解决方案

功能安全系统及ADI工业功能安全监控器解决方案

随着工业自动化4.0时代的到来，功能安全的重要性不言而喻，它所提供的更准确诊断和更高强韧性确保了工厂机器自主运行时的可靠性。自动化安全是智能的前提，也是未来工厂的基本要素，功能安全发挥着举足轻重的作用。

本文从多个维度对功能安全系统进行了阐述，首先介绍了工业领域功能安全执行的标准及相关含义、系统及完整性等级(SIL)；其次阐述了系统能力、可靠性预测和架构约束这三项满足SIL合规性的关键要求；第三部分就监控器件如何依据IEC 61508标准实现功能安全进行了分析，同时讲解了监控器作为诊断功能和安全功能的应用案例；最后介绍了工业功能安全器件的四大分类及特点，FS-Enabled、FS-Evaluated、FS-Compliant和FS-Certified。期望通过本文的全面分析，助力使用者对功能安全系统有充分的了解和认知，设计出高可靠性的产品。

功能安全概述

传感器是物理世界与数字世界的桥梁，通过传感器从物理环境采集数据并发送至处理器，处理器对数据进行过滤或聚合后发送至集中式云数据中心来进行更深入的计算，这样的数据路径主要是传统边缘计算不具备执行复杂分析的能力。随着智能边缘的发展，传统方式也见证着一场变革，就是说无需将所有数据传输至云端，而是通过人工智能和机器学习的结合使设备在数据中学习并在本地自主做出决策。显而易见，技术进步带来了诸多优势，同时也凸显了功能安全的必要性。

功能安全目标

预防故障或故障发生时将系统置于安全状态来保障系统的安全运行，这是普通意义的功能安全目标，也是执行时达成的方向。系统运行时存在系统性和随机性两种类型的故障，故障发生后要么通过安全方式关闭系统使其停止运行，要么让系统具备容错能力而在故障状态继续运行。

可控制的故障被称为系统性故障，是开发、设计及项目配置过程中出现的典型错误，比如选择了错误的元件或采用了不完善的验证策略或系统中存在的软件漏洞而造成的故障。针对这类故障采取的措施包括严格的流程开发，遵循IEC 61508等标准及相关编码规范，整个开发过程中开展严格的评审工作。系统性故障一般通过完善的质量管理进行预防，包括ADI在内的许多制造企业都是通过获取质量管理体系(QMS)认证来实现这一目标。

随机性故障是设备运行过程中出现的硬件故障，由硬件中一种或多种可能的退化机制引发，包括电阻或电容老化或者焊点失效等，这类故障发生的概率可预测。虽然能够预估硬件老化和导致故障的概率，但却无法预判具体的发生时间。一般在系统中实施诊断与冗余设计来对这类故障进行检测和预防，以便需要时将设备控制在安全状态。

功能安全标准

IEC61508是工业应用领域执行的功能安全标准，它为电子系统在规范、设计和运行方面制定了全面的要求。汽车领域使用的ISO26262标准及其它许多行业和产品安全标准都源于IEC61508。图1列出了全面的执行标准，ADI在现有严格的新产品开发流程基础上全面采纳该标准，确保在设计过程中实施所要求的安全规划、安全分析、验证和确认工作，降低产品的系统性故障风险，赢得客户的信任，确保客户的安全需求。

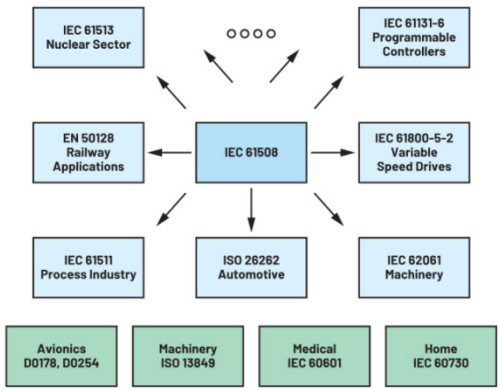

图1 功能安全标准

合规性是获得公众认可、提升产品安全性、降低法律与财务风险的必要条件，合规性涉及如下一些概念：

安全系统、安全功能、安全完整性等级(SIL)

1. 安全系统

安全系统是对安全功能的具体实现方案，通过执行必要的功能来保障安全的系统，一个系统中会包含一项或多项安全功能。

2. 安全功能

安全功能是系统针对特定危险所实现的功能，具备的能力包括通过传感器或类似的输入子系统进行检测；通过逻辑求解器进行决策；通过断路器或最终执行元件采取行动。

3. 安全完整性等级(SIL)

安全完整性等级(SIL)用于规定安全系统所需安全功能的安全完整性要求，采用分级形式进行表征。每项安全功能都有对应的安全完整性等级，本质上体现了安全功能在风险管控方面的表现。SIL等级越高，故障风险则越低，SIL-4的可靠性最高。设计高SIL系统的复杂性可能导致成本过高，有时甚至并无必要，因此等级设计由安全功能的重要性决定，实施安全要求时需要在成本与复杂性之间找到平衡。

SIL合规需突破的三大设计壁垒是系统能力、SIL要求及可靠性预测和架构约束，如图2维恩图所示。

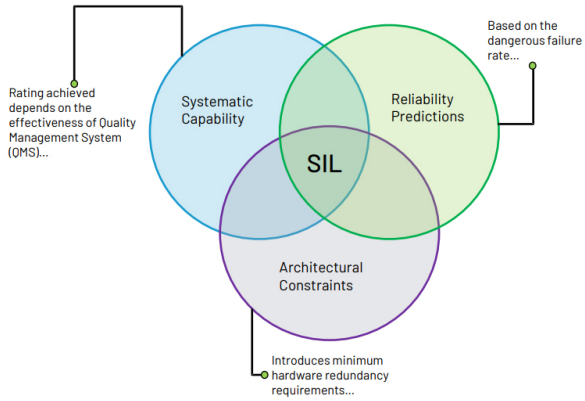

图2 SIL维恩图

a. 系统能力

系统能力也称为系统完整性，它是影响合规性的第一个因素，是抵御系统性故障的防护水平。系统能力的主要思想是确保系统在设计与构建时能够实现故障的规避与控制，核心思路是遵循严格的设计流程并实施质量管控，避免系统软件或硬件出现错误。IEC 61508标准明确规定了多种控制系统性故障的技术与措施。

表1示例的两个表格A-16和B-1为工程师的设计提供了指导，帮助开发出以安全为首要原则且符合相关安全标准的系统。

A表格中绿色框要求采取的措施包括电压击穿、电压波动、过/欠电压，这也正是电压监控器的应用场景。B表格中绿色框提到对程序序列的监控，这一功能通过看门狗定时器来实现。通过B表格要求可以完善文档记录，示例的检查清单和结构化规范共同构成了安全理念。安全理念是一套全面的计划，确保故障发生时系统安全运行的策略与措施，包括安全目标、危险分析与风险评估(HARA)、安全要求、安全机制以及验证与确认计划。

表1 系统能力示例

Table A.16 – Techniques and measures to control systematic failures caused by environmental stress or influences

	Technique/measure	See IEC 61508-7	SIL 1	SIL 2	SIL 3	SIL 4
	Measures against voltage breakdown, voltage variations, overvoltage, low voltage and other phenomena such as a.c. power supply frequency variation that can lead to dangerous failure	A.8	M low	M medium	M medium	M high
	Separation of electrical energy lines from information lines (see Note 4)	A.11.1	M	M	M	M
	Increase of interference immunity	A.11.3	M low	M low	M medium	M high
	Measures against the physical environment (for example, temperature, humidity, water, vibration, dust, corrosive substances)	A.14	M low	M high	M high	M high
	Program sequence monitoring	A.9	HR low	HR low	HR medium	HR high
	Measures against temperature increase	A.10	HR low	HR low	HR medium	HR high
	Spatial separation of multiple lines	A.11.2	HR low	HR low	HR medium	HR high
	Idle current principle (where continuous control is not needed to achieve or maintain a safe state of the EUC)	A.1.5	R	R	R	R
	Measure to detect breaks and shorts in signal lines		R	R	R	R
	Failure detection by on-line monitoring (see Note 5)	A.1.1	R low	R low	R medium	R high
	Tests by redundant hardware	A.2.1	R low	R low	R medium	R high
	Code protection	A.6.2	R low	R low	R medium	R high
	Antivalent signal transmission	A.11.4	R low	R low	R medium	R high
	Diverse hardware (see Note 6)	B.1.4	– low	– low	– medium	R high
	Software architecture	7.4.3 of IEC 61508-3	See Tables A.2 and C.2 of IEC 61508-3			

Table B.1 – Techniques and measures to avoid mistakes during specification of E/E/PE system design requirements (see 7.2)

	Technique/measure	See IEC 61508-7	SIL 1	SIL 2	SIL 3	SIL 4
	Project management	B.1.1	M low	M low	M medium	M high
	Documentation	B.1.2	M low	M low	M medium	M high
	Separation of E/E/PE system safety functions from non-safety functions	B.1.3	HR low	HR low	HR medium	HR high
	Structured specification	B.2.1	HR low	HR low	HR medium	HR high
	Inspection of the specification	B.2.6	– low	HR low	HR medium	HR high
	Semi-formal methods	B.2.3, see also Table B.7 of IEC 61508-3	R low	R low	HR medium	HR high
	Checklists	B.2.5	R low	R low	R medium	R high
	Computer aided specification tools	B.2.4	– low	R low	R medium	R high
	Formal methods	B.2.2	– low	– low	R medium	R high

All techniques marked "R" in the grey shaded group are replaceable, but at least one of these is required.

For the verification of this safety lifecycle phase, at least one of the techniques or measures shaded grey in this table or listed in Table B.5 shall be used.

NOTE 1 For the meaning of the entries under each safety integrity level, see the text preceding this table.

NOTE 2 The measures in this table can be used to varying effectiveness according to Table B.6, which gives examples for low and high effectiveness. The effort required for medium effectiveness lies somewhere between that specified for low and for high effectiveness.

NOTE 3 The overview of techniques and measures associated with this table is in Annex B of IEC 61508-7. Relevant subclauses are referenced in the second column.

ADI拥有ISO9001质量管理体系认证以确保产品开发流程符合多项标准要求。系统能力分为SC1到SC4四个等级，其中SC4代表最高置信等级。系统能力是对安全系统的质量检验，确保其在设计与构建过程中能够有效规避和管理错误，从而可靠地保障安全。

b. 可靠性预测

可靠性预测主要是评估系统或元件在特定条件和特定时间段内按要求正常运行而不发生故障的可能性，这种预测有助于确保系统可靠性和使用安全性，尤其适用于故障可能引发危险的场景。系统中的故障有危险型和安全型两类后果，而可靠性预测通常衡量的是未被检测到的危险型故障。

PFH = λ_{DU}是危险未检出故障率，PFH值越低越好。系统中采用的诊断措施（例如使用电压监控器）直接影响SIL合规性。如果具备更完善的故障监控或其他检测与预防故障的机制，危险未检出故障率就会更低，PFH值也会更优，从而有可能达到更高的SIL等级。根据IEC61508标准，危险故障概率存在高和低两个需求，若安全功能的触发频率低于每年一次即为低需求，高于每年一次则为高需求。表2示例了IEC61508对危险失败概率的要求。

表2 IEC 61508对危险失效概率的要求

Safety Integrity Level (SIL)	Low Demand Mode of Operation (PFD_{avg})	High Demand or Continuous Mode of Operation (PFH)
SIL 4	$\geq 10^{-5}$ to $<10^{-4}$	$\geq 10^{-9}$ to $<10^{-8}$
SIL 3	$\geq 10^{-4}$ to $<10^{-3}$	$\geq 10^{-8}$ to $<10^{-7}$
SIL 2	$\geq 10^{-3}$ to $<10^{-2}$	$\geq 10^{-7}$ to $<10^{-6}$
SIL 1	$\geq 10^{-2}$ to $<10^{-1}$	$\geq 10^{-6}$ to $<10^{-5}$

安全功能包含输入子系统（即传感器）、逻辑求解器和最终执行元件（或执行器）。图3是安全功能的典型PFH分配情况，其中传感器占34%，逻辑器占15%，执行器占49%。

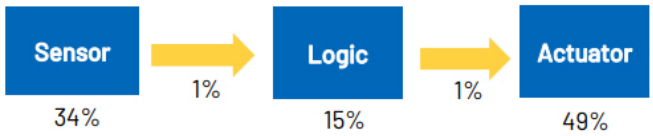

图3 典型PFH分配-安全功能

c. 架构约束

架构约束是安全关键系统中规定系统的设计与构建方式，以此来防止可能导致危险情况的故障。SFF和HFT是架构约束条件下的两项衡量指标。

SFF（安全失效比率）用于衡量系统失效时的安全性，如果系统中某一部件出现故障，SFF分值则体现该故障引发危险的可能性。图4示例了SFF的计算公式：SFF值越高越好，这意味着检出危险故障的比例越高，通过加强故障监控来达到更高的SIL等级。

$$SFF = \frac{\sum\lambda_{SD}+\sum\lambda_{SU}+\sum\lambda_{DD}}{\sum\lambda_{SD}+\sum\lambda_{SU}+\sum\lambda_{DD}+\sum\lambda_{DU}}$$

Failure Supervision ↑ SIL ↑ λ_{DD} ↑ SFF ↑

Note:
SD – Safe detected
SU – Safe undetected
DD – Dangerous detected
DU – Dangerous undetected

图4 SFF（安全失效比率）理论计算

HFT（硬件容错能力）反映了系统的冗余度，即系统在无法正常履行功能前最多能承受的故障次数。HFT为0意味着只要出现1次故障系统就需要启动安全功能，这类系统为单通道系统。根据IEC 61508标准，如果SFF在0到99%之间且需要达到SIL 3等级，那么系统的HFT必须达到1，这是架构约束下衡量并实现SIL等级的方式。

监控电路在功能安全系统的重要性

安全关键型应用中，故障检测诊断功能是避免对人员、财产和环境造成损害的核心环节，通过检测引脚来识别各类异常并借助输出引脚将系统转入安全状态。安全功能中输入逻辑和输出子系统是必备的，如图5示例，与之配套的还有电源模块和监控电路。

安全性的关键应用场景中，功能安全的任何细节考量都可能关乎生命安全，因此，功能安全产品必须时刻保持正常的工作状态，这也确保了诊断功能的完整性。监控电路的功能安全特性包括：通过过压和欠压监控检测电压是否异常；通过窗口看门狗监控微控制器是否发生故障；从操作角度确定采用锁存模式还是非锁存模式；是否具备片内诊断功能以提高诊断覆盖率并降低元件危险故障率；是否具备无毛刺特性以避免误触发；精度指标是否满足功能安全要求。

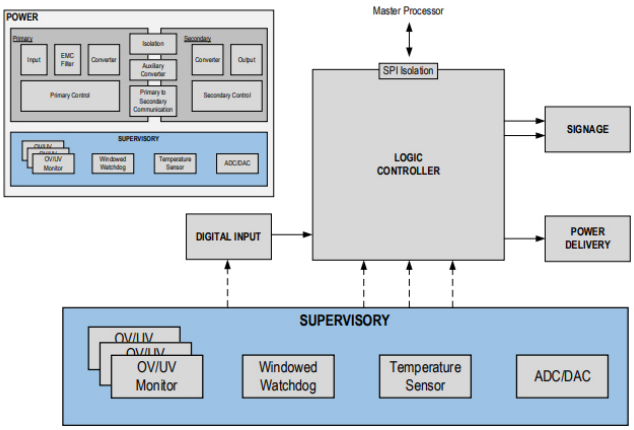

图5 监控器模块框图

符合IEC 61508基础功能安全标准需满足定性和定量这两个关键要求，如图6所示。定性要求涉及系统能力和质量管理体系(QMS)，是为解决系统性故障所采取的诊断措施力度。定量要求包括可靠性预测和架构约束。

定性要求在标准中设有专门表格，规定了控制系统性故障的相关技术和措施，包括应对电压击穿、电压波动、过压、欠压等问题的措施。“M”代表“强制性要求”，即无论SIL等级如何都须满足这项要求。程序序列监控被列为“高度推荐”项，尽管只是推荐但更受外部功能安全评估机构的青睐，尤其是在使用单通道微控制器单元时。其它措施还包括应对温度升高、检测信号线断裂与短路及低温保护等。

定量要求涉及可靠性预测和架构约束，通过加强故障监控能减少未检出的危险故障，同时改善危险故障概率和安全失效比率(SFF)。因此，PFH和SFF的提升都与SIL合规性的提高直接相关。

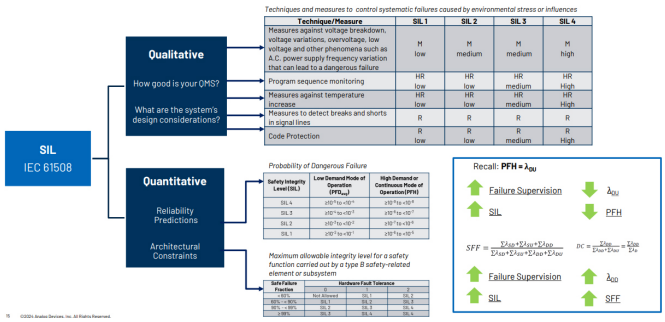

图6 IEC 61508观点概述

功能安全文档的定义与使用方法

ADI将工业级功能安全产品划分为四类，分别是FS-Enabled (Enabled at System Level)、FS-Evaluated (Enabled at System Level)、FS-Compliant (Compliant at Device Level)、FS-Certified (Compliant at Device Level with Certification)。

1. FS-Enabled

FS-Enabled产品遵循ISO9001但未依据IEC61508标准开发，ISO9001证书是满足IEC 61508标准对整体安全生命周期及功能安全评估要求的必备文件。FS-Enabled为系统层面功能安全提供支持，配有安全应用笔记，提供质量管理证书、故障发生次数(FIT)计算、故障模式分布(FMD)以及引脚故障模式与影响分析(FMEA)。FIT、FMD和FMEA对系统层面FMEDA的分析（故障模式、影响及诊断分析）起着极大的帮助。

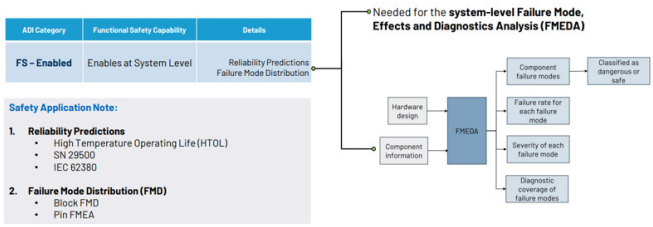

图7 FS-Enabled产品组合类别

故障发生次数(FIT)是衡量器件或系统可靠性的单位，是指每10亿小时运行中可能出现的故障次数。若某元件的故障率为1FIT，意味着从统计角度来看该元件每连续运行10亿小时可能出现1次故障。故障模式分布(FMD)是对系统内潜在故障模式的分析与分类，它聚焦于影响系统安全功能的故障模式的分析。引脚FMEA是对半导体器件引脚的详细检查，旨在识别潜在故障模式及其对整个系统运行的影响。客户通过ADI提供的这些文档可以轻松了解元件故障模式以及每种故障模式对应的故障率。

在选择可转化为FS-Enabled产品的器件时首先考虑已在实际应用中大量使用的器件及相关的安全功能与特性。比如电压监控器，其欠压和过压监控、高压耐受能力以及看门狗定时器等这些特性在功能安全系统中尤为关键，因此进行转换时首先挑选具备这些特性的产品。

表3是已发布的FS-Enabled监控器产品系列，当然并非仅限于列出产品。ADI按照FS-Enabled类别为这些器件提供了相应的文档资料，使用者进入每个产品页面可以下载并查看安全应用笔记和相关的文档内容。

表3 已发布的FS-Enabled产品

型号	描述
MAX16134	低压、精密、单/双/三/四电压微处理器电源监控器
MAX6762	低功耗、单/双电压窗口检波器
MAX6399	MAX6399高压开关控制器，具备过压/欠压保护功能
MAX6759	MAX6759低功耗、单/双电压窗口检波器
MAX6459	MAX6459高压、低电流电压监控器，采用SOT封装
MAX6764	MAX6764低功耗、单/双电压窗口检波器
MAX16059	MAX16059 125nA nanoPower监控电路，具备电容可调复位功能
MAX16010	MAX16010超小型过压保护/检测电路
MAX16128	MAX16128抛负载/反向电压保护电路
MAX16126	抛负载/反向电压保护电路

2. FS-Evaluated

FS-Evaluated产品除了提供FS-Enabled已有的文档外，还提供FMEDA和安全数据手册，旨在帮助设计者了解如何在功能安全场景中正确使用此类产品。FMEDA涉及诊断覆盖率，这意味着FS-Evaluated产品需具备内置自检这样的集成诊断功能。

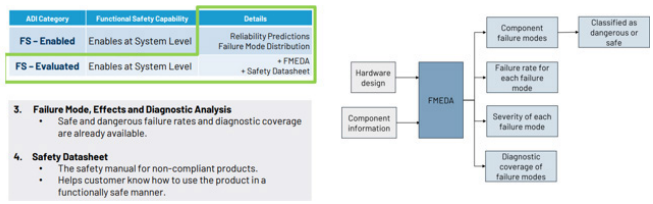

图8 FS-Evaluated产品组合类别

3. FS-Compliant

FS-Enabled和FS-Evaluated可以由非功能安全类产品转化而来，需要注意的是在转化过程满足相关的标准即可。而FS-Compliant和FS-Certified类产品则必须依据功能安全开发流程进行开发，也就是需要遵循IEC 61508标准，并且为客户提供安全手册。

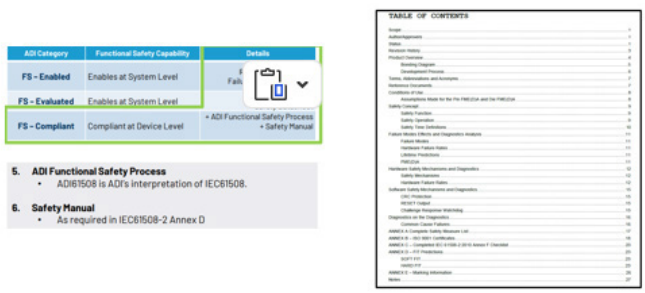

图9 FS-Compliant产品组合类别

4. FS-Certified

这类产品需要通过如TUV Nord、TUV Rheinland和Exida等外部功能安全评估机构的审核和认证。

图10 FS-Certified产品组合类别

MAX42500

首款通过TUV Nord认证的电源监控器产品，达到SIL-3等级的工业级安全功能，具备支持任意电源树的灵活性。MAX42500拥有4至7路电压监控输入，欠压阈值可在2.5%至10%之间选择，整个温度范围内的精度可达到1%至1.3%。该产品配备了响应式看门狗定时器以及可编程的上电时序记录器和片内诊断功能。如需了解更多信息，可登录analog.com/cn网站搜索相关产品型号，即可下载数据手册并深入了解该产品。

电压/电源监控器既可以发挥监控器的诊断功能，也可以设计符合功能安全标准的电源，当出现随机硬件故障时协助系统转入安全状态。

虽然一些应用场景可以使用普通监控器但仍选择SIL等级监控器，主要源于SIL等级产品具有如下六大关键优势：

1. 提供FMEDA为技术安全分析提供支持，在进行系统级FMEDA分析时掌握故障指标数据；

2. 集成了多项安全特性，涵盖丰富的诊断功能，比如集成多路电压监控和看门狗定时器等；

3. 具备片内诊断功能，能够检测自身的随机硬件故障，因此其危险故障检出率得到了显著提升；

4. 适应IEC 61508标准未来的修订版本，尤其是针对诊断方面的新要求；

5. 兼顾其他国家标准要求/地区的安全标准和指令，例如符合机械指令中的使用建议；

6. 符合功能安全要求且相关安全文档齐全，为功能安全评估工作提供便利。

小结

工业环境中的设备通常全年无休运行，安全性和可靠性至关重要，功能安全提供的诊断功能确保运行的可靠性。ADI拥有行业认证的功能安全领域专家，大力推行零缺陷文化，致力于为客户提供全面的产品开发流程，帮助客户打造符合第三方认证标准的产品并加快上市进程。

为方便客户灵活的使用功能安全产品，ADI提供了丰富且全面的工具，使用者可以下载技术文章、在EngineerZone页面、博客、相关专题页、解决方案页面查看讨论及感兴趣的主题，同时也可以通过联系方式进行直接沟通。

技术文档:

利用高性能电压监控器提高工业功能安全合规性—第1部分

使用SIL 2器件设计功能安全的SIL 3模拟输出模块

工程师社区:

安全事项博客

电源监控器EngineerZone页面

解决方案页面:

工业功能安全解决方案

MAX42500数据手册和产品信息

监控电路页面

联系我们!

支持团队 | ADI公司