Technical Article

Functional Safety for Industrial Motor Drives

Sam G. Sabapathy

Updated 9/23/2020

Industrial functional safety relies on a system functioning correctly in response to its inputs. The system should be able to detect potentially dangerous faults and deploy safety mechanisms to prevent or minimize the impact of a hazardous event. Historically, industrial applications supported simple hardware and software combinations to ensure functionally safe execution and equipment protection. In contrast, today's industrial products and systems have increasingly complex microelectronics, including high-megahertz microcontrollers (MCUs), microprocessors (MPUs), field-programmable gate arrays (FPGAs) and application-specific integrated circuits (ASICs). Consequently, the software now includes sophisticated control algorithms, state machines and user interface functions. The added complexity of hardware and software integration is a challenge for designers to assess, implement and verify/validate.

MCUs that include mixed-signal sensing can control various motors such as alternating current induction, brushless and brushed motors. To assist in making these systems functionally safe, however, several international standards evolved that are applicable to industrial drives:

- International Electrotechnical Commission (IEC) 61800-5-2: safety requirements for adjustable-speed electrical power drive systems.
- Safety integrity levels (SILs) as defined by IEC 61508.
- Performance levels (PLs) as defined by the International Organization for Standardization (ISO13849) machinery safety standard.

Industrial Drives and Functional Safety

TI C2000™ microcontrollers control the power stages that drive electrical machines and power-conversion systems like digital power and solar inverters. Functional safety is applicable to all of these systems. Variable-speed electrical drive systems can directly affect machinery, humans and the environment. These involve the safe operation of high-voltage motors and motion during power up and sustained operation. The location of these drives is often hostile to operators and demands safety and protection so that the machine, material and operator are safe in the event of an electrical, electronic/programmable electronic or mechanical failure.

Variable frequency drives (VFDs) are built with C2000 real-time microcontrollers that generate pulse-width modulation (PWM) signals to switch the high-voltage power electronics that drive motors. Efficient PWM generation involves complex algorithms based on real-time feedback (both analog and digital) from the motor assembly. C2000 MCUs are capable of not only generating motor-control signals, but also detecting faults within their own resources and in connected motor system components. Additionally, these MCUs can issue a safe torque off (STO) signal to shut the power stage down in case of a credible fault.

STO signals are often associated with ancillary signals that allow braking of the related motion equipment to avoid damage to machines, material and operators. An STO signal is the basic safety function in the majority of the industrial systems that extend protection to the power stage and related motion equipment. The IEC 61800-5-2 standard extends this with an exhaustive list of drive safety functions that allow small and big motion systems to reach a functionally safe state. The execution of these safety functions requires additional MCU processing power and independent sensing capabilities.

Functional safety standards such as IEC 61508 outline several requirements for MCUs classified as Type B elements. IEC 61508 defines normative requirements for systematic, random hardware failure metrics and software development methodologies for MCUs to implement safety functions with high confidence. The diagnostics capabilities of these MCUs at the hardware and software levels allow components to reach SILs of 1, 2, 3 and 4 (4 being the most stringent and difficult to achieve).

Even after leveraging a component's (i.e. an MCU's) diagnostic capability, motor drive systems cannot reach functional safety compliance unless they comply with ISO 13849 machinery directive and metrics. According to ISO 13849, all motor- and machinery-related safety functions (such as STO signals) are required to meet a performance level (PL) using a well-designed safety logic circuit with deterministic diagnostic capabilities. In general, all motor safe-functions (STO signals defined by IEC 61800-5-2) can reach a PL if the safety circuit is also designed to meet a category 3 (Cat 3) or category 4 (Cat 4) type of topology.

Categories and PLs are ISO 13849 metrics defined for safe functions (STO signals) to be implemented with a high certainty. Category 3 and Category 4 outline hardware fault tolerant (HFT=1) architectures. These are inherently dual channel systems with each channel comprising of an MCU, position and feedback sensing capabilities. It is mandatory to have these safety channels to be assessed/certified for high diagnostic coverage with Safety integrity level (SIL2) or greater and safety failure fraction (SFF) >90%. The resulting functional safety module or circuit shown in Figure 1 (the orange box) can monitor the main drive controller and motion system and issue an STO signal when detecting a fault.

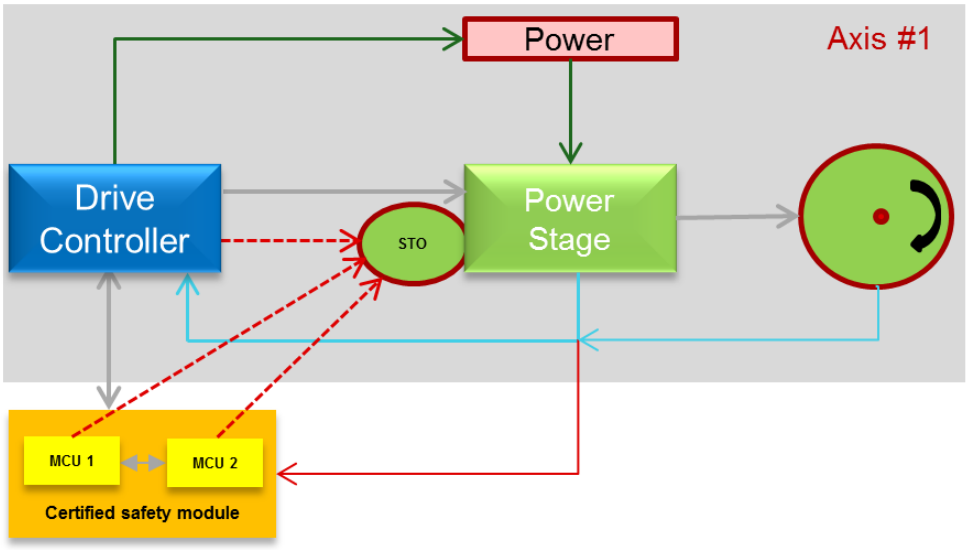

Figure 1. Two-channel functional safety module example

An STO from this certified safety module can come from either of the MCUs when any fault is detected. These MCUs are in constant communication about machine health and the motion system, and at any instant at least one of the MCUs will have the mastership to issue an STO signal or advanced STO signals (Safe Limited Speed –SLS, Safe Brake Control-SBC etc.) to safely shut down the motor and motion equipment under all operating conditions. This two-channel module is certifiable by functional safety assessors and its STO action is capable of reaching SIL 3 and a PL of PLd or PLe. PLd and PLe indicate a higher probability of dangerous failures per hour, which is greater than 10^{-7} and 10^{-8}, respectively.

The F2837x, F2838x, F28004x, and F28002x C2000 real-time MCUs are built with inherent functional safety features to handle any real-time power stage control very efficiently. Low cost C2000 MCU derivatives can be used to build dual-channel safety modules capable of high diagnostic coverage with on-chip position and feedback sensing. The C2000 MCU functional safety enablers comprise of a rich assembly of documentation, tools and software diagnostic libraries that help you (the system integrator) navigate the complex certification process of your functionally safe drive systems or equipment.

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