集成电路的功能安全

Tom Meany
ADI公司

摘要

集成电路(IC)是所有现代安全系统的根本。集成电路提供逻辑，控制传感器，从很大程度上看，其本身就是传感器。集成电路驱动最终元件以实现安全状态，它们是软件运行的平台。半导体内部的高集成度可以简化系统级实现，其代价是IC内部复杂性增加。这种集成会减少器件数量，改善系统可靠性，并为提高诊断覆盖率和缩短诊断测试间隔创造机会——所有的这些都是为了达到安全的同时成本可接受。有人可能会认为，由于复杂性增加，这种高集成度是一件坏事。然而，虽然集成电路复杂性提高，但在模块和系统层面上可以大大简化。令人吃惊的是，过程控制、机械、电梯、变速驱动器和有毒气体传感器都有相应的功能安全标准，但关于集成电路却没有专门的功能安全标准。相反，相关要求和知识是零散地分布在IEC 61508和其他B级、C级标准中。本文为解读现有半导体功能安全标准提供指导。

简介

通常，集成电路按照IEC 61508或ISO 26262标准进行开发。另外，二级和三级标准中有时还会有其他要求。只有按照功能安全标准进行开发和评估，才能让人放心这些复杂的集成电路足够安全。当编写IEC 61508时，其针对的是定制系统，而不是开放市场批量生产的集成电路。本文将回顾并评论集成电路的已知功能安全要求。虽然本文集中讨论IEC 61508及其在工业领域的应用，但很多内容都与汽车、航空电子和医疗等应用有关。

功能安全

功能安全是安全性的一部分，用以应对安全相关系统的可靠性需求。功能安全不同于其他被动形式的安全，如电气安全、机械安全或本质安全。

功能安全是一种主动形式的安全。例如，它能确保马达以足够快的速度关闭，防止对打开防护门的操作员造成伤害，或者当有人在附近时，机器人会降低运行的速度和力度。

标准

主要功能安全标准是IEC 61508 [1]。该标准的第一版于1998年出版，第二版于2010年出版，并于2017年开始更新至第三版的工作，可能的完成日期是在2022年。自从1998年公布IEC 61508第一版以来，基本IEC 61508标准已针对不同领域进行适应性修改，例如汽车(ISO 26262)、过程控制(IEC 61511)、PLC (IEC 61131-6)、IEC 62061（机械）、变速驱动器(IEC 61800-5-2)以及其他许多领域。此类标准有助于对非常宽泛的IEC 61508进行解释以便用于这些受到更大限制的领域。

一些功能安全标准，例如ISO 13849和D0-178/D0-254，并非衍生自IEC 61508。尽管如此，任何熟悉IEC 61508并阅读这些标准的人都不会对其内容感到过于吃惊。

在安全系统内，当系统运行时，执行关键功能安全活动的是安全功能。安全功能定义了实现或保持安全所必须执行的操作。典型的安全功能包含输入子系统、逻辑子系统和输出子系统。通常，这意味着对潜在的不安全状态进行检测，并且基于检测到的值做出决定，如果认为有潜在危害，则指示输出子系统将系统置于已定义的安全状态。

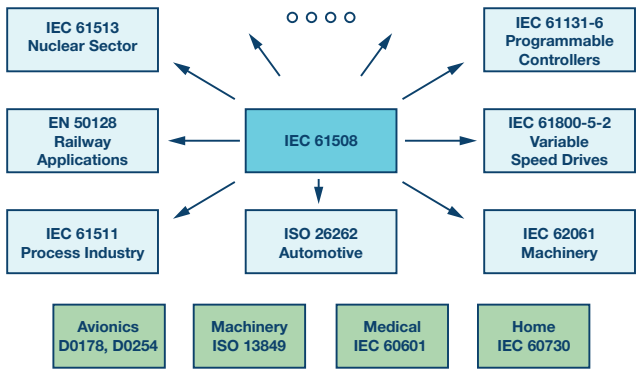

图1. 功能安全标准示例。

从不安全状态出现到进入安全状态所用的时间至关重要。例如，安全功能可能包括如下器件：一个传感器用来检测机器上的防护装置是否打开，一个PLC用来处理数据，以及一个具有安全扭矩关闭输入的变速驱动器，应该在插入机器中的手可能接近运动部件之前关闭电机。

安全完整性等级

SIL代表安全完整性等级，是表示需要将风险降至何种程度才能达到可接受水平的手段。根据IEC 61508标准，安全等级有1、2、3、4四级，从一个级别到下一个级别，安全性会提高一个数量级。机器和工厂自动化场景中不会看到SIL 4，因为一般情况下，这种场合中遭受危险的人员通常不会超过一个。SIL 4针对的是数百甚至数千人可能受到伤害的核能和铁路等应用。还有其他功能安全标准，例如汽车使用ASIL（汽车安全完整性等级）A、B、C和D，以及ISO 13849标准。其性能等级a、b、c、d和e可以对应到SIL 1至SIL 3尺度。

表1. 各应用领域安全等级的粗略对应

IEC 61508 SIL	ISO 26262 ASIL	航空电子级别	ISO 13849 PL	核类别
1	A	D	b	A
2	B	C	c	A
3	C/D	B	d	A
4	—	A	e	C

笔者不相信单个IC可能有超过SIL 3的安全水平。但值得注意的是，IEC 61508-2:2010附录F中的表格显示了一个SIL 4列。

三项关键要求

功能安全对IC开发提出了三项关键要求。下面研究这些要求。

要求1—遵循严格的开发流程

IEC 61508是一个全生命周期模型，涵盖了从安全概念到需求采集、维护，直至最终废弃处理的所有阶段。不是所有这些阶段都与集成电路相关，甄别哪些阶段有关需要培训和经验。IEC 61508为ASIC提供了一个V模型，另外还有审查、审核及其他要求，它代表了一个体系，虽然不能保证安全，但过去已证明它能指导我们设计制造出安全的系统和IC。

由于更改有缺陷的集成电路的成本很高，所以大多数IC制造商已经建立严格的新产品开发标准。对于小几何尺寸工艺，仅仅一套掩膜的成本就可能超过50万美元。这种情况加上长交货期，迫使集成电路设计商不得不实施严格的开发流程和进行严谨的检查与验证。功能安全的一大区别在于，不仅必须实现安全性，还要证明安全性，即使是最好的IC制造商也需要在其正常开发流程之上添加安全流程，以确保用来证明合规性相应的证据得以创建并存档。

开发流程引入的故障称为系统故障。这些故障只能通过设计变更来解决。与需求采集相关的故障、EMC鲁棒性不足和测试不充分就是此类故障。

IEC 61508-2:2010的附录F列出了一系列专门测量，IEC委员会专家认为这些测量适合用于集成电路开发。表F.2适用于FPGA和CPLD，表F.1适用于数字ASIC。这些测量分为R（推荐）或HR（强烈推荐）两类，具体取决于SII，某些情况下还提供了备选技术。对于拥有良好开发流程的IC供应商来说，其中的要求很少会让人感到意外，但SIL 3的99%故障覆盖率要求是有挑战性的，尤其是对于小型数字或混合信号器件，其中很多电路位于模块的外围。该标准第二版中的要求仅适用于数字IC，但许多要求也可应用于模拟或混合信号IC（ISO 26262的下一版本将包含类似表格，并有针对模拟和混合信号集成电路的版本）。

除表F.1和表F.2外，还有一些介绍性文字也提供了一些见解。例如，这个介绍性文字说允许使用经过实际验证的工具，在复杂度相似的项目中使用18个月是合理的时间长度。这意味着并不需要应用IEC 61508-3关于工具的全部要求。

如果模块/系统设计者过去曾成功使用某一IC，并且了解其应用和现场故障率，那么他可以宣称其“经过实际验证”。对于集成电路设计者或制造商来说，作出这种宣称要困难得多，因为他们一般不太了解最终应用或拥有完备的现场失效器件收集、失效分析流程及数据。

软件

所有软件错误都是系统性的，因为软件不会老化。任何片内软件都应考虑IEC 61508-3的要求。通常，片内软件可能包括微控制器/DSP的内核/引导程序。但在某些情况下，微控制器/DSP可能包含一个由IC制造商预编程的小型微控制器来实现一个逻辑块，而不是使用状态机。该预编程的微控制器软件还需要符合IEC 61508-3的要求。应用级软件通常是模块/系统设计者的责任，而不是IC制造商的责任，但IC供应商可能需要提供编译器或低级驱动程序等工具。如果这些工具用于安全相关应用软件的开发，那么IC制造商需要为最终用户提供足够的信息，以满足IEC 61508-3:2010第7.4.4条中的工具要求。

笔者也使用C语言和其他很多编程语言做过编程。笔者还做过少量Verilog编程。Verilog及其姊妹语言VHDL是用于设计数字集成电路的两种代表性硬件定义语言(HDL)。一个有趣的问题是HDL是否是软件，但现在遵循IEC 61508-2:2010附录F就足够了。在实践中，笔者发现如果遵循附录F，那么结合IEC 61508的其他要求（生命周期阶段等），HDL是否是软件的问题并不重要，因为开发者最终仍要完成所有必需的任务。一个值得注意的相关标准是IEC 62566[2]，它处理的是利用HDL开发的核工业安全功能。

要求2—固有可靠性

IEC 61508以PFH（每小时危险故障平均频率）或PFD（需要时发生故障的概率）的形式提出了可靠性要求。这些限制与成年人因自然原因而死亡的风险，以及人们认为工作或处理日常业务不应显著增加这一风险的想法有关。SIL 3安全功能的最大PFH为10^{-7}/h，或者每1000年约有一次的危险故障率。表示为FIT（故障次数/每运行十亿小时的故障率）的话，即为100 FIT。

鉴于典型的安全功能有一个输入模块、一个逻辑模块和一个执行器模块，并且PFH预算必须分配给所有三个模块，所以某一IC的PFH完全可能是个位数(<10 FIT)。可以使用冗余架构来提高这些数字，若有两个100 FIT结构，则每个可以提供相同的置信度，使模块可靠性达到10 FIT（受常见原因故障(CCF)限制）。然而，冗余会消耗大量空间和能量，并增加成本。

ADI公司之类的IC制造商在网站上（例如*analog.com/reliabilitydata*）提供其所有已发布IC的基于加速寿命测试的可靠性信息。此信息有时会不被重视，因为这种可靠性评估是在人为条件下于实验室中完成的。推荐使用行业标准，如SN 29500 [3]或IEC 62380 [4]，但这些标准有一些问题：

- 它们预测99%置信度下的可靠性，IEC 61508仅要求70%置信度下的数据，因此标准偏悲观。
- 它们将随机故障模式和系统故障模式混为一谈。根据IEC 61508的规定，应以不同方式处理这些故障模式。
- 它们不是经常更新。
- 它们未考虑不同供应商之间的质量差异。

SN 29500之类的标准说明的是片内晶体管的可靠性。如果使用两个IC（每个有50万个晶体管）来实现安全功能，每个IC的FIT为70，那么整个系统的FIT为140。但是，如果用一个含100万个晶体管的IC来替代这两个IC，那么这一个IC的FIT只有80，减少了40%以上。

IC内部的软错误往往被忽略。软错误不同于传统的可靠性预测，因为一旦断电再通电，软错误就会消失。引起软错误的原因是空间中的中子或封装材料中的 粒子，它们撞击片内RAM单元或触发器(FF)，改变其中存储的值。ECC（双比特错误检测和单比特错误纠正）可用来检测并无缝纠正RAM中的错误，但代价是速度降低和片内错误增多。奇偶校验增加的开销更少，但系统设计人员需要解决错误恢复问题。如果不使用奇偶校验或ECC技术，则软错误率可能会比传统硬错误率高出多达1000倍（IEC 61508提供的RAM数值为1000 FIT/MB）。用于解决实现逻辑电路的FF（触发器）中软错误的技术不那么令人满意，但看门狗定时器、计算中的时间冗余以及其他技术可提供帮助。

要求3—容错性

无论产品有多可靠，有时候还是会出事。容错性承认这一现实并予以解决。容错性主要包含两方面。一个是使用冗余，另一个是使用诊断。从这两方面看，无论IC的可靠性或IC开发流程有多好，故障难免会发生。

冗余可以是相同的或不同的，可以在片内或片外。IEC 61508-2:2010的附录E提供了一组技术来证明，已经采取了充分的措施来支持关于数字电路使用相同冗余的片内冗余性声明。附录E似乎是针对双锁步微控制器的，针对以下方面的片内独立性没有给出任何指导：

- 模拟和混频信号集成电路
- 模块与其片内诊断之间
- 采用不同冗余的数字电路

但在某些情况下，可以针对这些情况对附录E加以灵活解释。附录E中有一个有意思的内容是β_{IC}计算，其衡量片内常见原因故障。通过它可以判断间隔是否足够，前提是常见原因故障的来源所代表的 小于25%，这与IEC 61508-6:2010的表格中的1%、5%或10%相比是较高的。

诊断是集成电路真正可以大放异彩的领域。片内诊断可以：

- 通过设计来适应片内模块的预期失效模式（在功能安全领域会更好）
- 不增加PCB空间，因为外部引脚需求有限
- 以高速率运行（最小化诊断测试间隔）
- 无需冗余器件来通过比较进行诊断

这意味着片内诊断可以最大限度地减少系统成本和面积。一般而言，诊断功能模块相对于其监控的片内模块具有多样性（不同的实现方式），因此它们不太可能以与被监控模块相同的方式和同时发生故障。当这种情况发生时，它们遇到的很可能是同样的问题（常常与EMC、电源问题和温度过高有关），哪怕诊断功能是在单独的芯片上实现。虽然该标准不包含此要求，因为片内电源监视器和看门狗电路是最后的诊断手段，所以存在对于使用片内电源监视器和看门狗电路的担忧。某些外部评估人员会坚持将此类诊断放在片外。

一般来说，对较简单集成电路的诊断将由远程微控制器/DSP控制，测量在片内完成，但结果发送到芯片外进行处理。

IEC 61508有最低级别诊断覆盖率的要求，用SFF（安全失效比率）给出，其考虑安全故障和危险故障，与忽略安全故障的DC（诊断覆盖率）相关但不同。已实施诊断的成功程度可以使用量化FMEA或FMEDA来衡量。但是，在IC中实施的诊断也可以覆盖IC外部的器件，IC内的模块可以通过系统级诊断来覆盖。当IC开发人员执行FMEDA时，必须将基于一定假设的最终应用场景告知IC开发人员。在ISO 26262术语中，这被称为SEooC（独立安全单元）。对于要利用IC级FMEDA的最终用户，他们必须确信上述假设对其系统仍然成立。

虽然IEC 61508-2:2010的表A.1（实际上是表A.2至A.14）就IC失效提供了很好的指导，分析IC时应予以考虑，但IEC 60730:2010 [5]的附录H就该主题提供了更好的论述。

集成电路的开发方案

开发用于功能安全系统的集成电路有几种方案。标准中没有要求只能使用符合标准的集成电路，而是要求模块或系统设计人员确信所选的集成电路适用于目标系统。

可用方案包括：

- 方案1：完全依照IEC 61508标准进行开发，使用外部评估和安全手册
- 方案2：依照IEC 61508标准进行开发，无外部评估，但有安全手册
- 方案3：依照半导体公司的标准开发流程进行开发，但会发布安全数据手册
- 方案4：依照半导体公司的标准流程进行开发

注意：未依照IEC 61508开发的器件，其安全手册可能被称为安全数据手册或类似名称，以避免与遵照安全手册开发的器件发生混淆。

对于半导体制造商来说，方案1成本最高，但对模块或系统设计商来说可能最有利。拥有这样一个器件，其中集成电路安全概念中显示的应用与系统的应用相匹配，可以降低模块或系统进行外部评估时遇到问题的风险。SIL 2安全功能的额外设计工作量可能在20%或更多。即使没有功能安全，半导体制造商通常也已经实施了严格的开发流程，而且额外工作量可能会更多。

方案2节省了外部评估的成本，但其他方面的影响相同。如果客户无论如何都要让模块/系统进行外部认证，并且集成电路是该系统的重要组成部分，那么此方案是合适的。

方案3最适合于已经发布的集成电路，提供安全数据手册可以让模块或系统设计人员获得其在更高级别上进行安全设计所需的额外信息。这包括如下信息：所用实际开发流程的详细信息，集成电路的FIT数据，任何诊断的详细信息，以及制造现场的ISO 9001认证证据等。

然而，方案4仍然是开发集成电路最常用的方法。使用此类器件开发安全模块或系统，将需要额外的器件和开支用于模块/系统设计，因为这些器件没有充分的诊断能力，需要双通道架构以资比较，而不是单通道架构。若没有安全数据手册，模块/系统设计人员还需要做出保守的假设，并将集成电路视为黑盒子。

此外，半导体公司需要制定自己对标准的解释，笔者自己的公司为此开发了内部文件ADI61508和ADI26262。ADI61508采用了IEC 61508:2010的七个部分，并根据集成电路开发解释了相关要求。

SIL 2/3开发

有时候，集成电路可以依照SIL 3的所有系统要求进行开发。这意味着IEC 61508-2:2010表F.1针对SIL 3的所有相关项目都得到遵守，并且所有设计评审和其他分析都按照SIL 3级要求完成。但是，硬件度量标准可能只对SIL 2来说是够好的。这种电路可以被标识为SIL 2/3或更典型的SIL M/N，其中M表示根据硬件度量标准可以声明的最高SIL级别，N表示根据系统要求可以声明的最高SIL级别。两个SIL 2/3集成电路可用来实现SIL 3模块或系统，因为根据硬件度量标准，两个SIL 2项目并联就会将该组合升级到SIL 3，但就系统要求而言，各项目已经是SIL 3。如果集成电路仅是SIL 2/2，那么将两个这样的集成电路并联不会使其成为SIL 3，因为其充其量不过是SIL 3/2。

将硬件度量标准应用于集成电路

除了几乎全部安全功能都由集成电路实现的情况之外，很难为半导体指定SFF、DC或PFH限值。以SFF为例，SIL 3要求SFF大于99%，这适用于完整安全功能，而不只是集成电路。如果集成电路为98%，仍然可以利用它来实现SIL 3安全功能，但系统的其他部分需要实现更高的覆盖率以进行补偿。集成电路的安全手册或安全数据手册需要公布λ_{DD}、λ_{DU}和λ以用于系统级FMEDA。

理想情况下，IC要求是在系统级分析中导出的，但通常情况并非如此，开发实际上是一个SEooC（参见ISO 26262，独立安全单元）。在SEooC的情况下，IC开发者需要假设IC在系统中将会如何使用。然后，系统或模块设计者必须将这些假设与实际系统进行比较，以确定IC的功能安全性对系统是否足够。这些假设可以决定诊断是在IC上实施，还是在系统级实施，并因此影响IC级特性和功能。

保密性(Security)

系统的安全性与保密性密不可分。目前，IEC 61508或ISO 26262中与保密性有关的唯一指导是让读者参考IEC 62443系列[6]。但是，IEC 62443似乎更多地是针对较大的组件，例如整个PLC组件，而不是单个IC。好消息是，功能安全标准中消除系统故障的大部分要求也适用于保密性。没有任何参照是很有趣的，因为在某些情况下，硬件可以提供硬件信任根和类似PUF（物理上不可克隆的功能）的功能，这对于安全性和保密性十分重要。

结论

现有IEC 61508涵盖了从集成电路开发到炼油厂的一切。虽然针对机械和过程控制等领域有专门的行业专用标准，并且IEC 61508第二版中有关于集成电路的一些指导，但针对集成电路并无专用标准。缺乏具体要求导致要求被任意解释，因此不同客户和外部评估人员的期望之间可能出现冲突。

这意味着，各行业将倾向于按照更高层次的标准对集成电路提出行业特定的要求。这样的要求已经可以在EN 50402 [7]等标准中看到，但最特别的是ISO 26262的2016版草案[8]中，其中新增的第11部分专门处理集成电路。

笔者希望将于2021年左右发布的IEC 61508第三版会扩充和澄清关于集成电路的指导意见。笔者很幸运能够加入IEC TC65/SC65A MT61508-1/2和MT 61508-3起草团队，得以有机会参与此类工作。也许未来的修订版会有专门针对半导体的第8部分，以便各行业之间保持一致，使得所开发的集成电路能够满足所有行业的要求。

即便如此，该标准也不太可能包含IC制造商设计满足功能安全要求的IC所需的一切。与保密性、EMC等相关的要求仍然需要从系统应用知识中衍生出来。

参考文献

[1] IEC 61508:2010：电气/电子/可编程电子安全相关系统的功能安全。国际电工委员会，2010年。

[2] IEC 62566:2012：*核电站—事关安全的仪器仪表和控制—执行A类功能的HDL编程集成电路的开发*。国际电工委员会，2012年。

[3] SN 29500-2：集成电路的期望值。Siemens，2010年。

[4] IEC TR 62380:2004：可靠性数据手册—电子元件、PCB和设备的可靠性预测的通用模型。国际电工委员会，2004年。

[5] IEC 60370-1:2010：家用和类似用途的自动电气控制—第1部分：一般要求。国际电工委员会，2010年。

[6] ISA/IEC 62443：*工业通信网络—网络和系统安全*。国际自动化协会和国际电工委员会。

[7] EN 50402:2016：*用于检测和测量可燃或有毒气体或蒸汽或氧气的电气装置—气体检测系统的功能安全要求*。欧洲标准委员会—电气，2016年。

[8] ISO 26262:2011：道路车辆功能安全。国际标准化组织，2011年。

作者简介

Tom是ADI公司30年的资深员工，拥有电子学一级学士学位和应用数学与计算机一级硕士学位。Tom持有8项美国专利，并且是经过认证的机械领域TÜV莱茵功能安全工程师。Tom是功能安全领域多个IEC工作组的成员，包括与IEC 61508-2、IEC 61508-3和IEC 61800-5-2相关的工作组。联系方式：*tom.meany@analog.com*。

在线支持社区

访问ADI在线支持社区，与ADI技术专家互动。提出您的棘手设计问题、浏览常见问题解答，或参与讨论。

EngineerZone™
ANALOG DEVICES 中文技术论坛

请访问*ezchina.analog.com*

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

TA16603sc-0-2/18

analog.com/cn

ANALOG DEVICES
超越一切可能™