vertical or inclined axes can be a danger, in particular when disconnected from the grid voltage because of the risk of unintentional falling. Safe braking and holding system provides protection against such dangers. The holding brake is locked when voltage applied to the electromagnetic brake coil gets disconnected.

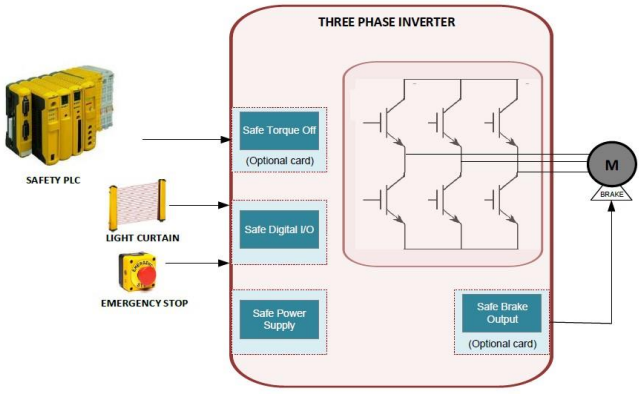

Figure1. Block diagram of a safety-integrated drive

The safe digital input is received from external sensors or actuators. Safe digital output interfaces are used to control external components like safety relays/solenoids. These digital I/Os require redundancy and robust protection against faults. The safe power supply generates redundant voltage rails to power field side circuits with protection against over voltage.

III. IMPLEMENTATION OF SAFE TORQUE OFF

The STO implementation in this proposal is based on 2oo2 (2 out of 2) architecture which corresponds to "OR" operation. There are two independent hardware channels both capable of disconnecting the gate driver power supply to ensure that the torque generating energy to the motor can be controlled when the STO inputs have been properly utilized in accordance with IEC/EN 61800-5-2. In case one unit fails the system is still functional. Figure 2 shows the block diagram of the STO function providing hardware fault tolerance of 1. STO1 and STO2 control the primary and secondary side power to the gate driver through load switch and high side switch respectively. It is a single fault tolerant system. As long as a logic 1 (+24-V DC) is present at both STO inputs, the motor is operable. If there is a logic 0 (0-V DC) at one or both of the STO inputs power to the gate driver is disconnected and the motor coasts down to zero.

The microcontroller can also be configured to disable the pulse width modulated (PWM) signal using either of the STO signals until a software RESET operation is performed.

The digital isolator protects the STO pins against reverse polarity and has an input tolerance of ±60 V. It also has the ability to draw constant current at its input irrespective of STO voltage being +24 V or 60 V. This current limit helps minimize power dissipated in the system. The smart high side switch eliminates the need of discrete field effect transistor (FET) and helps in system integration, controlled rise time and reduces inrush current. The MCU runs diagnostics on the STO function and monitors the STO signals as well as overall health of the safety circuit.

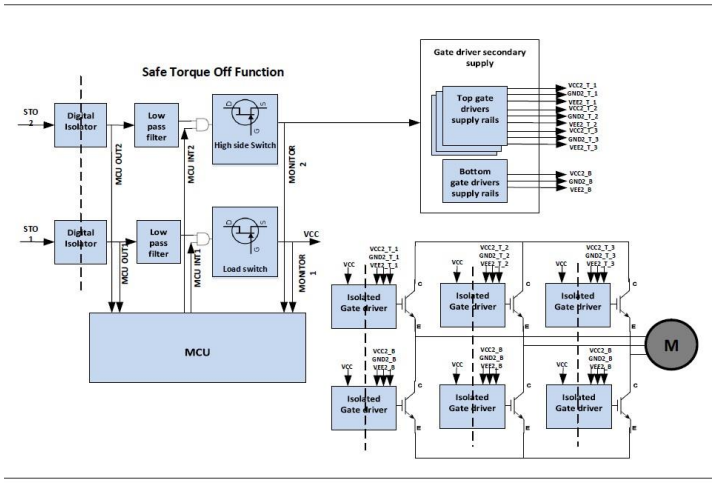

Figure2. Block diagram of STO function

A. Diagnostics to check if same signal is present on STO inputs

The safety PLC performs the monitoring by periodically checking the two stop paths for errors. The PLC performs these checks by sending pulses logic low pulses of 1-ms duration which are monitored by the MCU as MCU OUT1 and MCU OUT2. This helps in identifying stuck at high faults. This design utilizes an RC low-pass filter to reject the 1-ms pulses from the PLC so that the primary side gate driver supply and secondary side gate driver supply of the gate driver does not fall below the under voltage lockout (UVLO) threshold of the device during this time period.

B. Diagnostics to check working of high side switch and Load switch

The MCU interface periodically sends 200-µs pulses at the input of the switches (MCU INT1 and MCU INT2) to disable the switches intermittently and check whether the switches respond to these pulses. The outputs of the switches are connected to the general-purpose input/outputs (GPIOs) of the MCU as MONITOR1 and MONITOR2. This helps in identifying stuck high faults of the high side switches. The gate driver does not power off during these periodic pulses. A capacitor with an appropriate value is used at the input of gate drivers to hold the supply voltages.

C. Monitoring gate driver power supply

The ready (RDY) pin of the smart gate driver indicates the status of the UVLO for the primary and secondary sides of the gate driver. If either side of the device has an insufficient supply, the RDY pin output goes low, irrespective of inputs. By checking the status of the RDY pin, the signal path from STO1 and STO2 to primary and secondary gate driver supply can be monitored.

D. Detection of stuck-at faults

Stuck-at faults at the output of high side switch can be detected by using the diagnostic features of this device. When the switch is on, "short to ground" condition causes

overcurrent which triggers the fault condition. The value of current limit is adjustable and can be set externally.
The device can recognize “short to supply” condition under both on and off condition of the switch.

Table 1 highlights the diagnostic capabilities of the proposed design.

Table1. Diagnostic coverage on proposed safe torque off design

S No.	Fault condition	Diagnostic coverage
1.	±60V at the input of the digital isolator	The digital isolator is capable of handling ±60V.
2.	STO signals stuck at high faults from safety PLC and at output of digital isolators	The PLC periodically checks the two STO paths for errors by sending 1-ms pulse and monitoring MCU OUT1 and MCU OUT2
3.	Load malfunction	The MCU periodically sends 200-µs pulses to the switches for diagnostic purposes (MCU INT1 and MCU INT2) and monitors the output which is then fed back to the MCU.
		RDY signal from gate driver is fed back to the MCU

E. Functionality of STO1

As shown in Figure3 the STO1 signal is pulled low for a period of 15 milliseconds. The output voltage of load switch, primary gate driver supply voltage-VCC1 and ready signal from the gate driver are monitored.

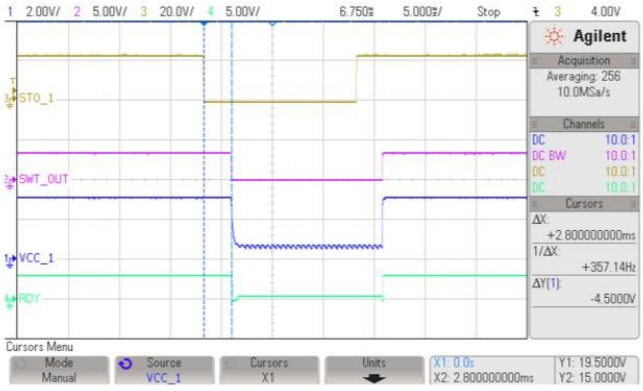

Figure3. Propagation of STO1 to primary supply of gate driver

The response time measured between the STO1 going low to the activation of the RDY signal is 2.7 ms. The response time is a function of the capacitance at the output of the load switch. As the VCC1 goes below the UVLO threshold, the RDY signal is activated.

F. Functionality of STO2

Similarly, in Figure4 the STO2 signal on the second channel is pulled low a period of 15 ms and output of TPS27S100, secondary gate driver secondary supply voltage VCC2, Ready pin of the gate driver. The response time measured between the STO2 signal going low to the activation of the RDY pin is 7.4 ms. As the VCC2 goes below the UVLO threshold, the RDY pin is activated.

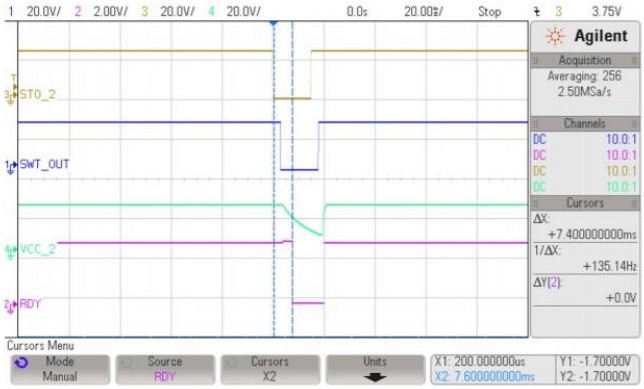

Figure4. Propagation of STO2 to secondary supply of gate driver

IV. IMPLEMENTATION OF SAFE BRAKE CONTROL

The SBC implementation in this proposal uses two independent paths that must deliver a consistent result to control the electromagnetic brake of the motor. It is based on 1oo2 (1 out of 2) architecture which corresponds to “AND” operation.
The brake coil is connected between the outputs of two independent switches which control the 24-V supply to the electromagnetic brake as shown in Figure5. The motor shaft is free to rotate if the 24-V supply voltage is applied to the brake coil and gets locked when supply voltage to the coil is removed. The switches receive digital control signals generated by MCU through the digital isolator.

The brake of the motor needs peak current only during actuation. However once the coil of the brake is actuated, it needs approximately 30% of its nominal current. Brake coil when operated with nominal current raises the temperature in the coil due to higher power dissipation. Traditional way of dealing with this problem uses PWM control of the switch to regulate peak and hold currents of the brake coil. This proposal uses solenoid current controller to reduce power dissipation.

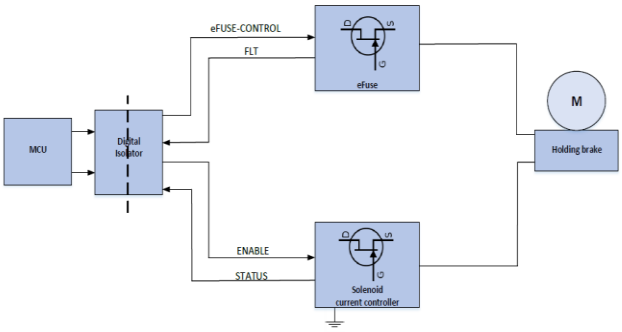

Figure5. Block diagram of *SBC*

A. Diagnostics on eFuse and solenoid current controller

The FLT signal from the eFuse and STATUS signal from the current controller provides diagnostic coverage under the different fault conditions. The fault signal asserts low under following conditions: under voltage, overvoltage, overload, reverse current, and thermal shutdown. This fault signal is fed to the MCU through the digital isolator. The isolator can also withstand and protect the loads from positive and negative supply voltages up to ±60 V. The STATUS pin of the current controller is activated if the under voltage lockout (UVLO) or thermal shutdown have triggered, or if the ENABLE pin is low.

B. Power saving by current controller

The brake of the motor needs peak current only during actuation. After initial ramping the brake coil current is kept at peak value by the solenoid current controller to ensure correct operation, after which it is reduced to a lower hold level in order to avoid thermal problems and reduce power dissipation. The peak current duration is set with an external capacitor. The current ramp peak and hold levels, as well as PWM frequency can be independently set with external resistors.

C. Current regulation by solenoid current controller

Figure6 shows the fixed hold currents of the brake coil for an input voltage of 19V and 28V. The STATUS signal which is an active low signal goes low as the brake voltage is applied. The brake hold current remains constant irrespective of the variations in the input supply voltages.

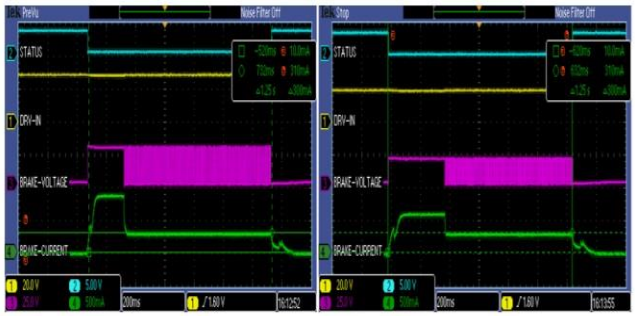

Figure6. Hold current of brake fixed to 300 mA at 19V and 28-V input voltage

V. IMPLEMENTATION OF SAFE DIGITAL I/O

The block diagram of safe digital I/O is shown is Figure 7.

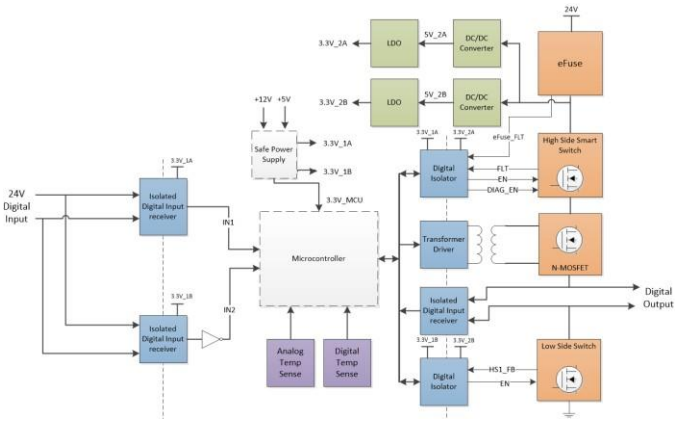

Figure7. Block diagram of safe digital I/O

A. Safe digital input receivers

This proposal implements hardware redundancy in safe digital I/O using two isolated digital input receivers compliant with IEC 61131-2. A ±60V input tolerance with reverse polarity protection helps ensure that the digital inputs are protected in case of faults like miswiring.

B. Safety microcontroller

The isolated digital inputs are fed to the high performance MCU for diagnostics. The MCU has integrated safety in hardware to detect potential failure modes with a quick response time. The safety architecture includes dual central processing units (CPUs) in lockstep, CPU and memory built- in self-test (BIST) logic, parity on peripheral memories, and loopback capability on peripheral I/Os. Cross monitoring of digital input from first channel and inverted input from second redundant channel is implemented by the MCU.

C. Safe digital outputs

The isolated outputs of the MCU are maintained at a low output fail safe state by the digital isolator when the input signals to the isolator or the power is lost. The digital output is generated through two redundant high side switches and a low side switch. The two different architectures with high side smart switch and a switch controlled by a transformer driver enables overcoming common cause failures. The digital output is high only when all the switches are turned on. The switches have integrated diagnostics features to protect against loss of ground, overload and short circuit conditions. The digital output is fed back to the MCU for continuous monitoring and detecting faults like output wire break.

D. Safe power supply for digital I/O and temperature monitoring

In this proposal, 3.3V is generated from an external 24V supply through two redundant channels to avoid common cause failures. The eFuse at 24V supply input has a ±60V input tolerance with protection against reverse polarity, overvoltage and under voltage faults. In case of a fault, the eFuse generates a fault signal which is used to bring the system to a safe state. The printed circuit board (PCB) temperature is continuously monitored by analog temperature

sensor and digital temperature sensor. If the temperature increases beyond 85˚C, a signal is generated by digital temperature sensor which brings the system to a safe state. The output of the analog temperature sensor is continuously monitored by the MCU to protect against high PCB temperature to validate if the PCB is running at rated conditions.

When a fault condition is detected by the MCU, the high side and low side switches are disabled bringing the system to a safe state. The diagnosis of faults is discussed in detail in Table 2.

Table2. Diagnostic coverage of proposed method of safe digital I/O

S No.	Fault Condition	Diagnostic coverage
1.	Overvoltage or under voltage detection at 24V input supply	The eFuse generates a fault signal eFUSE FLT fed to MCU.
2.	PCB temperature exceeds recommended operating range	Digital temperature sensor generates signal to the MCU. Output of analog temperature sensor is monitored by MCU 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.

VI. 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.

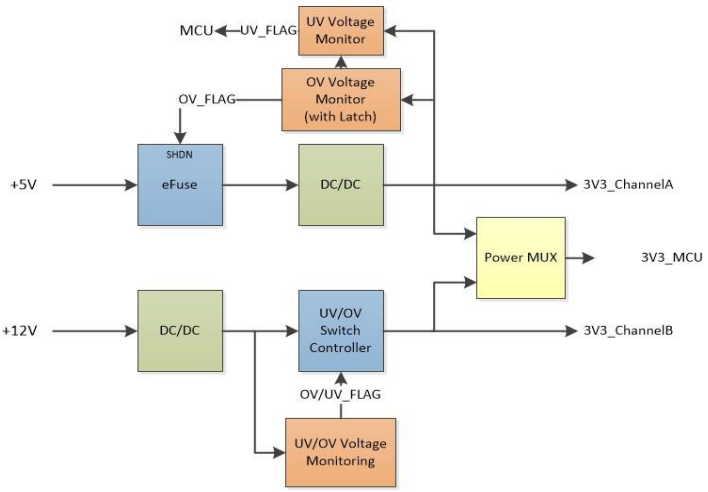

Figure8. Block diagram of safe power supply

A. 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 eFuse at the input, thereby disconnecting the input supply. The eFuse 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 eFuse enables a controlled startup thereby regulating the inrush current.

B. 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 60V. 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 3.3V_ChannelB power supplies are multiplexed using a priority power MUX where the priority is given to the highest input voltage.

VII. 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.

VIII. 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-mΩ Single-Channel High-Side Switch (Rev. A) (SLVSE42A)," TPS27S100x Datasheet, Mar 2018
3. Texas Instruments, "TPS22919-5.5 V, 1.5 A, 90-mΩ 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 eFuse 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 Micropackage (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. Texas Instruments, "SN6505x - Low-Noise 1-A Transformer Drivers for Isolated Power Supplies (Rev. G) (SLLSEP9G)," SN6505x Datasheet, Nov 2018
14. Texas Instruments, "TPL7407L - 40-V 7-Channel Low Side Driver (Rev. D) (SLRS066D)," TPL7407L Datasheet, Mar 2016
15. Texas Instruments, "TPS212x - 2.8-V to 22-V Priority power MUX with seamless switchover (Rev. C) (SLVSEA3C)," TPS212x Datasheet, Feb 2019
16. Texas Instruments, "TPS3703-Q1 - Overvoltage and Undervoltage Reset IC With Time Delay and Manual Reset (Rev. A) (SBVS344A)," TPS3703-Q1 Datasheet, Nov 2018
17. Texas Instruments, "TMS320F2837xD Dual-Core Delfino™ Microcontrollers (Rev. K) (SPRS880K)," TMS320F2837XD Datasheet, Nov 2018
18. "IEC 61800-5-2", International Standard, "Adjustable speed electrical power drive systems – Part 5-2: Safety requirements – Functional"