变速驱动器中所用集成电路的功能安全

Tom Meany
ADI公司

摘要

功能安全指与电气和电子系统正常运行相关的安全性能。目前，变速驱动器在实现功能安全方面发挥着重要作用。以前，面向电机控制应用的功能安全是通过驱动器外部的安全继电器和接触器来实现的。但随着安全特性被集成到驱动器当中，STO、SLS等安全功能可以集成到驱动器上，从而提高工厂的生产效率。集成安全要求采用集成电路，但是，解读变速驱动器中所用集成电路的功能安全要求并非易事。理想情况下，所有此类IC均应符合IEC 61508规范，但其成本高昂，因此各项标准并未予以要求。本文将尝试总结相关指导方针，以便在变速驱动器的设计中选用正确的集成电路。本文的目标之一是不使用术语概括各个主题。

功能安全的三个关键要求

功能安全有三个关键要求：

要求1—使用可靠组件。这是指FIT率足够低的IC。FIT率通常依照IEC 62380或SN 29500等标准进行计算，其结果基于各类组件在现场的平均故障率。此外，数据可能基于加速寿命测试，例如*analog.com/ReliabilityData*上提供的数据。一个重要的考虑因素是，IEC 61508和类似标准中给出的PFH (每小时发生危险故障的概率)数字是针对整个安全功能，而不仅仅针对一个IC。因此，SIL 3安全功能(100 FIT)的PFH数字10^{-7} h^{-1}可能会给出错误的预算，即给定的IC只有1 FIT。另外还需要注意的是，PFH实际上是指每小时发生危险故障的概率。可以说，至少50%的故障是安全的，并且IC的可靠性限制可以翻倍。

要求2—实施过去已证明能够设计高安全性产品的一系列措施。这是指称为系统完整性的标准。不同于随机的硬件故障，系统故障内置于系统中，只需要更改设计就能消除它们。软件缺陷便是系统故障和EMC故障的例子。

要求3—容忍缺陷和接受缺陷，因为无论组件多么可靠或者多么遵循开发流程，都会出现随机硬件故障或系统故障。应对故障的两种方法是诊断和冗余。诊断可以检测故障，并使系统处于安全状态。对于电机控制，安全状态通常会使电机利用安全子功能停止，如IEC 61800-5-2的STO。另一个替代方法是实现冗余，这样会有两个或两个以上的项目，任意一个项目可以检测到不安全的状态，并在必要时使系统处于安全状态。标准通常允许在诊断和冗余之间进行权衡。提高有效性的措施包括IEC 61508中的SFF、ISO 13849中的诊断覆盖率(DC)和ISO 26262中的单点故障指标。

IEC 61800-5-2

IEC 61800-5-2是C类标准。这意味着此标准提出了特定机器类别的要求，在这种情况下是指变速驱动器。采用C类标准是非常有价值的，因为它解释了这种设备类型的通用标准IEC 61508，并且只保留了与该机器相关的内容。通用标准本质上必须能够应对许多不同类型的设备和情况，这意味着它包含很多与特定设计不相关的信息和要求。IEC 61800-5-2声称，“通过采用IEC 61800系列的这一部分要求，可以满足PDS (SR)所需要的IEC 61508相应要求。”然而，对于C类标准(如IEC 61800-5-2)没有提供指导的主题，则可以参考IEC 61508。

IEC 61800-5-2中定义了STO (安全转矩关闭)和SLS (安全限制速度)等安全子功能，并概括了功能安全生命周期。

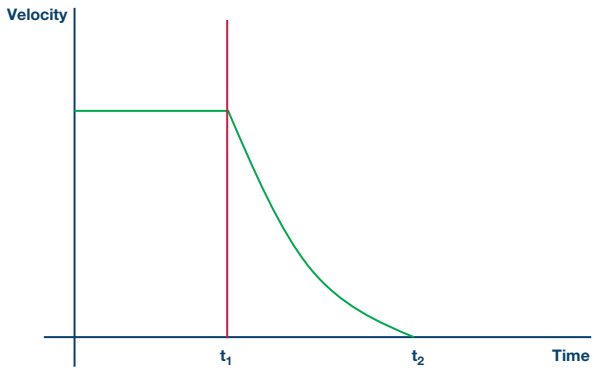


图1. STO安全功能。

借助STO安全子功能，通过防止为电机提供发电的力，可以达到安全状态。通常，当防护装置打开时，可以通过在栅极驱动器阻塞脉冲或切断电源来完成。由于驱动器的总电源切断了，当防护装置关闭时，有助于快速重启。

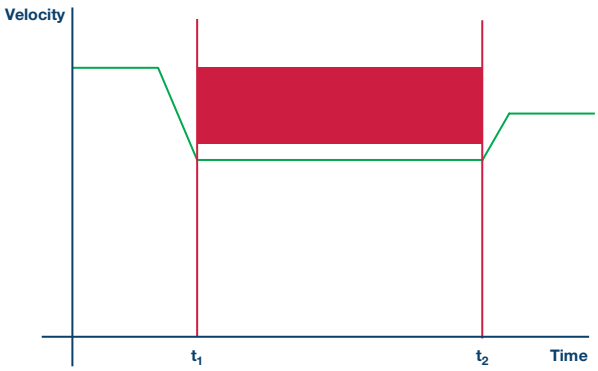


图2. 安全限制速度。

借助SLS安全子功能，可以监控电机的速度，如果超过了设定的水平，驱动器会使电机进入安全状态，通常是STO。这个安全子功能通常用于滚轴的清洗过程中，并与三位控制开关配合使用。图2显示了SLS在t_1处接合，在t_2处脱开。红色方块表示(如果进入)将导致驱动器进入安全状态的速度区域。

虽然IEC 61800-5-2不强制要求双通道安全，但大多数驱动器制造商也希望宣称符合ISO 13849的性能水平，因此双通道非常常见。

ISO 13849

ISO 13849是基于目前冗余的EN954标准的机器标准。与IEC 61800-5-2、IEC 61508和IEC 62061相比，它采用了性能水平(PL)，而不是SIL水平。水平为PLa至PLe。ISO 13849也明显偏好用双通道系统来实现更高的性能水平，因此必须使用三类或四类系统。ISO 13849使用DC (诊断覆盖率)作为诊断有效性的指标，而其他标准使用SFF作为指标。假设缺陷是50%安全/50%危险，则SFF和DC的关系可以用下面的方程式表示。

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

IEC 62061

IEC 62061是IEC 61508的机器解读。它实际上是ISO 13849的平行标准 — 事实上，ISO/IEC 17305将这两个机器标准结合在了一起。

在IEC 62061的范围中，它指出，“在此标准中，可以推测出复杂可编程电子子系统或子系统元件的设计符合IEC 61508的相关要求。此标准提供了SRECS的此类子系统和子系统元件的使用方法，而不是开发方法。”

IEC 61508

IEC 61508-2:2010包含了重要的IC要求，但是如果随意阅读或阅读部分标准，很容易漏掉这些要求。这些要求包括一个ASIC开发V模型，请参见IEC 61508-2:2010图3。V模型针对数字ASIC，它引用合成位置和路由以及最后的编码，但用一点想象力就可以把V模型解读为模拟或混合信号ASIC。

标题为“ASIC的技术和措施—避免系统故障”的附录F介绍了数字ASIC的首选项，并且注释1中指出，“以下技术和措施仅与数字ASIC和用户可编程IC相关。对于混合模式和模拟ASIC，目前没有提供通用技术和措施”。尽管存在限制，但是仍然可以完成混合信号ASIC的数字部分的检查清单，以及不适用于纯模拟IC的一些用途。

附录E的标题为“具有芯片冗余的集成电路(IC)的特殊架构要求。”同样，该附录说明了数字限制，它在E.1中指出，“下列要求仅与数字IC相关。对于混合模式和模拟IC，目前没有提供通用要求”。当其他标准中引用附录E时，往往忽视了关于附录E的另一个限制，即“此标准中使用的芯片冗余是指功能单元的成倍重复(或三倍重复)，以便实现大于零的硬件容错。”“重复”一词意味着相同的冗余，并且本文作者认为，其目标是可能使用同步技术的双核微指令。虽然大多数技术是有用的，但是当应用于各种冗余模块之间或一个模块与另一个芯片模块(用于对第一个模块进行诊断)之间的分离时，它们可能是多余的。复制的模块可能出现常见原因引起的故障，例如温度、ESD、电源故障和其他不太可能在同一时间以相同方式影响不同模块的因素。在ISO 13849-2:2012的D.2.4部分，可以找到引用附录E的方式，其指出，“因此，如果使用单个集成电路，不大可能实现满足2类、3类或4类的容错和/或检测要求所需要的多通道功能，除非它满足IEC 61508-2:2010附录E中的特殊架构要求。”IEC 61800-5-2 FDIS (2015年秋季)允许根据IEC 61508-2:2010附录E的要求，排除芯片短路，但是通过查看附录E您会发现，只有第f)和g)条直接指向芯片短路。第f)条要求独立模块之间的间距至少是流程最低设计规定的10倍，而第g)条仅讨论了相邻行的独立物理模块。

IEC 61508-2:2010的表A.1给出了计算SFF时假设的缺陷或故障。表A.2至A.14给出了典型诊断覆盖率的示例，可宣称为典型诊断，但是这些表有时需要解读为集成电路。IEC 62380的附录H和UL 1998的相关附录A更为详细，尤其是对数字微控制器和类似产品。

对于计算集成电路的FIT率，则引用了IEC 62380和SN29500以及其他来源。

该标准的2010年修订版中添加了考虑软错误的要求，并暗示了为易失性存储器(如RAM)添加ECC和奇偶校验，以便检测和控制尤其影响RAM的软错误。

ISO 26262要求

ISO 26262是IEC 61508派生出的汽车版本标准。它与IEC 61508的第2版同时开发，包含IEC 61508未提供的一些集成电路相关要求，并澄清了IEC 61508中的一些项目，但省略了其他要求。例如，ISO 26262-10:2012包含IEC 61508-2:2010的附录F和ISO 26262-5:2011的表D.1的汽车版本，它澄清了关于如何考虑汽车上的芯片短路的位置，“这里并不需要进行详尽的分析，例如并不需要对桥接故障进行详尽的分析，而桥接故障可能会影响微控制器或复杂PCB中的任何信号的任何理论组合。分析主要针对通过布局级别分析识别的重要信号或高度耦合的互连。”

第10部分特别包含了重点内容，比如“如果一个CPU面积占据了整个微控制器芯片面积的3%，则可以假设它的故障率等于总微控制器故障率的3%。”虽然此类流程是IEC 61508的自定义和实践部分，但是写出来也很有用。

ISO 26262的集成电路说明可作为ISO/TC 22/SC32中的ISO/AWI PAS 19451-1使用。

集成电路设计辅助

查看各项标准之后，作者提出了关于IC制造商如何协助驱动器制造商在驱动器中设计集成电路的许多建议。

首先，集成电路安全手册应该会对集成电路设计人员很有帮助。即使ASIC或设备未按照IEC 61508开发，也可以制作安全手册。

安全手册中的项目包括：

- 所使用的开发流程和生命周期模型。
- IEC 61508-2:2010的完整附录F检查清单。
- 假定任务说明。
- 根据IEC 62380和SN29500，以合理的平均工作温度预测FIT率，例如55°C，在24小时内的热循环温度为10°C。
- 芯片尺寸、芯片数量、RAM单元数量和晶体管数量，以便设计人员使用SN29500和IEC 62380计算他们自己的FIT率(如果计算已经完成并已给出计算的详细信息，则会更好)。
- 支持芯片分离的证据。
- 支持排除任何相关故障的证据。
- 芯片诊断的详细信息。
- 假定系统级诊断的详细信息。
- 给出λ_{DU}、λ_{DD}、λ_S的引脚FMEA，并针对查看预期封装故障模式的一组假设诊断计算SFF和DC的结果。
- 给出λ_{DU}、λ_{DD}、λ_S的引脚FME(D)A，并针对查看预期芯片故障模式的一组假设诊断计算SFF和DC的结果。
- 数据手册上显示的各种模块的FIT率，以便驱动器制造商重新进行FME(D)A。

鉴于数据的性质，安全手册可能只在签订NDA(保密协议)后提供。

与电机控制安全有关的部分，ADI公司目前正在开发安全手册，包括AD7403隔离式ADC和ADuM4135隔离式栅极驱动器。

其次，了解系统级设计的IC制造商可以帮助设计实现功能安全所需要的特性。例如：

- 知道只有一小部分PFH可用于IC，也许只有1%。
- 知道虽然一般来说功能安全越简单越好，但是在芯片上安装晶体管是非常可靠的，而且如果芯片上的晶体管数量增加10倍，则PCB上的组件将会减少，整体PFH将会下降。
- 知道芯片上的诊断可以比系统级诊断反应更快，可以帮助预防错误的积累。
- 知道驱动器的一般生命周期是20年，数据应该证明IC可以在给定的任务下匹配这一生命周期。
- 知道添加硬件加速器(如CRC引擎)可以减少软件负担。

第三，一系列建议架构显示了如何组合使用IC来实施IEC 61800-5-2的安全功能。可能涉及：

- 关于系统级诊断的建议。
- 关于适用组件的建议。
- 关于满足不同通道之间的独立要求的建议。
- 关于安全和非安全软件之间的软件独立性的建议，如果控制和安全可以组合到至少一个处理器上，则可以将所需要的处理器数从三个减少到两个。如果无法展现足够的独立性，则必须将一切事宜视为安全事宜。

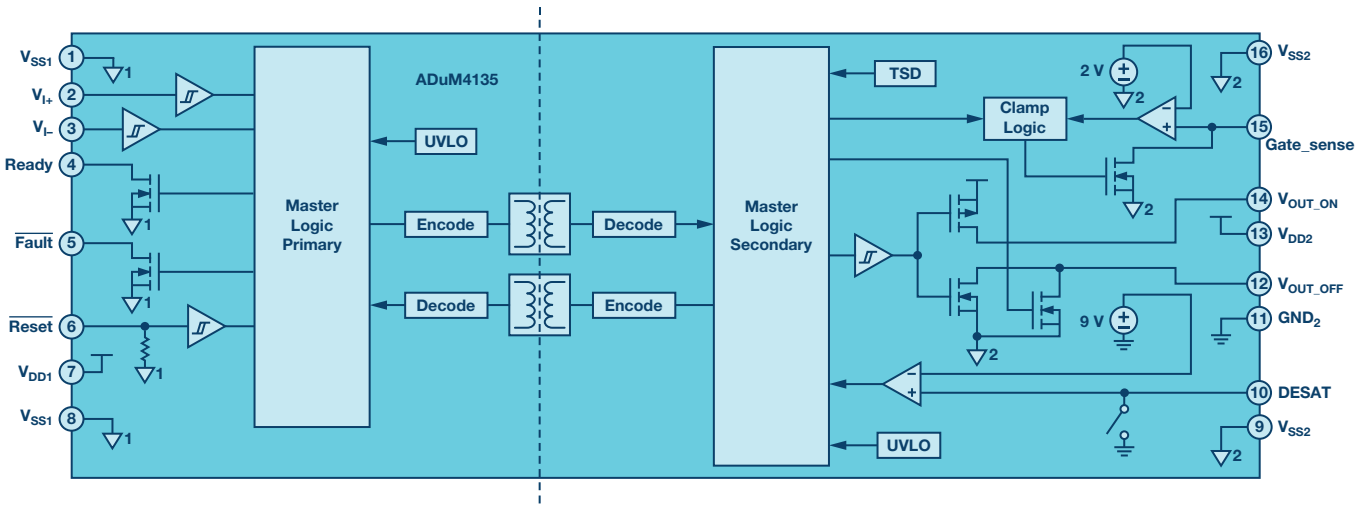
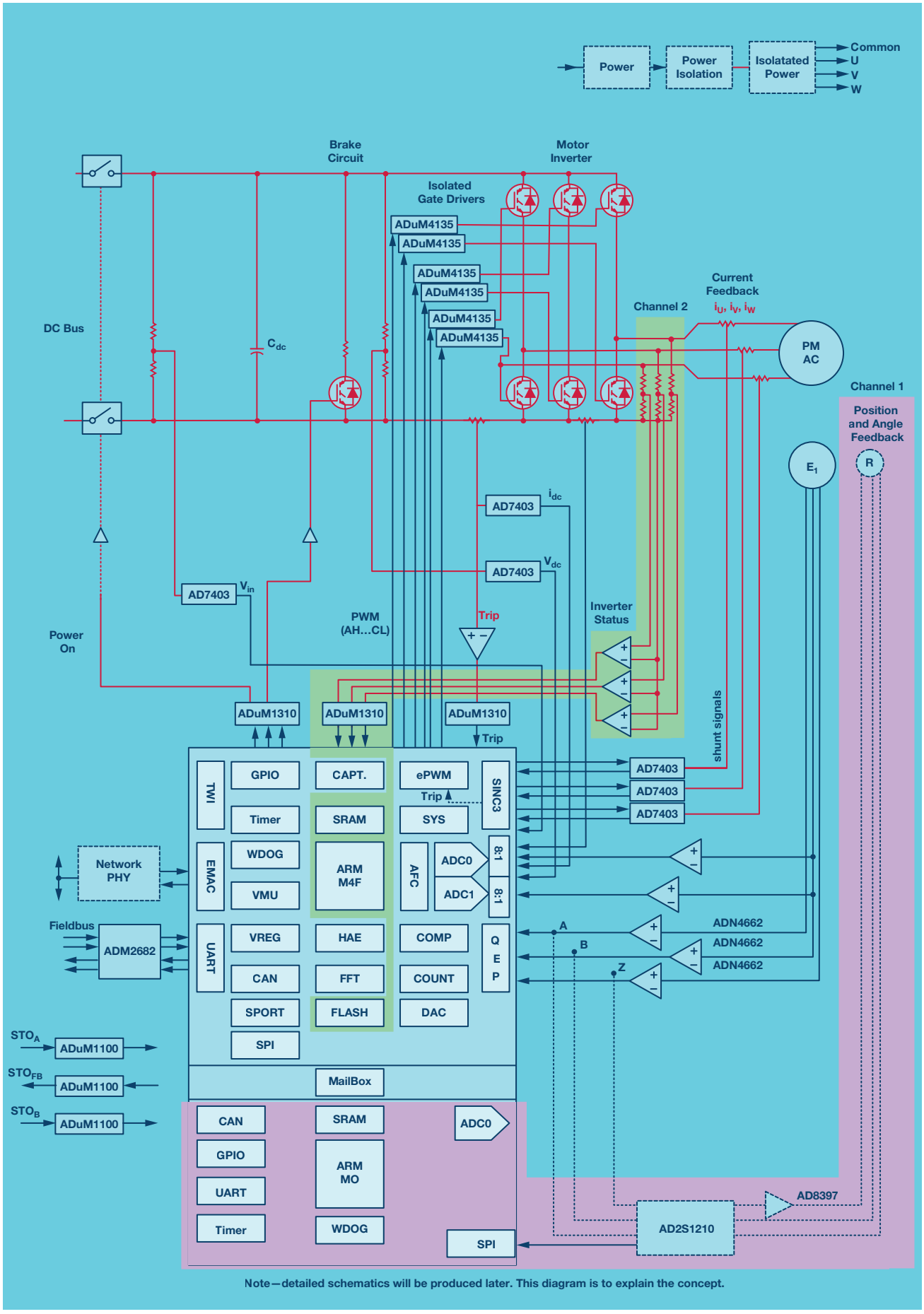


图3. ADuM4135隔离式栅极驱动器。



Note—detailed schematics will be produced later. This diagram is to explain the concept.

图4. 双通道概念架构，用于使用ADSP-CM419 (/8/7/6) DSP内核实施IEC 61800-5-2的SLS安全子功能。

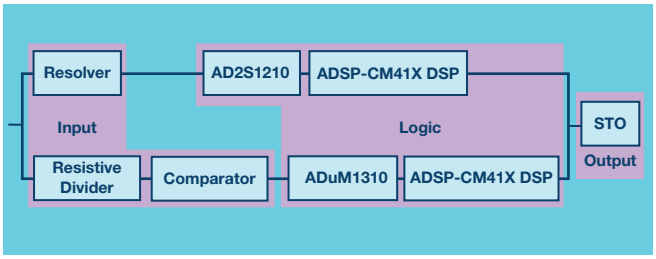


图5. SLS解读的可靠性模块图。

第四，为了澄清要求，应当引用标准。例如：

- 为了防止数据损坏，应当对将ADC连接到同一个PCB上的微控制器或DSP的SPI接口采取什么预防措施？IEC 61800-5-2:2006等标准让读者参考IEC 61508，进而参考电轨标准。IEC 61800-5-2的下一个版本添加了一些文本，用于澄清IEC 61784-3的要求不适用于此类接口，但是当作者阅读新标准中他自己的文字时，澄清并不像他所希望的那样清晰。EN 50402的最新标准草案做出了更好的澄清，它区分了空间上独立模块的信号传输与空间上不独立模块的信号传输。
- 澄清实施各种冗余的IC芯片独立要求。
- 澄清模拟和混合信号IC芯片独立要求。

第五，从标准中删除对特定解决方案的引用，因为这会导致一些读者认为这些是唯一的问题解决方案。例如，众所周知，光耦合器是实现信号隔离的一种传统方式，但与较新的数字隔离器相比，在可靠性、功率和速度方面有一些劣势。编辑ISO 13849和IEC 61800-5-2等标准，并将光耦合器的引用替换为更通用的术语，如电流隔离器，也将有助于采用更可靠的新型数字隔离器。2015年，IEC 61800-5-2的最新FDIS(终稿)已经这样做了。

结论

本文概括介绍了与机器和变速驱动器相关的主要功能安全标准。同时，得出了关于集成电路相关要求的结论。其中一个结论是，为了帮助满足功能安全IC要求，制造商可以提供更多附加信息和功能。本文列出了最重要的一些信息要点。第二个结论是，半导体制造商需要了解更多系统级要求，而ADI公司已开始着手分析自己的非功能安全、电机控制演示系统设计。目标是了解如何修改架构来满足功能安全要求，并了解缺少哪些信息，以便让我们的客户将我们的产品设计到符合功能安全要求的驱动器中。

参考文献

AD2S1210数据手册。

AD7403数据手册。

AD8397数据手册。

ADM2682数据手册。

ADSP-CM408F数据手册。

ADSP-CM41x混合信号控制处理器。

ADuM1310数据手册。

ADuM4135数据手册。

ADI公司电机控制网页：*http://www.analog.com/cn/motorcontrol*。

ADI公司功能安全计划：*http://www.analog.com/cn/about-adi/quality-reliability/functional-safety-program.html*。

BGIA报告2/2008e，机器控制的功能安全—EN ISO 13849的应用。

IEC 61508-2:2010，电气/电子/可编程电子安全相关系统的功能安全—第2部分：电气/电子/可编程电子安全相关系统的要求。

IEC 61800-5-2:2007, 可调速电力驱动系统，安全要求，功能安全。

IEC 62061:2005，机器安全—电气、电子和可编程电子控制相关系统的功能安全。

ISO 13849-1:2006，机器安全—控制系统的安全相关部分—第1部分：一般设计原则。

ISO 13849-2:2012，机器安全—控制系统的安全相关部分—第2部分：验证。

ISO 26262:2011，道路车辆—功能安全。

作者简介

Tom Meany是八项美国专利的持有者，并且是ISA和IEEE的高级成员。Tom是一位应用领域机器的FS工程师(莱茵公司)，获得了Technis的可靠性和功能安全方面的认证。他也是IEC SC22G/MT12的成员，负责IEC 61800-5-2的二稿(变速驱动器的功能安全要求)。Tom于1987年加入ADI公司，目前担工业产品的功能安全技术专家职位。

全球总部
One Technology Way
P.O. Box 9106, Norwood, MA
02062-9106 U.S.A.
Tel: (1 781) 329 4700
Fax: (1 781) 461 3113

大中华区总部
上海市浦东新区张江高科技园区
祖冲之路 2290 号展想广场 5 楼
邮编 : 201203
电话 : (86 21) 2320 8000
传真 : (86 21) 2320 8222

深圳分公司
深圳市福田中心区
益田路与福华三路交汇处
深圳国际商会中心
4205-4210 室
邮编 : 518048
电话 : (86 755) 8202 3200
传真 : (86 755) 8202 3222

北京分公司
北京市海淀区
西小口路 66 号
中关村东升科技园
B-6 号楼 A 座一层
邮编 : 100191
电话 : (86 10) 5987 1000
传真 : (86 10) 6298 3574

武汉分公司
湖北省武汉市东湖高新区
珞瑜路 889 号光谷国际广场
写字楼 B 座 2403-2405 室
邮编 : 430073
电话 : (86 27) 8715 9968
传真 : (86 27) 8715 9931

TA14491sc-0-9/16

analog.com/cn

ANALOG DEVICES
超越一切可能™