Implementing STO functionality with diagnostic and monitoring for industrial motor drives

By Aishwarya Bhatnagar
System Engineer, Motor Drives, Industrial Systems

Introduction

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

Safety-integrated drives must comply with certain standards, such as those listed in Table 1.

Table 1. Safety standards

Standard	Title
International Electro technical Commission (IEC) 61800-5-2	Adjustable speed electrical power drive systems Part 5-2: Safety requirements—Functional
IEC 61508	Functional safety of electrical/electronic/programmable electronic safety-related systems
International Organization for Standardization (ISO) 13849-1/2	Safety of machinery—Safety-related parts of control systems: Part 1: General principles for design Part 2: Validation
IEC 60204-1	Safety of machinery—Electrical equipment of machines: Part 1: General requirements
IEC 62061	Safety of machinery—Functional safety of electrical, electronic and programmable electronic control systems

Understanding safety terminology

IEC 61800-5-2 is a drive-specific standard that defines different safety sub-functions and their safety performance levels that are to be implemented for prevention of hazardous conditions. One of the most common sub-functions is:

- Safe torque-off (STO). A stopping function that prevents torque-producing power from being provided to the motor. For example, in any industrial scenario, a production cell is often protected by an interlocked guard door. Operators commonly (and mistakenly) open the guard door without stopping the machine. STO functionality mitigates such hazardous situations and triggers an emergency stop.

Any safety-related system can be specified in terms of its safety-integrity-level (SIL) requirements. SIL specifies a target level of risk reduction by a functional safety function. The highest SIL that can be claimed for a safety sub-function is limited by the hardware fault tolerance (HFT), safe failure fraction (SFF) and the type of subsystems that carry out the safety sub-function. These can be defined in terms of the following parameters:

- "Probability of dangerous failures per hour (PFHD)" is the average frequency of a dangerous failure of a system to perform a specified safety sub-function over a given period of time. Table 2 shows that the lower the probability of undetected dangerous failures per hour, the higher the SIL level.

Table 2. Target failure measures for power drive system (safety-related) sub-functions

SIL	PFHD
3	$\geq 10^{-8}$ to $<10^{-7}$
2	$\geq 10^{-7}$ to $<10^{-6}$
1	$\geq 10^{-6}$ to $<10^{-5}$

- The "safe failure fraction (SFF)" of the subsystem is calculated with Equation 1:

$$SFF = \frac{(\sum \lambda S + \sum \lambda Dd)}{(\sum \lambda S + \sum \lambda Dd + \sum \lambda Du)} \quad (1)$$

where $\Sigma\lambda S$ is the sum of safe failures (safety function not affected), $\Sigma\lambda Dd$ is the sum of detected dangerous failures (safety function not affected) and $\Sigma\lambda Du$ is the sum of undetected dangerous failures (safety function affected).

Increasing the diagnostic coverage of the safety function and introducing fault tolerance increases the SFF. An HFT of N means that an N+1 number of dangerous failures could cause a loss of the safety sub-function. Industrial drives are usually designed to maintain the STO function even in the presence of a single fault (HFT ≥ 1). Introducing hardware redundancy can increase the HFT.

- "Subsystem" denotes part of the top-level architectural design of a safety-related system, the failure of which will result in a failure of a safety-related function.

Components play an important role in achieving safety standards. For instance, failure mode and effects analysis (FMEA) is a structured approach to discovering potential failures that may exist within the design of a product or process. The pin FMEA of any device can be translated to a system FMEA to develop fault models for a system.

The failure-in-time (FIT) rate is defined as a failure rate of 1 per billion hours. For functional safety designs, the FIT rate calculation is not straightforward and follows a more stringent process. Failure distribution analysis

within the device is crucial in determining the overall FIT rate of a system. If any particular function of a device has a high chance of failing, then appropriate hardware design around that function can help reduce the probability of failure.

Table 3 defines two types of subsystems. Depending on the type of subsystem, the SIL for a particular combination of HFT and SFF will vary.

- "Process safety time" (PST) is one of the most crucial parameters when dealing with safety. It is defined as the period of time between a hazardous failure and the time by which action has to be completed in the control system to prevent the hazardous event from occurring. The system should be fast enough to respond within the PST to prevent hazards.

How is STO implemented?

There are different electronic ways to remove torque from a motor, as shown in Figure1.

One way is to implement hardware that disables the motor power by turning off the gate drivers. This implementation is based on a 1-out-of-2 (1oo2d) architecture with diagnostics. A 1oo2 architecture has two channels; if a failure occurs in one of the channels, the other is still capable of implementing the safety function.

In Figure 1, both independent-hardware channels (channel 5 and channel 6) are capable of disconnecting the gate-driver power supply to ensure that the torque generating energy to the motor can be removed when the either of the STO inputs is triggered. In case one unit fails, the system is still functional.

Table 3. Types of subsystems

Subsystem A				Subsystem B			
A subsystem can be regarded as type A if, for the components required to achieve the safety function: • The failure modes of all constituent components are well-understood. • The behavior of the subsystem under fault conditions can be completely determined. This can be translated to system FMEA. • There is sufficient dependable failure data from field experience to show that the claimed failure rates for detected and undetected dangerous failures are met. This can be translated to FIT rate.				A subsystem shall be regarded as type B if, for the components required to achieve the safety function, one or more of the criteria of type A is not satisfied. These subsystems generally include more complex components and require a higher SFF for a given SIL.			
SFF	**HFT N**			**SFF**	**HFT N**		
	0	1	2		0	1	2
<60%	SIL 1	SIL 2	SIL 3	<60%	N/A	SIL 1	SIL 2
60% to 90%	SIL 2	SIL 3	SIL 3	60% to 90%	SIL 1	SIL 2	SIL 3
90% to 99%	SIL 3	SIL 3	SIL 3	90% to 99%	SIL 2	SIL 3	SIL 3
≥99%	SIL 3	SIL 3	SIL 3	≥99%	SIL 3	SIL 3	SIL 3

Figure 1. Different ways of realizing STO

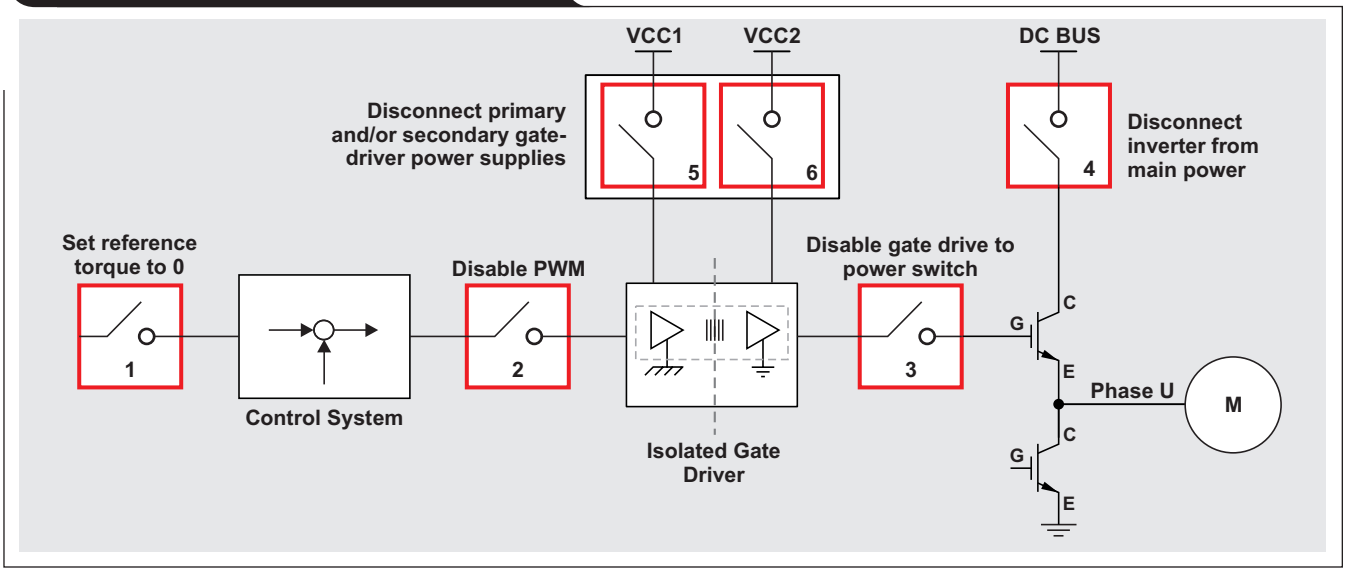


Figure 2 is a block diagram of the STO function for complementary metal-oxide semiconductor (CMOS) input-isolated gate drivers and logic-supply voltages, providing an HFT of 1. Implementing a hardware shutdown across channels by using a three-input AND gate and taking a third input from the other channel's low-pass filter output helps further enhances safety.

STO1 and STO2 control the primary- and secondary-side power to the gate driver through the power switch and high-side switch, respectively. As long as a logic 1 (+24 VDC) is present at both STO inputs, the motor is operable. A logic 0 (0 V) at one or both of the STO inputs will disconnect power to the gate driver and bring the motor to an uncontrolled stop. It's also possible to configure the MCU to disable the pulse-width modulated signal using either of the STO signals until a software reset operation is performed.

Figure 2. Block diagram of STO function

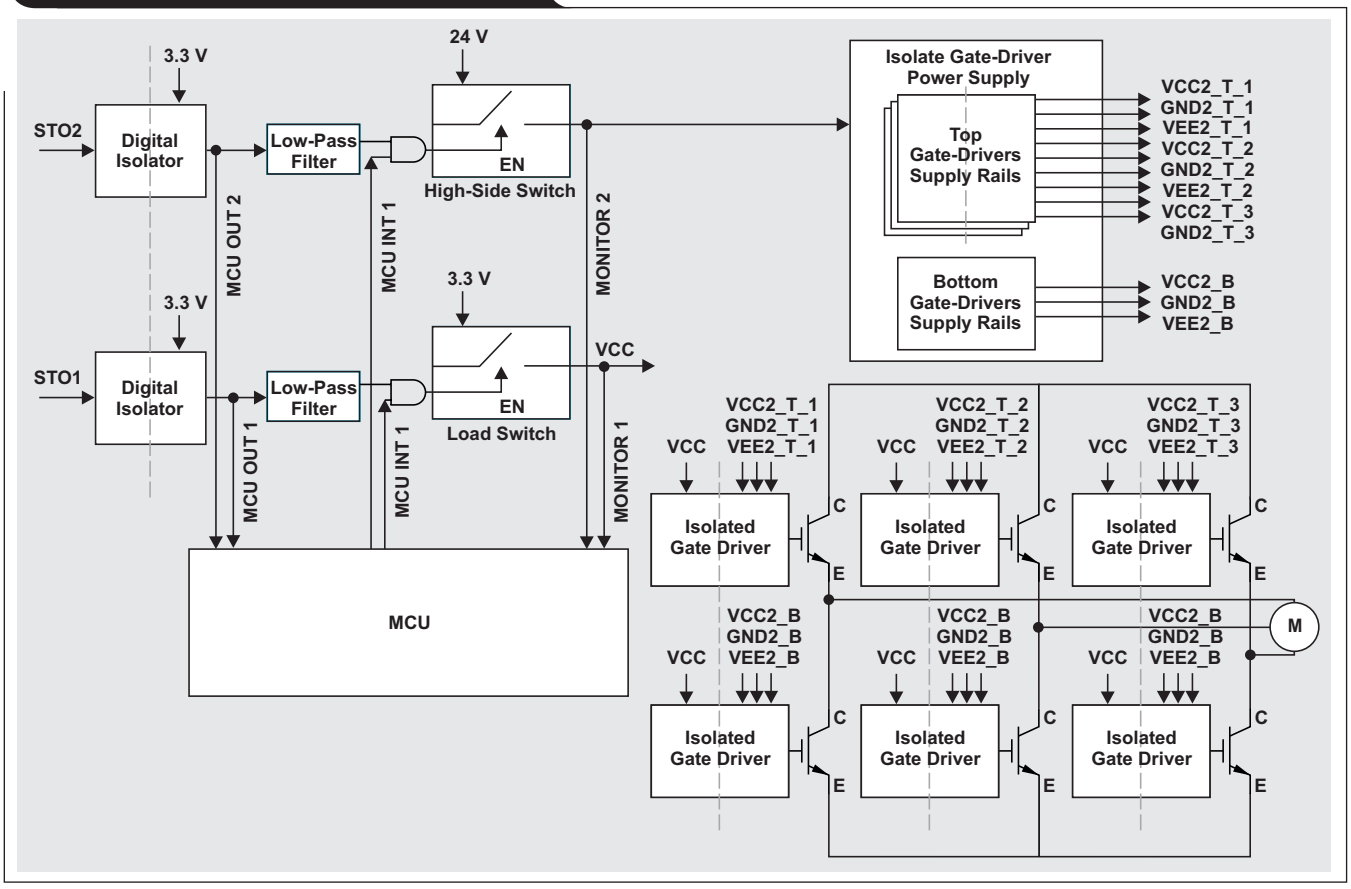


Table 4 highlights some of the diagnostic capabilities of the STO design when both STO signals are generated by external devices. The 1oo2d architecture helps achieve a HFT of 1. Only the occurrence of two simultaneous faults can cause failure of the safety function.

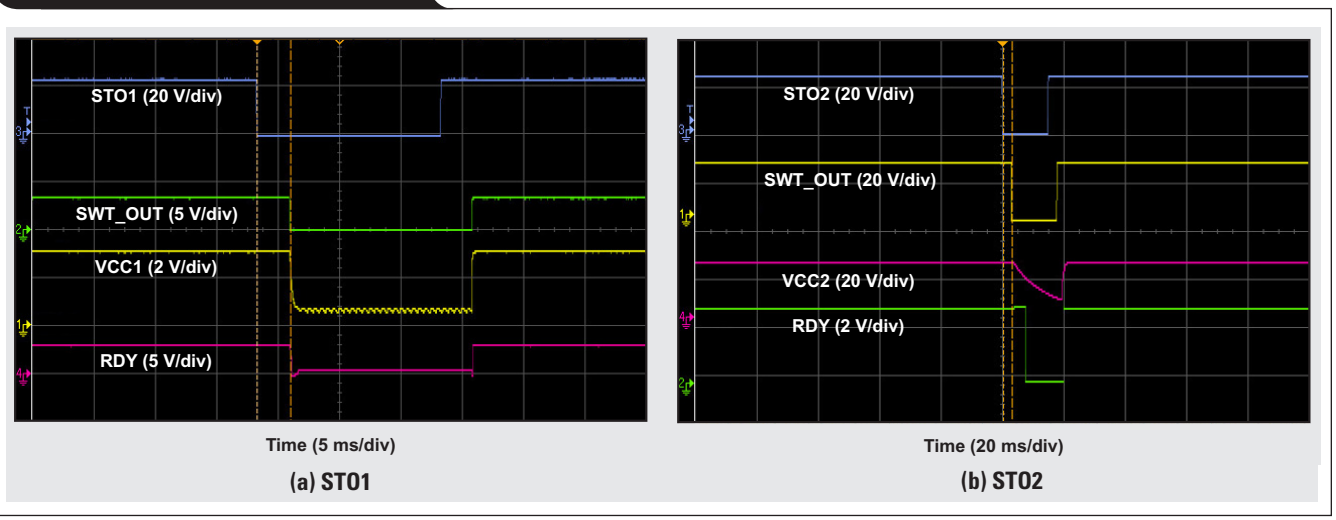
Since STO is not a controlled stopping function, the motor coasts down to zero speed. The time it takes for the motor to stop depends on the load conditions and type of motor. Figure 3 shows the response times of the proposed STO design. Figure 3a shows where STO1 is pulled low for a period of 15 ms. The output voltage of the power switch, primary gate-driver supply voltage (VCC1) and RDY signal from the gate driver were monitored and their waveforms captured. The response time between the STO1 going low to the activation of the RDY signal is 2.8 ms. The response time is a function of the capacitance at the output of the power switch. VCC1 going below the undervoltage lockout threshold activates the RDY signal.

Similarly, STO2 pulls low for a period of 15 ms. Figure 3b shows the output of the secondary gate-driver power supply (VCC2) and RDY pin of the gate driver. The response time measured between the STO2 going low to the activation of the RDY pin is 7.6 ms.

Table 4. Diagnostic coverage of the STO implementation per component

Number	Component	Component Function	Fault Condition	Impact on the Safety Function	Measure to Control/Detect the Fault (Fault reaction time/diagnostic test interval diagnostic coverage)
1	Digital isolator for STO1 (similar for STO2)	Isolation of STO signal and to correctly interpret the digital logic	MCUOUT1 is stuck to VCC1	Dangerous failure; inverter will continue to work despite STO1 being low	MCU can monitor the signal (MCUOUT1) for periodic low pulses sent by the PLC
			MCUOUT1 is stuck to ground	Safe failure; inverter will turn off	
2	Low-side power switch (similar for high-side power switch)	Turn supply rails to the isolated gate bipolar transistor (IGBT) gate driver power supply on or off	Power switch does not turn on	Safe failure; inverter will turn off	
			Power switch does not turn off	Dangerous failure; inverter will continue to work despite STO being low	Diagnostic pulse (MCUINT1) sent by the MCU can detect this fault (Monitor1) and turn the switch off
3	High-side Power switch	Turn the secondary supply rails to the IGBT gate driver power supply on or off	Output short to ground	Safe failure	When the switch is on, a short-to-ground condition causes overcurrent, which triggers the fault condition
			Output short to supply	Safe failure	The device can recognize a short-to-supply condition under the switch's on and off conditions

Figure 3. STO response times



Conclusion

Functional safety has become an integral part of motor drives. Its main objective is to bring machines to a safe state quickly. There are different ways to implement any safety function; each method is unique in terms of design requirements and achievable SIL. Various methods were shown for STO implementation in addition to diagnostic and response-time examples. Reference designs are available from Texas Instruments (TI) for STO and SBC implementations with detailed hardware-design guidelines and system test results.

Related Web sites

Product information:

Motor drive systems

Servo-drive functional safety module

TI reference designs:

Redundant dual channel safe torque off (STO) reference design for ac inverters and servo drives (TIDA-01599)

Smart brake control and diagnostics reference design for servo drives and robotics (TIDA-01600)

Smart holding brake controller reference design with current regulation for servo drives & robotics (TIDA-01621)

TI Worldwide Technical Support

TI Support

Thank you for your business. Find the answer to your support need or get in touch with our support center at

www.ti.com/support

China: http://www.ti.com.cn/guidedsupport/cn/docs/supporthome.tsp

Japan: http://www.tij.co.jp/guidedsupport/jp/docs/supporthome.tsp

Technical support forums

Search through millions of technical questions and answers at TI's E2E™ Community (engineer-to-engineer) at

e2e.ti.com

China: http://www.deyisupport.com/

Japan: http://e2e.ti.com/group/jp/

TI Training

From technology fundamentals to advanced implementation, we offer on-demand and live training to help bring your next-generation designs to life. Get started now at

training.ti.com

China: http://www.ti.com.cn/general/cn/docs/gencontent.tsp?contentId=71968

Japan: https://training.ti.com/jp

A011617

SLYT780

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, 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 (www.ti.com/legal/termsofsale.html) 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.

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265