Functional Safety for Integrated Circuits Used in Variable Speed Drives

Tom Meany
Analog Devices, Inc.

Abstract

Functional safety is the branch of safety related to the correct functioning of electrical and electronic systems. Variable speed drives now play an important part in implementing functional safety. Previously, functional safety for motor control applications was realized using safety relays and contactors external to the drive. But with safety integrated in the drive safety functions, such as STO and SLS, it can be implemented within the drive offering productivity enhancements on the factory floor. Integrated safety requires the use of integrated circuits but interpreting the functional safety requirements for integrated circuits used in variable speed drives is challenging. Ideally all such ICs would be assessed to IEC 61508 but this would be expensive and is not demanded by the standards. This article will attempt to summarize what guidance is available for integrated circuits being used in the design of variable speed drives. One of the goals for this article is to provide an overview of the topics without the use of jargon.

The Key Three Requirements of Functional Safety

Functional safety has three key requirements:

Requirement 1—To use reliable components. This means ICs with a sufficiently low FIT rate. FIT rates are often calculated according to standards such as IEC 62380 or SN 29500, which base their results on the average failure rate seen in the field for various types of components. Alternatively, data can be based on accelerated life testing such as that found at *analog.com/ReliabilityData*. One important consideration is that the PFH (probability of dangerous failures per hour) figures given in IEC 61508 and similar standards are for an entire safety function and not just for a single IC. Therefore, the PFH figure of 10^{-7} h^{-1} for a SIL 3 safety function (100 FIT) might give an error budget of only 1 FIT for a given IC. It is also worth noting that the term PFH actually means the probability of dangerous failures per hour. It can be argued that at least 50% of failures are safe and that the reliability limit for the IC can be doubled.

Requirement 2—Implement a set of measures that have been shown in the past to design products with high safety. This is referred to the standards as systematic integrity. Different from random hardware failures, systematic failures are built into a system and only a design change can eliminate them. Software bugs are examples of systematic failures, as well as EMC failures.

Requirement 3—Be fault tolerant and accept faults due to random hardware failures, or systematic faults will occur no matter how reliable the components or how good the development process followed. Two ways to then cope with the faults are through diagnostics and redundancy. Diagnostics detect the faults and take the system to a safe state. For motor control, the safe state is generally to bring the motor to a stop with a safety subfunction such as STO from IEC 61800-5-2. The other alternative is to implement redundancy so that there are two or more items, either one of which can detect an unsafe state and bring the system to a safe state when required to do so. Standards generally allow a trade-off between diagnostics and redundancy. Measures of the effectiveness include SFF from IEC 61508, diagnostic coverage (DC) from ISO 13849, and the single point fault metric from ISO 26262.

IEC 61800-5-2

IEC 61800-5-2 is a type C standard. This means that this standard sets out the requirements for a particular machine category, in this case a variable speed drive. Having a type C standard is very valuable because it interprets the generic standard IEC 61508 for that equipment type and only keeps what is relevant for that machine. A generic standard by its nature has to cope with many different types of equipment and situations, which means that it contains a lot of information and requirements that are not relevant to a specific design. IEC 61800-5-2 boasts that, "by applying the requirements from this part of the IEC 61800 series, the corresponding requirements of IEC 61508 that are necessary for a PDS (SR) are fulfilled." However, in the event of there being topics in which the type C standards, such as IEC 61800-5-2, give no guidance, then IEC 61508 is the fallback.

Within IEC 61800-5-2 safety subfunctions such as STO (safe torque off) and SLS (safely limited speed) are defined and a functional safety life cycle outlined.

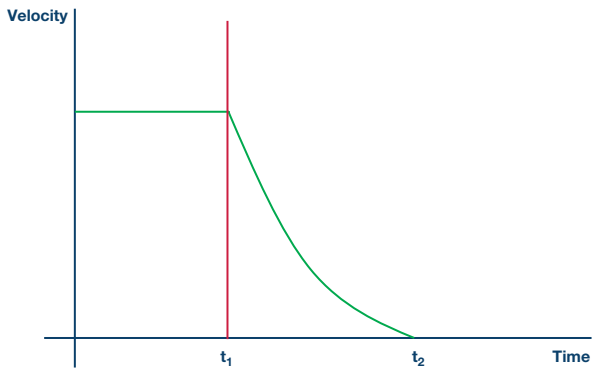

Figure 1. STO safety function.

With the STO safety subfunction a safe state can be achieved by preventing force producing power from being provided to the motor. Typically this will be done using pulse blocking or power removal at the gate driver when a guard is open. Since total power to the drive is not removed, a quick restart can be facilitated once the guard is closed.

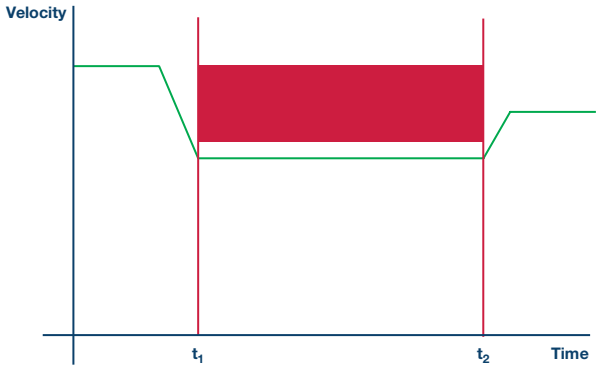

Figure 2. Safely limited speed.

With the SLS safety subfunction the speed of the motor is monitored and if a set level is exceeded the drive takes the motor to a safe state, most often STO. A typical use of this safety subfunction might be during the cleaning of a roller in conjunction with a three position grip switch. Figure 2 shows SLS engaging at t_1 and disengaging at t_2. The red block indicates a speed region that (if entered) will cause the drive to go to a safe state.

While IEC 61800-5-2 does not enforce a requirement for 2-channel safety, most drive manufacturers will also want to claim a performance level according to ISO 13849 and, therefore, two channels are common.

ISO 13849

ISO 13849 is the machinery standard based on the now redundant EN954 standard. In contrast to IEC 61800-5-2, IEC 61508, and IEC 62061 it uses performance levels (PL) instead of SIL levels. The levels are PLa through PLe. ISO 13849 also has a clear preference for 2-channel systems for the higher performance levels, a category three or four system must be used. ISO 13849 uses DC (diagnostic coverage) as a metric for diagnostic effectiveness as opposed to the SFF from other standards. On the assumption that faults are 50% safe/50% dangerous SFF and DC are related using the equation below.

$$SFF = 0.5 + 0.5 \times \mathrm{DC} \quad (1)$$

IEC 62061

IEC 62061 is the machinery interpretation of IEC 61508. It is in effect a parallel standard to ISO 13849—in fact, there is an effort to combine both machinery standards in ISO/IEC 17305.

In the scope of IEC 62061 it states that "In this standard, it is presumed that the design of complex programmable electronic subsystems or subsystem elements conforms to the relevant requirements of IEC 61508. This standard provides a methodology for the use, rather than development, of such subsystems and subsystem elements as part of an SRECS."

IEC 61508

IEC 61508-2:2010 contains significant IC requirements but they can be easy to miss on a casual or incomplete reading of the standard. The requirements include an ASIC development V model, see IEC 61508-2:2010 Figure 3. The V model is targeted at digital ASICs in the sense that it references synthesis placement and routing along with final coding, but the V model can be interpreted for analog or mixed-signal ASICs using a little imagination.

The preference for digital ASICs continues into Annex F, which is entitled, "Techniques and Measures for ASICs—Avoidance of Systematic Failures" and in Note 1 states, "The following techniques and measures are related to digital ASICs and user programmable ICs only. For mixed-mode and analog ASICs no general techniques and measures can be given at the moment." Despite the limitations, however, it is quite feasible to complete the checklist for the digital portion of a mixed-signal ASIC and with some use of not applicable to even a purely analog IC.

Annex E is entitled "Special Architecture Requirements for Integrated Circuits (ICs) with On-Chip Redundancy." Once again, a digital limitation is put on the annex when it states in E.1 that "The following requirements are related to digital ICs only. For mixed-mode and analog ICs no general requirements can be given at the moment." Another restriction on Annex E that seems to be widely ignored when the annex is quoted in other standards is that "on-chip redundancy as used in this standard means a duplication (or triplication) of functional units to establish a hardware fault tolerance greater than zero." The word duplication means identical redundancy and the author of this article believes the target was dual core micros possibly using the lockstep technique. While most of the techniques are good they may be excessive when applied to separation between diverse redundant blocks or between a block and another on-chip block used as a diagnostic on the first block. Duplicated blocks are subject to common cause failures such as temperature, ESD, power supply failures, and others that are less likely to affect diverse blocks in the same way at the same time. An example of how Annex E is quoted can be found in Section D.2.4 of ISO 13849-2:2012 where it states "Consequently, it is highly unlikely that the multichannel functionality necessary for the fault tolerance and/or detection requirements of category 2, 3, or 4 can be achieved using a single integrated circuit, unless it satisfies the special architecture requirements of IEC 61508-2:2010, Annex E." IEC 61800-5-2 FDIS (Autumn 2015) allows a possible exclusion for on-chip short circuits based on the requirements of Annex E of IEC 61508-2:2010, but examining Annex E you find that only items f) and g) refer to directly to on-chip shorts. Item f) requires spacing between separate blocks of at least 10× the minimum design rule for the process and item g) talks only about adjacent lines of separate physical blocks.

Table A.1 of IEC 61508-2:2010 gives faults or failures to be assumed when calculating the SFF. Tables A.2 to A.14 give examples of the typical diagnostic coverage, which can be claimed for typical diagnostics but the tables can sometimes need interpretation for integrated circuits. Annex H of IEC 62380 and the related Appendix A of UL 1998 are more detailed especially for digital microcontrollers and similar.

In terms of calculating FIT rates for integrated circuits, IEC 62380 and SN29500 are both referenced along with other sources.

The requirement to consider soft errors was added in the 2010 revision of the standard and has implications for the addition of ECC and parity to volatile memories (such as RAM) in order to detect and control soft errors that affect RAMs in particular.

ISO 26262 Requirements

ISO 26262 is the automotive interpretation of IEC 61508. It was developed in parallel to revision 2 of IEC 61508 and contains some requirements related to integrated circuits not found in IEC 61508, some clarification of items in IEC 61508 but omits other requirements. For instance, ISO 26262-10:2012 contains an automotive version of IEC 61508-2:2010 Annex F and Table D.1 of ISO 26262-5:2011, which clarifies the position for automotive on how to consider on-chip shorts with "It is not intended here to require an exhaustive analysis, for example to require the exhaustive analysis of bridging faults that can affect any theoretical combination of any signal inside a microcontroller or in a complex PCB. The analysis focuses on main signals or on very highly coupled interconnections identified with a layout level analysis."

Part 10 in particular contains nuggets such as "if a CPU area occupies 3% of the whole microcontroller die area, then its failure rate could be assumed to be equal to 3% of the total microcontroller failure rate." While such a process is part of the custom and practice of IEC 61508 it is good to see it written down.

An integrated circuit interpretation of ISO 26262 is being worked on as ISO/AWI PAS 19451-1 under ISO/TC 22/SC32.

Assistance in Designing Integrated Circuits

Having reviewed the standards, the author has a number of recommendations on how IC manufacturers can assist drive manufacturers in designing in integrated circuits into their drives.

Firstly, a safety manual for integrated circuits should be of benefit to drive designers. This can be produced even if the ASIC or device was not developed to IEC 61508.

Items that are available in the safety manual might include:

- The development process and lifecycle model used.
- A completed Annex F checklist from IEC 61508-2:2010.
- The assumed mission profile.
- FIT rate predictions according to IEC 62380 and SN29500 at a reasonable average operating temperature, for instance 55°C with thermal cycling of 10°C over a 24 hour period.
- Die size, number of die, number of RAM cells, and transistor counts to allow drive designers to calculate their own FIT rates using SN29500 and IEC 62380 (better still if the calculations are already completed and details of the calculations are given).
- Evidence to support claims of on-chip separation.
- Evidence to support the claiming of any relevant fault exclusions.
- Details of the on-chip diagnostics.
- Details of assumed system level diagnostics.
- Results of a pin FMEA giving λ_{DU}, λ_{DD}, λ_S, and calculated SFF and DC for an assumed set of diagnostics looking at expected package failure modes.
- Results of an FME(D)A giving λ_{DU}, λ_{DD}, λ_S, and calculated SFF and DC for an assumed set of diagnostics looking at expected die failure modes.
- A FIT rate for the various blocks shown on the data sheet to allow the drive manufacturer to redo the FME(D)A.

Given the nature of the data, safety manuals may only be available under NDA (nondisclosure agreement).

Parts relevant to motor control safety for which safety manuals are currently being developed at Analog Devices include the AD7403 isolated ADC and the ADuM4135 isolated gate driver.

Secondly, the IC manufacturer having an understanding of the system-level design can assist in designing the required features for functional safety. For example:

- Knowing that only a fraction of the PFH, perhaps just 1% is available to the IC.
- Knowing that while in general for functional safety, simpler is better but that having transistors on chip is extremely reliable and if increasing the number of transistors on chip by a factor of 10 leads to less components on a PCB, the overall PFH will come down.
- Knowing that on-chip diagnostics can react much faster than system-level diagnostics and can help in preventing an accumulation of errors.
- Knowing that the typical lifetime of a drive is 20 years and data should be available to prove the IC can match this lifetime under a given mission profile.
- Knowing that the addition of hardware accelerators such as CRC engines reduce the software burden.

Thirdly, a set of recommended architectures showing how ICs could be combined to implement the safety functions from IEC 61800-5-2. This may involve:

- Recommendations on system-level diagnostics.
- Recommendations on suitable components.
- Recommendations on meeting the independence requirements between different channels.
- Recommendations on software independence between safety and non-safety software, which can reduce the number of required processors from three to two if control and safety can be combined in at least one of the processors. If sufficient independence cannot be shown, then everything must be treated as safety related.

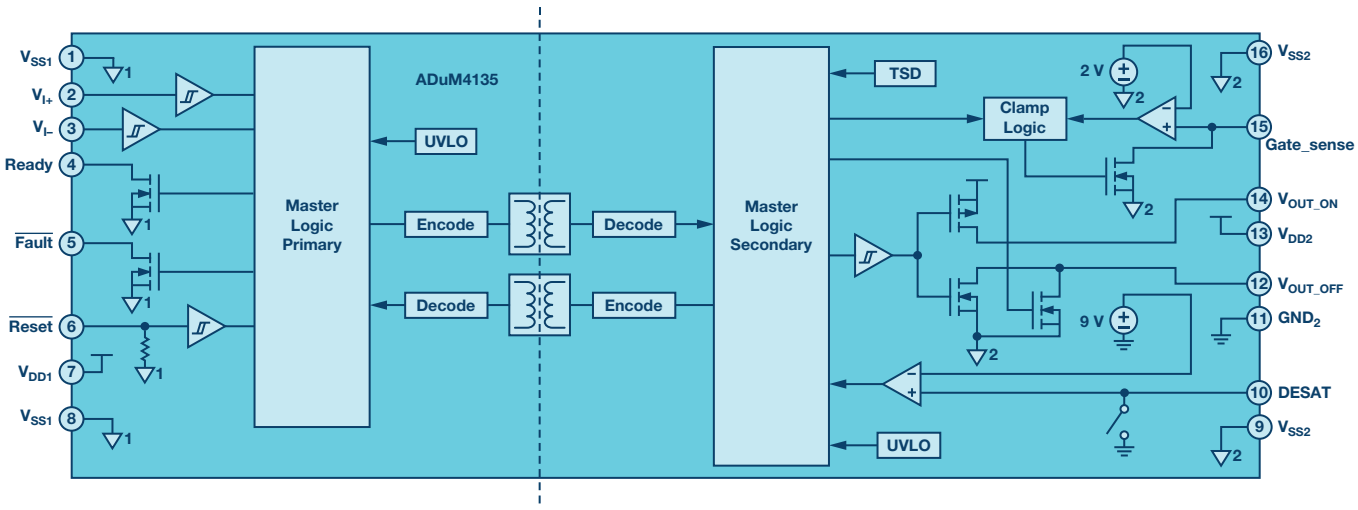

Figure 3. ADuM4135 isolated gate driver.

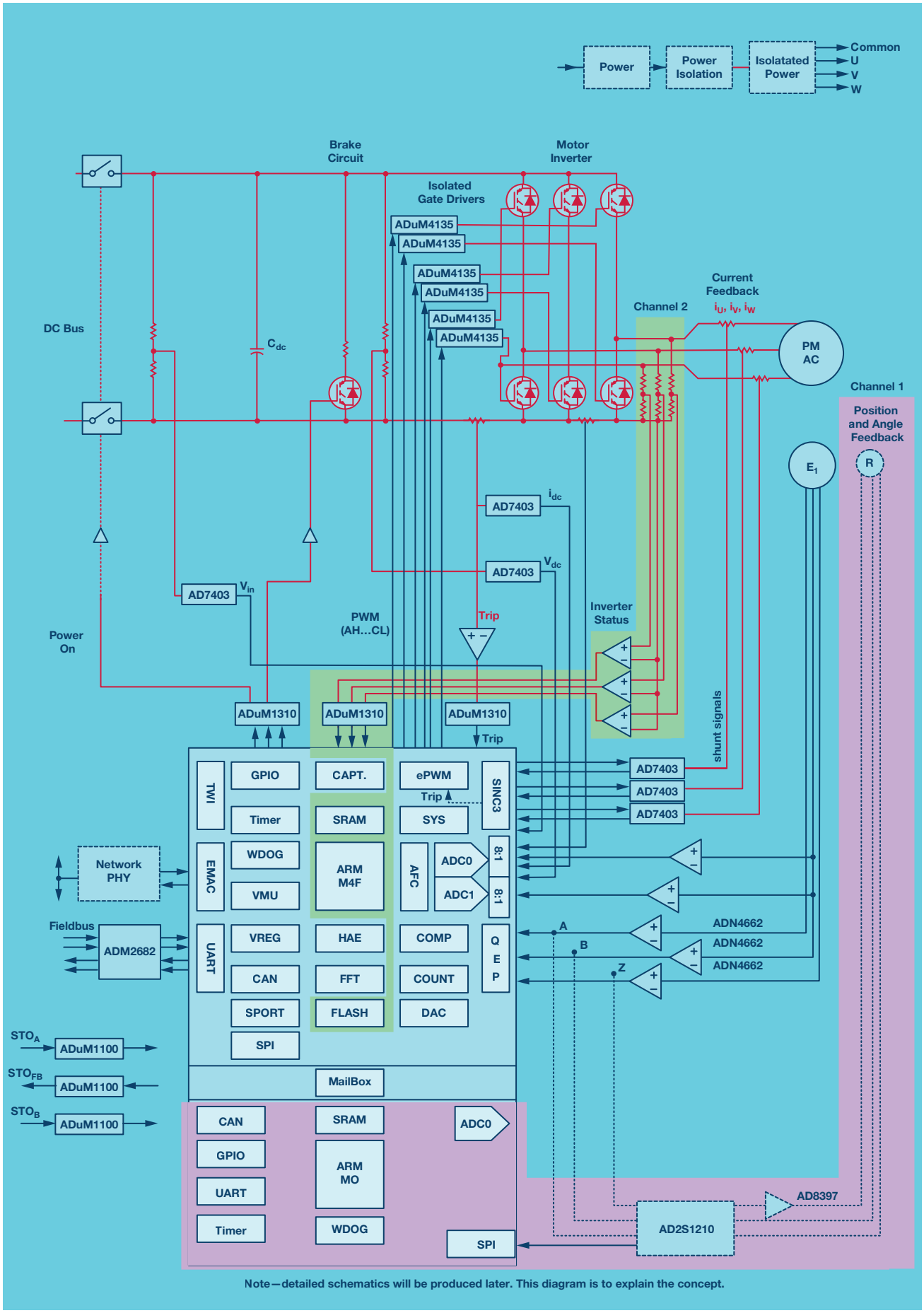

Figure 4. A concept 2-channel architecture for implementation of SLS safety subfunction from IEC 61800-5-2 using the ADSP-CM419(/8/7/6) DSP core.

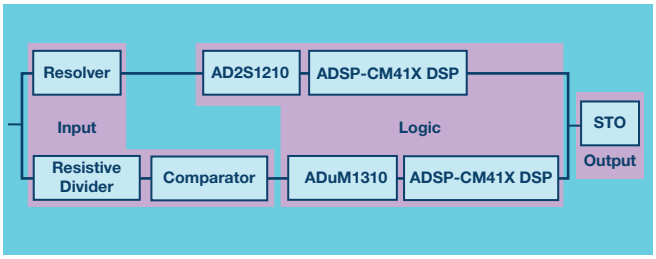

Figure 5. Reliability block diagram for the SLS interpretation.

Fourthly, the standards should be influenced to clarify requirements. For instance:

- What protection against data corruption should be placed on an SPI interface connecting an ADC to a microcontroller or DSP on the same PCB? Standards such as IEC 61800-5-2:2006 refer the reader back to IEC 61508, which in turn refers to rail standards. The next version of IEC 61800-5-2 has added text to clarify that the requirements of IEC 61784-3 do not apply to such interfaces, but when the author read his own words in the new standard the clarification is not as clear as he had hoped. A better clarification is contained in the new draft standard of EN 50402 where it distinguishes between signal transmission for a spatially separated module and signal transmission between modules not spatially separated.
- Clarification on the on-chip separation requirements for ICs implementing diverse redundancy.
- Clarification on the on-chip separation requirements for analog and mixed-signal ICS.

Fifthly, removing references to particular solutions from the standards, which leads some readers to believe these are the only solutions to a problem. For instance, optocouplers are an old and well known means to achieve signal isolation but have a number of disadvantages in terms of reliability, power, and speed compared to newer digital isolators. Editing standards such as ISO 13849 and IEC 61800-5-2 and replacing references to optocouplers with more generic terms such as galvanic isolators will also help the adoption of newer more reliable digital isolators. This has been done in the latest FDIS (final draft) of IEC 61800-5-2 in 2015.

Conclusion

This article presents a review of the main functional safety standards related to machines and variable speed drives in particular. From this review, conclusions on the requirements related to integrated circuits have been drawn. One conclusion is that, to aid in meeting the requirements of functional safety IC, manufacturers can supply additional information and features. This article lists some of the most important points of that information. A second conclusion is that semiconductor manufacturers need to know more about the system-level requirements and Analog Devices has embarked on an analysis of their own nonfunctional safety, motor control demo system design. The goal is to uncover how that architecture can be modified to meet the requirements of functional safety and to discover what information is missing to allow our customers to design our products into a drive with functional safety requirements.

References

AD2S1210 Data Sheet.

AD7403 Data Sheet.

AD8397 Data Sheet.

ADM2682 Data Sheet.

ADSP-CM408F Data Sheet.

ADSP-CM41x Mixed-Signal Control Processors.

ADuM1310 Data Sheet.

ADuM4135 Data Sheet.

Analog Devices Motor Control Web Page at *http://www.analog.com/motorcontrol.*

Analog Devices Functional Safety Program *http://www.analog.com/en/about-adi/quality-reliability/functional-safety-program.html.*

BGIA Report 2/2008e, Functional Safety of Machine Controls—Application of EN ISO 13849.

IEC 61508-2:2010, Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems—Part 2: Requirements for Electrical/Electronic/Programmable Electronic Safety Related Systems.

IEC 61800-5-2:2007, Adjustable Speed Electric Power Drive Systems, Safety Requirements, Functional Safety.

IEC 62061:2005, Safety of Machinery—Functional Safety of Safety Related Electrical, Electronic, and Programmable Electronic Control System.

ISO 13849-1:2006, Safety of Machinery—Safety Related Parts of Control Systems—Part 1: General Principles for Design.

ISO 13849-2:2012, Safety of Machinery—Safety Related Parts of Control Systems—Part 2: Validation.

ISO 26262:2011, Road Vehicles—Functional Safety.

About the Author

Tom Meany is the holder of eight U.S. patents and is a senior member of both the ISA and the IEEE. Tom is an FS engineer (TUV Rheinland) in the application area machinery and holds a certificate in reliability and functional safety from Technis. He is also a member of IEC SC22G/MT12 working on the second draft of IEC 61800-5-2 (functional safety requirements of variable speed drives). Tom has worked at Analog Devices since 1987 and currently holds the position of Functional Safety Technical Specialist for industrial products.

Analog Devices, Inc.
Worldwide Headquarters

Analog Devices, Inc.
One Technology Way
P.O. Box 9106
Norwood, MA 02062-9106
U.S.A.
Tel: 781.329.4700
(800.262.5643, U.S.A. only)
Fax: 781.461.3113

Analog Devices, Inc.
Europe Headquarters

Analog Devices, Inc.
Otl-Aicher-Str. 60-64
80807 München
Germany
Tel: 49.89.76903.0
Fax: 49.89.76903.157

Analog Devices, Inc.
Japan Headquarters

Analog Devices, KK
New Pier Takeshiba
South Tower Building
1-16-1 Kaigan, Minato-ku,
Tokyo, 105-6891
Japan
Tel: 813.5402.8200
Fax: 813.5402.1064

Analog Devices, Inc.
Asia Pacific Headquarters

Analog Devices
5F, Sandhill Plaza
2290 Zuchongzhi Road
Zhangjiang Hi-Tech Park
Pudong New District
Shanghai, China 201203
Tel: 86.21.2320.8000
Fax: 86.21.2320.8222

TA14491-0-7/16

analog.com

ANALOG DEVICES
AHEAD OF WHAT'S POSSIBLE™