Printed in Shanghai, 08/2020

intertek
Total Quality. Assured.

功能安全认证
计划及标志指南

Intertek工业自动化、加工机械及相关设备功能安全专有标准（INT/FS/2019）及认证计划指导文件

Intertek是全球领先的全面质量保障服务机构，始终以专业、精准、快速、热情的全面质量保障服务，为客户制胜市场保驾护航。凭借在全球100多个国家的1,000多家实验室和分支机构、及46,000多名专业员工，Intertek致力于以创新和定制的保障、测试、检验和认证解决方案，为客户的运营和供应链带来全方位的安心保障。

更多信息，敬请联络：

400-886-9926

service.china@intertek.com

intertek.com.cn

intertek
Total Quality. Assured.

intertek
Total Quality. Assured.

目 录

intertek
Total Quality. Assured.

引 言

机械安全是工业数字化和自动化（Industry 4.0中的一个重要方面）、机器人技术、智能建筑和智能城市中重要性增长最快的领域之一。新的安全策略为制造商提供一种提高生产力和市场竞争力的方式。安全成为机器功能性和可操作性中不可分割的组成部分，而不是为了满足法规要求而事后增加的考虑事项。

在发达经济体中，国家法律规定各种机器必须满足基本的健康和安全要求，也就是说，新机械在进口并供应到制造工厂时必须符合基本要求。制造商设计机器时，必须遵守专门针对机械安全规定的国际标准。这些标准获得全球认可，各项要求之间的换算表有利于促进各国之间的机械贸易和装运。

功能安全（FS）是强调作为独立部件、子组件和整机的防护系统的设计、操作和控制安全，从而降低该系统应用所造成的不合理风险的工程过程。功能安全最佳实践不是简单地遵守行业标准、预防事故，而是提升运营的有效性和生产力，减少设备检修时间和维修成本。将功能安全融入流程和设备的制造商，拥有国际公认安全评级的优势，有利于在全球舞台上销售其解决方案。

为减轻功能安全风险、减小危害而设计的机械系统具有以下特点：

- 增强机械安全
- 可用性（减少检修时间）
- 可靠性（按需耐用）
- 可维护性（生命周期能力）
- 提高生产力（绩效）
- 成本效益

针对不同学科，有阐明安全相关系统必要安全措施、潜在故障、开发要求及建议的各项功能安全标准。其中一项规定机械系统设计一般功能安全要求的标准为ISO 12100标准。

已制定Intertek功能安全专有标准（INT/FS/2019），其目标是达到工业价值链中各利益相关方的要求。我们的模块化解决方案为制造商提供灵活选项，我们的广泛服务和认证为行业利益相关方提供更详细评审安全措施的选项，这是买方和监管机构的一项共同要求。

本指导文件阐明确定机械设计所需的评估和确认流程，采用国际标准、国家标准和Intertek 功能安全专有标准（INT/FS/2019），作为以风险为基础的逆向设计评估方法的参考资料，从而确认和认证各种机器的功能安全和通用安全。

功能安全(FS)认证：
计划及标志指南

intertek
Total Quality. Assured.

第1条

符合性 框架

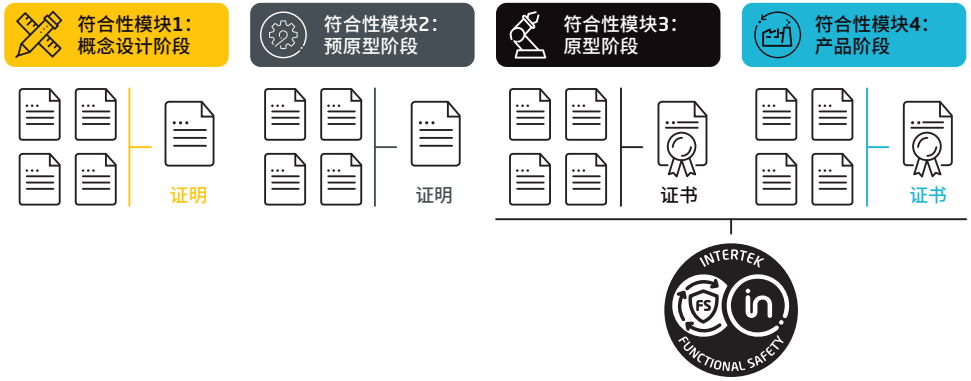
本指南的主要目的是提供Intertek确认设计完整性和判定所声称机械安全、性能等级（PL）和安全完整性等级（SIL）从而授予Intertek功能安全（FS）标志所用方法的符合性框架概述。

采取的方法以风险为基础，在考虑机械设计依据、机械设计评估、风险评估、确认、验证和检验方法时，将ISO 12100作为基本横向标准，将Intertek功能安全专有标准(INT/FS/2019)和特定设备或产品标准作为纵向平台，确认设计依据。

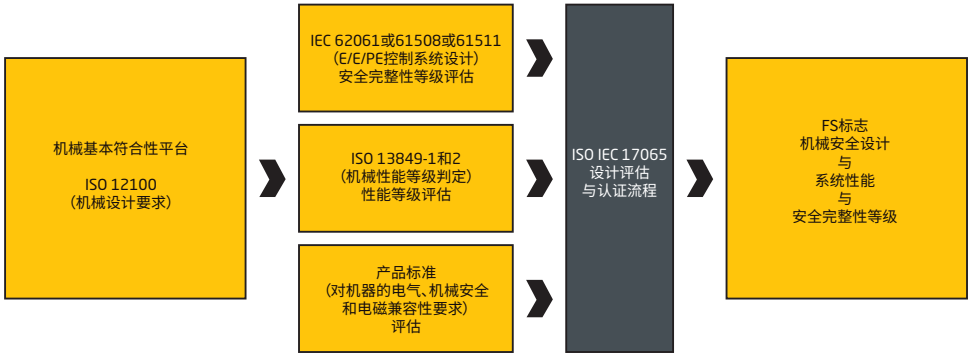
INT/FS/2019专有标准：

- 符合性方法的模块化等级
- 工程块结构
- 以风险为基础的方法/设计评估方法
- 性能等级（PL）和安全完整性等级（SIL）
- 硬件和软件集成

无论您处在概念设计阶段、预原型阶段、原型阶段还是将所有安全元素融入产品阶段，我们的模块化功能安全解决方案都为行业利益相关方提供更详细评审安全要求的选项。



本符合性评估方法的结果是根据产品认证方法的ISO/IEC 17065流程关键决策路径，为授予机械系统或流程的认证或标记（功能安全标志），确认所声称的性能等级（PL）和安全完整性等级（SIL）以及通用安全。这些方法是指对完整系统、子系统或部件/各独立式设备符合性的应用、评估、认证评审和认证最终决策。



安全完整性等级

SIL代表安全完整性等级，是将风险降低到可接受水平所需要的风险降低程度的一种表达方式。根据IEC 61508标准，安全等级分为1、2、3、4，从一个等级向另一个等级转变时，按安全要求的数量级递增顺序排列。一般来讲，如果暴露于危险的人员通常不超过一人，则在机械和工厂自动化中见不到SIL4。而在涉及数百人甚至数千人的应用中，比如核能和轨道，则需保持该等级。

性能等级

ISO 13849。其性能可按a、b、c、d、e进行分类。
计算PL和SIL评级时，将参考各类可靠性相关数据。
根据IEC 61508标准单独评价SIL时，不能按PL类别a、b、c、d或e分类。

功能安全(FS)认证：
计划及标志指南

功能安全的意义和目的是在出现实时故障的情况下采取防护措施，预防受到对以下几项产生影响的损害、已预见和未预见的危害：

- 人员
- 环境
- 资产（机器）

功能安全通过执行降低非期望事件概率从而最大限度地减少机器整个生命周期内故障的控制和防护概念这一设计意图，实现上述目的。

安全标准将“安全”定义为免于不可接受的风险。消除风险的最有效方式是从设计上远离风险。但通过设计降低风险不一定具有可能性或可行性，出于若干原因，采取静态防护措施通常是退而求其次的选项。与意外安全停止装置相比，快速安全地停机，不仅能降低风险，还能增加机器的正常运转时间，提高生产力。同时，满足法律义务，确保人员、环境和资产的安全。

机械功能安全通常是指对机器应用进行安全监控并在必要时撤销机器应用从而确保安全运行的系统。因此，安全相关系统通过探测危险状况执行必要安全功能，通过确保采取预期措施（比如：安全停机），使运行达到安全状态。

1.1 系统符合性框架：总则

为了进行符合性评估，Intertek将ISO 12100标准和Intertek专有标准INT/FS/2019作为以风险为基础的方法，本指南所包含的规范性引用文件应通过判定设计安全、所声称的机械功能安全（PL和SIL）和通用安全，提供覆盖机器生命周期的基本安全框架。

ISO 12100规定实现机械设计安全的基本术语、原则和方法。该标准针对设计要求，规定风险评估和风险减少原则。这些原则以机械设计、使用、事件、事故及相关风险等知识和经验为基础。

ISO 12100规定代表不同粒度等级的三类标准：

- A类标准规定总体、首要指导原则 - 所有机器（横向标准）
- B类标准针对具体技术，规定具体设计原则（横向标准）
- C类标准是针对应用情况的特定标准或产品标准（纵向标准）

好处

纳入功能安全设计原则，可提供以下好处：

- 降低风险水平
- 安全的机械设计
- 对操作员、环境、机器生命周期的保护和防护措施

1.2 功能安全（FS）标志 - 符合性框架（所有系统层面）

总体上，ISO 12100适用于系统层面（整机），但具体要素可追溯到产品或部件层面。ISO 12100是A类标准，适用于一切被定义为机器的物品。B类标准阐述机器的子系统或子组件，C类标准专用于特定产品或机器或者机器的部件。

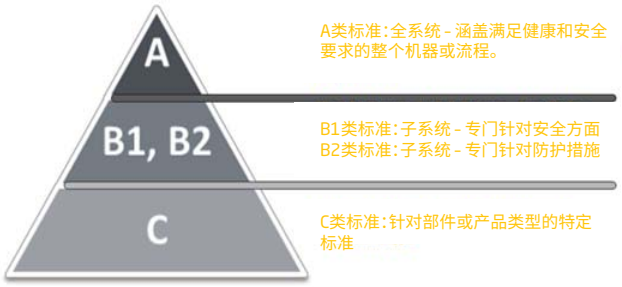


图1.1（标准分类结构）

1.3 A类分类：系统符合性评估

表1.1给出用于全系统（整机）风险评估框架的典型A类标准实例。

A类分类（全系统）	ISO 标准
机械安全–设计通则 – 风险评估与风险减少	ISO 12100
机器人与机器人装置 – 工业环境用机器人安全要求	ISO 10218

表1.1

功能安全(FS)认证：
计划及标志指南

1.4 B1类分类：子系统符合性评估

表1.2提供适用于子系统符合性评估框架的典型B1类标准实例。

B1类分类（子系统） 特定方面	ISO 标准
固定式防护装置和可移动防护装置(安全围栏、屏障、防护盖罩)	ISO 14120
带防护装置的联锁装置（联锁安全闸门等）	ISO 14119
防止意外启动	ISO 14118
压敏保护装置（压敏垫等）	ISO 13856
双手控制 装置	ISO 13851
限制进入固定式防护装置和可移动防护装置的可调安全设施	ISO 14120
紧急停止	ISO 13850

表1.2

1.5 B2类分类：子系统符合性评估

表1.3中给出的实例为适用于子系统符合性评估框架的典型B2类标准。

B2类分类（子系统） 功能安全及安全相关控制装置	标准
控制系统安全相关部件	ISO 13489 IEC 62061
气动系统的安全相关要求	ISO 4414
液压系统的安全相关要求	ISO 4413
通用安全电气设备	IEC 60204
电气电子及可编程电子的功能安全	IEC 61508
过程工业安全仪表系统的功能安全	IEC 61511

表1.3

1.6 C类分类：独立设备或部件层面

表1.4中的产品符合性评估框架典型C类标准实例。

C类分类 特定设备	标准
压力机	ISO 16092
机器人，机器人系统	ISO 10218 - 1和2
协作机器人	ISO TS 15066
木工机器	ISO 19085
自动导引车（AGV）	ISO 3691
半导体器件	IEC 60747

表1.4

第2条

术语和定义

在所有情况下，本参考文件中采用的术语和定义均应依据下表1.5列出的特定标准和条款。在引用当前版次标准的基础上，特意删除了发布年份。

标准和条款
ISO 12100：机械安全 – 设计通则 – 风险评估和风险减少
IEC 61508-1：电气/电子/可编程电子安全相关系统的功能安全 – 第1部分：一般要求
IEC 61508-2：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 61508-3：电气/电子/可编程电子安全相关系统的功能安全 – 第3部分：软件要求
IEC 61508-4：电气/电子/可编程电子安全相关系统的功能安全 – 第4部分：定义和缩略语
IEC 61508-5：电气/电子/可编程电子安全相关系统的功能安全 – 第5部分：确定方法实例
IEC 61508-6：电气/电子/可编程电子安全相关系统的功能安全 – 第6部分：IEC 61508-2和IEC 61508-3的应用
IEC 61508-7：电气/电子/可编程电子安全相关系统的功能安全 – 第7部分：技术和措施概述
IEC 61511 -1: 功能安全 – 加工工业部门的安全仪表系统 – 第1部分：框架、定义、系统、硬件及应用程序编程要求
IEC 61511-2：功能安全 – 加工工业部门的安全仪表系统 – 第2部分：应用指南
IEC 61511-3：功能安全 – 加工工业部门的安全仪表系统 – 第3部分：所需安全完整性等级确定指南
ISO 13489-1：机械安全 – 控制系统的安全相关部件 – 第1部分：设计通则
ISO 13489-2：机械安全 – 控制系统的安全相关部件 – 第2部分：确认

表1.5

第3条

范围

确定控制系统安全相关部件（SRP/CS）的性能等级和安全完整性等级以及机械结构设计的下游影响，须经过设计评估、检验和认证过程，包括附加Intertek功能安全标志。本流程适用于以下工业部门：

- 独立式工业和商业机械设备
- 独立式工业和服务机器人
- 定制集成/自动工业机械（包括工业机器人和索引系统）
- 能源储存系统、充能系统
- 自动导引车（AGV）
- 储能
- 机床
- 自动化系统
- 工业炉
- 制冷系统
- 包装机械
- 农业机器
- 食品加工设备
- 施工设备
- 爆炸性环境设备
- 采矿
- 石油/天然气/化工设备
- 加工
- 土方和隧道工程
- 起重机/升降机/材料装卸设备
- 林业/工厂机械
- 以及许多其他部门

功能安全(FS)认证：
计划及标志指南

第4条

工程
块结构

评估和确定机械性能等级和安全完整性等级（包括上游和下游对机械整体设计的影响）时，选择A、B1、B2、C等分类等级，运用工程块结构设计，一经选择，则构成总体符合性方法。

图1.2中给出的以下实例代表完全集成的自动化机械系统，包括集成到一起形成一套完整端到端机械系统的独立式机器。

A类（+C类）工程块结构：

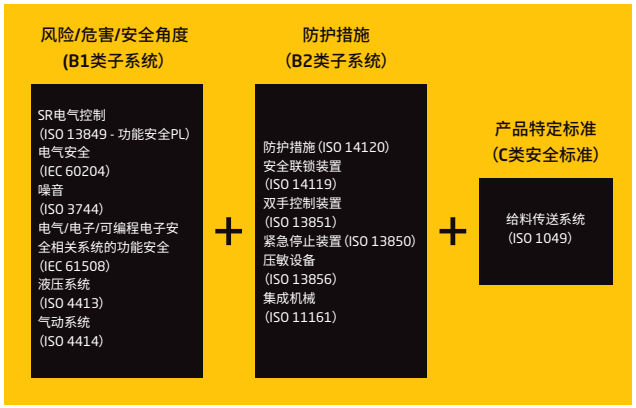


图1.2（A类+C类）

第5条

符合性模块

5.1 应以ISO 12100为符合性依据，对申请功能安全认证的所有机械执行设计评估、确认、验证和认证流程。

5.2 达到设计阶段关卡内的机械状态之前，在按照规定评估模块进行机械设计的基础上确定符合性，每个模块采用从ISO 12100标准中选定的条款，以逆向设计计算作为确认和验证纳入机器预期设计或结构打造的设计意图或防护概念的一种方式，确定机器的符合性（Intertek专有标准INT/FS/2019）。

5.3 下文图1.3给出四个符合性模块图示：

- 符合性模块 1 - 概念（设计阶段）
- 符合性模块 2 - 预原型（首次构建）
- 符合性模块 3 - 原型（预生产构建阶段）
- 符合性模块 4 - 生产（运行中构建）

设计阶段关卡和符合性模块可交付成果概要：

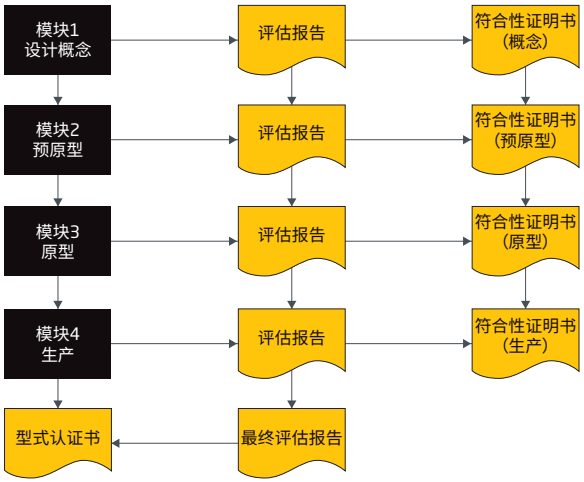


图1.3（基本符合性模块）

5.4 本图诠释当用于确定符合性时，适用于特定符合性模块的A类标准和B 类标准选定条款的变化。

5.5 每个功能安全符合性模块（ISO 12100基本等级）应将风险评估细分为四个子模块，遵照相同的评估流程。此子模块方法是为了按下文图1.4所示识别、量化、确认和评估风险。

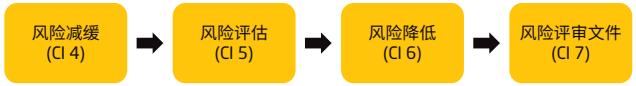


图1.4（基本符合性方法中的主题）

5.6 上一条 “A类标准（ISO 12100）”中定义的工程块结构是机械端到端设计评估的横向依据，包括B1类和B2类标准，用于评估所声称的PL（ISO 13489）和SIL（IEC 62061、61508和61511系列标准）。

注：ISO 13489、IEC 61508或IEC 61511系列功能安全标准中的任何标准，不包括机器的电气安全。电气安全应参见IEC 60204系列标准。

5.7 除了采用工程块结构以外，上述模块化方法和子模块结构应同样适用于：

- 整机，也称为全系统
- 整机的子系统或子组件
- 整机或独立式机器的零部件

第6条

认证：
一般要求

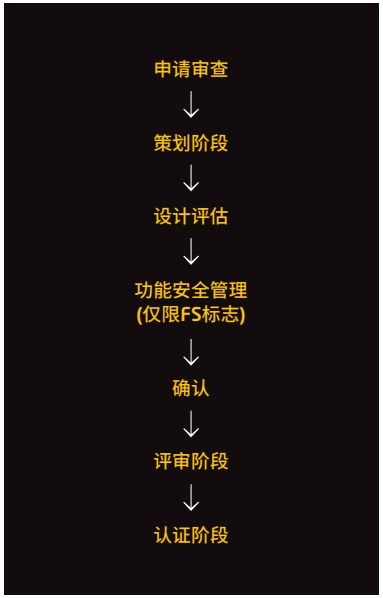
概述

6.1 在授予符合性证明书或型式认可证书和附加Intertek功能安全(FS)标志之前，评估整机、子系统、组件、部件或独立式产品时，需要执行的一般认证流程，应参见ISO/IEC 17065和17067标准中的规定。

6.2 在所有情况下，均应依据ISO IEC 17067标准，针对签发符合性证明书或型式认可证书所需采用的符合性评估系统，执行1类、1a类或3类符合性方法。

6.3 根据ISO 17065标准，应针对全系统(完整的机器装备或独立式机器)或全系统的子系统或零部件，执行功能安全和设计安全评估流程：

- 申请人提出认证申请(Intertek功能安全标志)
- 签订关于功能安全标志和认证计划的具体认证协议
- 制定认证计划(规定标准分类、工程块结构以及采用的符合性模块)
- 根据既定符合性模块及相关C类分类标准进行评估，对制造商在全系统、子系统或组件或独立式产品/部件层面上所做的风险评估/失效模式影响与诊断分析、声称的PL和SIL等级以及适用于建筑施工所采取安全等级的应用安全系数(FoS)进行设计评估，以此完成评估和确认
- 通过现场检验设计评估/测试和确认阶段识别的关键要素，验证与施工建造相关的关键构建/装配要素
- 确认全系统(整机)、子系统或组件或独立式产品/部件符合所用符合性模块，在推荐证明书或型式认可证书之前确认所声称的PL或SIL等级，进行认证技术评审
- 确保在签发任何认证和授权附加Intertek功能安全标志之前已完全落实最终决策前的所有步骤，继而做出最终认证决策



认证流程

6.4 与功能安全或机械设计安全相关的设计评估和验证确认方式采用的所有计算和数值表(例如MTTFd值)，应源自功能安全规范标准、产品、工程应用标准以及工程科学参考资料中的已知信息。

6.5 应执行设计评估、确认和验证(检验)，通过逆向设计工程技术(计算校核)或成熟工程实践(SEP)中的工程知识应用，确认全系统、子系统或组件或者独立式产品/部件的总体安全构建，并通过对设计构建安全完整性设计意图的工程声明确认，形成文件。

6.6 完全达到符合性模块1和2中相关要求，圆满完成评估、确认、验证、认证评审和最终决策后，应签发符合性证明书，并且在以下设计阶段关卡层面，为全系统(整机)、子系统或组件或者产品/部件签发符合性证明书：

- 符合性模块 1 - 概念(设计阶段)
- 符合性模块 2 - 预原型(首次构建)

并非只要完成符合性模块1和2，就能在任何情况下签发带有Intertek功能安全标志的型式认可证书。

6.7 完全达到符合性模块3和4中相关要求，圆满完成评估、确认、验证、认证评审和最终决策后，应签发带有功能安全标志的完整型式认可证书，并且在以下设计阶段关卡层面，为全系统(整机)、子系统或组件或者产品/部件签发型式认可证书：

- 符合性模块 3 - 原型(预生产构建阶段)
- 符合性模块 4 - 生产(运行中构建)

6.8 符合性证明书或型式认可证书的持续有效性，取决于生命周期内获得认可的型式。对PL、SIL、FoS和通用安全完整性存在影响的授权设计变更，只能由签发机构批准。

功能安全标志使用

6.9 对PL、SIL、FoS完整性和通用安全存在影响的未授权设计变更，应导致已签发的证书和功能安全标志被撤销、(功能安全标志)许可申请被终止。

6.10 在所有情况下，通过不当使用，以虚假声称或广告宣传对Intertek功能安全标志进行滥用或未经授权使用，应导致功能安全标志被撤销、(功能安全标志)使用许可申请被终止。

6.11 圆满完成"评估、确认和验证"章节详述和图1.5演示的符合性评估方法后，应授予下图所示的Intertek 功能安全(FS)标志。

图1.5

注：对以上范本标志中的"声称"，将予以解释，包括声称达到相应职能和一般国际/国家标准的能力。

功能安全型式审查证书：实例

6.12 圆满达到符合性模块3和4要求时签发的功能安全型式审查证书实例。

intertek
Total Quality. Assured.

Type Examination Certificate

Certificate Number: BBB-SSS-NNNNNNNRn
Page 1 of 3

<Intertek Office> hereby confirms the below listed <equipment / component> on satisfactory evaluation is authorised to affix the Intertek Functional Safety Mark:

Model: <Model Name & Description & Rating / Characteristics>

Manufacturer: <Legal Entity & Full Address>

Has been evaluated in accordance to below listed Standards and deemed to provide a Performance Level (PL) CAT X and Safety Integrity Level (SIL) Y

Standard:	Title:

The decision to recommend affixing the Functional Safety Mark is based on satisfactory Certification Review of the following reports:

Report Number:	Issuing Body:

Safety Function:

Limitations:

Validity Date: <dd mm yyyy>

SAMPLE

Signature
<Name>
Certification Officer
Issue Date: <dd mm yyyy>

This Certificate is for the exclusive use of Intertek's client and is provided pursuant to the agreement between Intertek and its Client. Intertek's responsibility and liability are limited to the terms and conditions of the agreement. Intertek assumes no liability to any party, other than to the Client in accordance with the agreement, for any loss, expense or damage occasioned by the use of this Certificate. Only the Client is authorized to permit copying or distribution of this Certificate and then only in its entirety. Any use of the Intertek name or one of its marks for the sale or advertisement of the tested material, product or service must first be approved in writing by Intertek.

<Intertek Legal Entity Address>

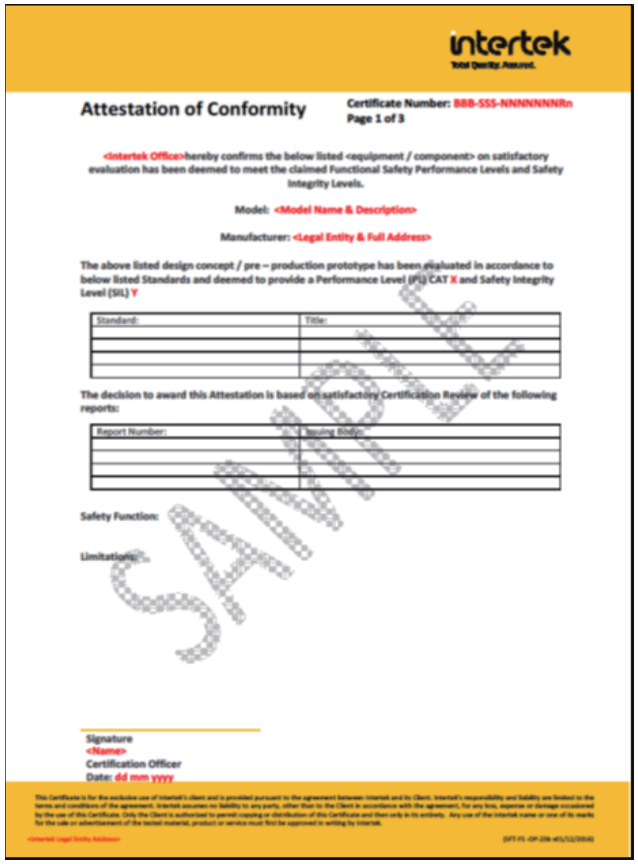
(TF-FS -OP-23a V1 14 May 2020)

型式审查证书

- 型式认可证书
- 针对符合模块1-4要求的整机系统签发
- 针对电气/电子/可编程电子控制系统签发
- 针对部件/独立式机器签发
- 涵盖功能安全管理(IEC 61508-1 Cl 6)
- Intertek功能安全标志
- 证书1年有效期
- A类、B1类或C类标准产品符合性及辅助评估报告
- PL和SIL结果
- PL和SIL确认等级
- 参考已评估的技术施工文件及内容
- 依据ISO IEC 17065标准予以认可

功能安全符合性证明书：实例

6.13　圆满达到符合性模块1和2要求时签发的符合性证明书实例。



Attestation of Conformity

Certificate Number: BBB-SSS-NNNNNNNRn
Page 1 of 3

<Intertek Office> hereby confirms the below listed <equipment / component> on satisfactory evaluation has been deemed to meet the claimed Functional Safety Performance Levels and Safety Integrity Levels.

Model: <Model Name & Description>

Manufacturer: <Legal Entity & Full Address>

The above listed design concept / pre – production prototype has been evaluated in accordance to below listed Standards and deemed to provide a Performance Level (PL) CAT X and Safety Integrity Level (SIL) Y

Standard:	Title:

The decision to award this Attestation is based on satisfactory Certification Review of the following reports:

Report Number:	Issuing Body:

Safety Function:

Limitations:

Signature
<Name>
Certification Officer
Date: dd mm yyyy

SAMPLE

符合性证明书

- 只需完成模块1-4，即可作为型式认可证书签发
- 无有效期
- 针对PL评级或SIL评级或者PL评级和SIL评级签发
- 按A类、B类和C类分类进行确认
- 针对概念阶段或预原型设计阶段签发
- 针对产品阶段或原型构建阶段签发
- 未授予Intertek功能安全标志
- 参考已评估的技术施工文件及内容
- 依据ISO/IEC 17065标准予以认可

功能安全装置验证证书：实例

6.14　针对定制机器签发的功能安全装置验证证书实例。

Certificate of Unit Verification

Certificate Number: <XXXXXXXX>
Page 1 of 3

<Intertek Legal Entity> hereby confirms the listed integrated automated machine consisting of sub element machines listed below by satisfactory evaluation is authorised to affix the Intertek Functional Safety Mark by conforming to Class A, B and C standards for:

<Ref: Equipment / Machine Standard>

Model:	Description:	Rating / Characteristics

<Manufacturers Name & Address>

Class C Standards Applied: See table 1, page 2.

The above integrated machines have been evaluated for Functional Safety in accordance to Class A and B Standards and deemed to provide a Performance Level (PL) CAT X and Safety Integrity Level (SIL) Y.

Class A and B Standards Applied: See table 2 page 2:

The decision to recommend affixing the Functional Safety Mark is based on satisfactory Certification Review of the following reports:

Report Number:	Report Reference:

Safety Function:

Limitations:

Signature
<Name>
Certification Officer
Issue Date: <dd mm yyyy>

SAMPLE

装置验证证书

- 型式认可证书
- 针对定制集成复杂机器和系统签发
- 针对定制独立式复杂机器和系统签发
- 无指定有效期
- 在一次性设计基础上，给予型式认可
- 产品符合性认证（A类、B1类或C类）
- 确定PL和SIL等级
- PL/SIL计算结果
- 需要FSM - IEC 61508-1 Cl 6，作为一次性事件
- 授予Intertek功能安全标志
- 参考已评估的技术施工文件及内容
- 依据ISO IEC 17065标准予以认可

第7条

符合性模块/符合性确认：一般说明

7.1 对性能等级、安全完整性等级和机械安全设计方面的功能安全声称进行评估和确认时，应参考A类、B类和C类标准。通过确认（计算）和确定设计FMEA风险评估输出（ISO 12100）及总体机械设计（确定所采用的FoS和SEP），完成上述工作。由此表明机器在其生命周期内的预期安全功能，并充分降低风险。

7.2 性能等级、安全完整性等级及机械安全设计展示、工程块结构和符合性模块相结合，适用时，构成对以下几项设备的功能安全符合性评估方法：

- 全系统（整机或多机集成）- A类
- 子系统（全系统安全相关控制系统实例）- B类
- 独立式机器或部件 - C类

7.3 选择适当符合性模块，确定需采用的功能安全、性能等级、安全完整性等级和机械安全完整性评估和确认方法，取决于机器在阶段关卡的设计构建状态。

7.4 作为评估和确认方法采用的符合性模块（1、2、3、4）包括一般设计意图、与工业机械相关的安全考虑事项以及对汽车行业相关危害的安全考虑事项，以ISO 12100（A类）作为建筑施工范围内相应工程应用的纵向标准：

- 机械
- 环境
- 化工
- 电气
- 电气/电气/可编程控制系统
- 软件
- 网络安全（可选）
- 人体工学
- 调试
- 可操作性
- 维护
- 运输

工程块结构

7.5 确定性能等级、安全完整性等级和总体机械安全的功能安全符合性方法是选择A类 + B1类 + B2类 + C类标准，通过形成工程块结构展示流程。举例来讲，包括输入给料和输出传送系统的预生产集成工业材料处理装置，如图1.6和表1.6所示。

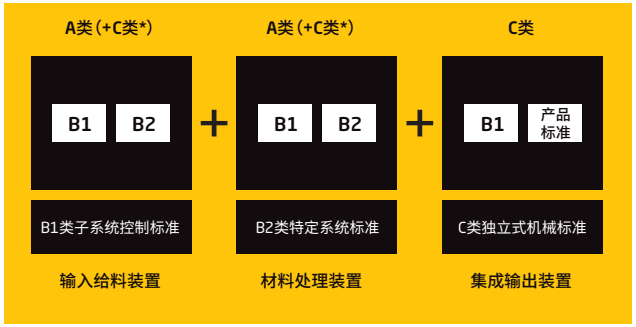


图1.6

机器	功能安全符合性模块	分类	功能安全符合性系统（流程）	机械控制评估	所采用的参考标准	功能安全和M/C设计评估
材料处理装置	4	A	A	A	ISO 12100和14121	M/C设计风险评估评估
			B	B2	IEC 61508-1	总体安全生命周期要求
			B	B2	IEC 61508-2	E/E/PE系统安全生命周期要求
			B	B2	IEC 61508-3	软件安全生命周期要求
			B	B2	ISO 13489-1和2	电子控制系统安全 - PLr
				B2	IEC 60204	机器电气安全
				B2	ISO 4413	液压系统
				B2	ISO 4414	气动系统
				B1	ISO 13850	紧急停机
				B1	ISO 14118	意外启动
				B1	ISO 14119	联锁装置
				B1	ISO 14120	固定/移动防护装置
				B2	ISO 11161	机械集成
传送装置			C	C	ISO 1049	传送给料系统

表1.6（模块4：需采用的A类、B类和C类分类标准）

第8条

评估、确认和验证

8.1 获得全系统整机、子系统或组件/独立式机器通用安全、性能等级和安全完整性等级等认证的通用评估、确认和验证方法，如以下流程图1.7所示：

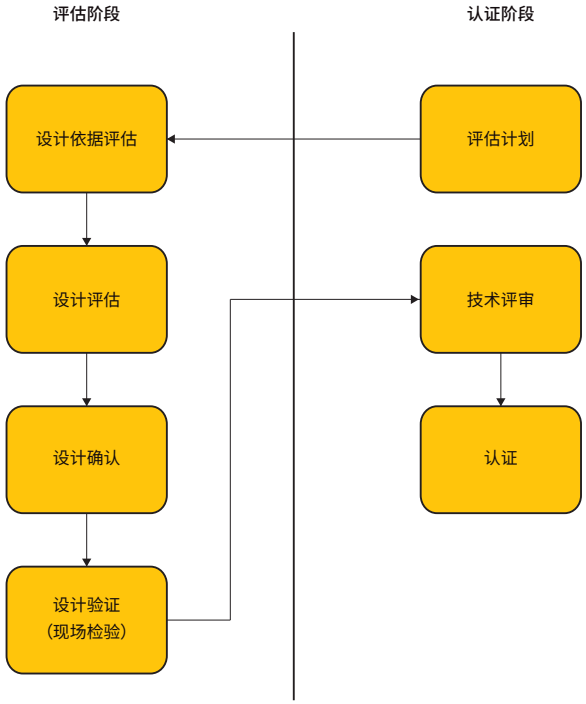


图1.7（符合性方法评估、检验和认证）

功能安全(FS)认证：
计划及标志指南

8.2 设计依据评估

8.2.1 视施工建造阶段关卡周期而定，应从下文表1.8中选择需要采用的符合性模块：

符合性模块	生命周期阶段关卡
1	设计概念（设计阶段）
2	预原型（首次构建）
3	原型（产品阶段）
4	生产（运行中构建）

表1.8（符合性模块类型）

8.2.2 以下流程图（图1.8）中与风险方法相关的评估准则，规定了来自ISO 12100标准的主要条款，这些条款在应用时构成符合性模块的基础：

图1.8（风险评估符合性方法）

8.2.3 设计依据评估应将ISO 12100作为一般指南，确定相应全系统（整机）、子系统组件或部件的风险评估/设计FMEA输出对施工建造具有代表性，确认设计输出列明：

- 所有风险和危害均已得到识别，并且与施工建造的设计意图相关
- 声明的设计输出识别符合的危害减缓概念和参考资料（标准）
- 运行限值和最大限值的结构设计意图
- 文件登记簿是指所有外供设计文件生成的列表

8.2.4 子模块：确定适用的分类标准和块结构架构（每个符合性模块和工程块结构中的子模块及A类 + B类子模块）时，应确定需要采用的横向标准（B1类和B2类），并且在适用时，概述需要采用的C类分类标准（实例 - 模块4：符合性系统流程A、B和C）。

8.3 设计评估

8.3.1 通常，用于评估和验证设计FMEA/风险评估的功能安全（PL和SIL）和总体机械安全符合性的横向和纵向参考标准，将取决于总体施工建造所采用的工程块结构，以下表格列示符合性方法以及评估和确认方法所需采用的主要规范标准。

表1.9给出设计评估符合性和确认方法资料的实例。

全系统（集成自动化机械）预期用途 – 工业部门	评估符合性标准
机械安全 - 设计、风险评估和风险减少一般原则	ISO 12100（适用部分）
机械安全 - 控制系统安全相关部件的设计和集成原则	ISO 13489-1
机械安全 - 控制系统安全相关部件，确认 (PLr)	ISO 13489 -2
机械安全 - 机器的电气设备	IEC 60204-1
电气、电子和可编程电子控制系统的功能安全 (SIL)	IEC 61508
其他B1类和B2类标准，视施工建造情况而定	B1类和B2类，视情况而定
如果是集成机械特定产品标准（若使用），则属于其他C类标准	C类，视情况而定

表1.9（全系统机械符合性参考标准）

8.3.2 符合性评估流程应以FMEA/ISO 12100风险输出的评估为基础，用于确定符合性的评估方法应通过设计评估确保所有设计输出符合已识别的风险危害，确保采用适当横向和纵向分类标准，而且以下几项完全满足上述标准：

- 全系统（完整端到端构建）
- 子系统组件
- 部件层面或独立式机器

8.3.3 视机器和建造水平而定的符合性方法，将采用ISO 12100识别各类机器、子系统和部件/独立式机器层面中包含的工程设计应用。

8.4 设计确认

8.4.1 设计评估得出的输出结果（确定所有风险已通过设计意图得到识别和减缓）、风险评估设计FMEA输出/声称的施工建造性能等级（PL）和安全完整性等级（SIL），应予以确认。

8.4.2 应对设计FMEA/风险评估输出进行确认，作为下文表1.10列出的特定标准实例。

确认方法	评估符合性标准
通过计算FoS和MoS（安全边际）确认中采用的SEP，进行设计意图确认	ISO 12100
通过重新计算声明的PLr，确认设计FMEA中的PLr声称，计算确认 实际PL，即确认声称的结果	ISO 13489-1 及第2部分
通过重新计算声明的SIL，确认设计FMEA中的SIL声称，确认实际 SIL，即确认声称的结果	IEC 62061或 IEC 60158
液压流体动力 - 系统和部件的安全性	ISO 4413
液压流体动力 - 系统和部件的安全性	ISO 4414
电气/电子/可编程电子软件要求	IEC 60158-3

表1.10（列表 - 评估和确认）

8.5 设计验证

8.5.1 应通过对初始构建/制造情况或调试运行/签字移交情况的现场实地检查，验证认为与总体安全和"产品"构建和运行功能安全完整性相关的施工建造设计关键要素。

8.5.2 符合性评估的设计评估和确认阶段，应参照设计意图/设计评估，识别任何认为需要验证的部件、子组件或子系统，从而验证安全性和运行性能完整性。

8.5.3 验证应通过测量、现场测试或两者相结合，按规定参考进行实地检验，确定和确认与声称的总体设计安全性和完整性相关的参数计算值或设计限值。

8.5.4 设计验证检验结果应作为对形成文件的总体计算结果的最终确认，弄清最终安全性和声称的功能安全等级。

8.5.5 应评审此时的功能安全管理。

故障来源

功能安全标准通常会识别两种故障，然后提出故障解决方法。

随机硬件故障最容易理解，顾名思义，是由设备随机意外故障造成的。随机故障引起的故障概率以系统的PFH（危险故障平均频率）表示。容许PFH取决于所需要的SIL，范围从SIL 1级10^{-5}/h到SIL 3级10^{-7}/h。

系统故障是指设计中固有的故障，也就是说，只能通过设计变更予以修复。EMC稳健性不足可被视为系统错误，要求中的缺陷、验证和确认不足以及所有的软件错误，也是如此。系统错误是所生产的每个部分存在的有效缺陷，而不是单个装置中出现的缺陷。如果出现特定情况，发生故障的概率将达到100%。

为了使设备适合在需要SIL X安全功能的情况下使用，则须同时达到相关标准针对该SIL等级提出的随机和系统化要求。只达到硬件要求，是不够的。

8.6 评估计划

8.6.1 应制定评估计划（认证或测试计划），识别需要评估的全系统（整机）、子系统或部件/独立式机器的各个方面。

8.6.2 评估计划应识别确保在评估通用安全和功能安全时对所有预期设计领域做出适宜规定的指定参考标准/确认方法。

8.7 认证技术评审

8.7.1 认证技术评审应包括评审符合性评估流程的输出和结果，确定已评估和确认的结果符合附录A到附录F中规定的必要限值以及在以下工作中声明的结果和限值：

- 评估计划
- 评估前的设计依据评审
- 设计评估
- 设计确认
- 设计验证

8.8 认证

8.8.1 应依据Intertek内部程序SMS-FS-OP-19和Intertek专有标准INT/FS/2019，执行认证流程，授予Intertek功能安全标志。关于最终认证评审，在确认已圆满完成技术评审的各个部分并达到所有标准后，Intertek将授予功能安全标志。

intertek
Total Quality. Assured.

第9条

功能安全管理

9.1 IEC 61508和IEC 61511系列标准要求进行功能安全管理。功能安全管理基础设施，应在现场考察检验阶段予以审核。

9.2 目标是评估已执行的生命周期模型，即在整个生命周期内哪些部分具有相关性，明确责任，规定建立文件编制框架的管理和技术活动。

9.3 形成文件的功能安全管理计划应促进和展示对标准的符合性，计划验证、确认和评估活动，提供能在整个生命周期内保留的"有效"策划文件。

9.4 功能安全管理计划的典型纲要应当包括：

- 相关人员的责任
- 有文件证明的生命周期
- 验证计划
- 确认计划
- 质量策划

9.5 该计划一定要适合公司的广泛风险管理框架背景，不应孤立对待。功能安全系统使得出总体风险管理策略的风险降低因素生效。

9.6 该计划的结构可能需要许多层面的功能安全管理策划：

- 全公司总体计划
- 针对各操作设施的计划
- 特定项目的项目计划

9.7 系统供应商可能有计划，与质量流程相似，只涵盖其工作范围。拥有质量计划的公司，通常会针对各个项目制定项目执行计划。

9.8 文件/生命周期计划识别生命周期中的哪些阶段适用所策划的工作范围，即：

- 概念设计和要求制定
- 系统设计和工程
- 测试（FAT, SIT, SAT）
- 安装和调试
- 操作、维护和持续改进

9.9 被识别为功能安全管理计划和结构输出的主要文件包括：

- 风险分析（设计FMEA）
- 安全要求规范（SRS）
- 详细设计规范
- 测试规范

9.10 安全要求规范（SRS）是整理许多要素的结果，包括：

- 控制和防护措施理念
- 架构规范
- 危险与可操作性分析（HAZOP）报告
- SIL确定报告
- 因果图
- 功能规范
- 陈述
- 范围、警报和跳闸设定计划
- 重写

9.11 需要详细设计规范，详细设计中的常见要素为：

- 硬件制作规范和图纸
- 软件架构
- 软件标准
- 详细功能要求
- 详细非功能要求

9.12 质量计划的考虑事项包括：

- 管理能力
- 程序 - 内部操作程序
- 技术和措施
- 供应商质量
- 分包商和第三方承包商
- 变更管理 - 设计变更
- 跟踪和可追溯性
- 配置管理
- 问题管理（投诉）
- 事件和绩效分析
- 功能安全审核和评估

9.13 功能安全管理计划的关键要素，在图1.12中详述：

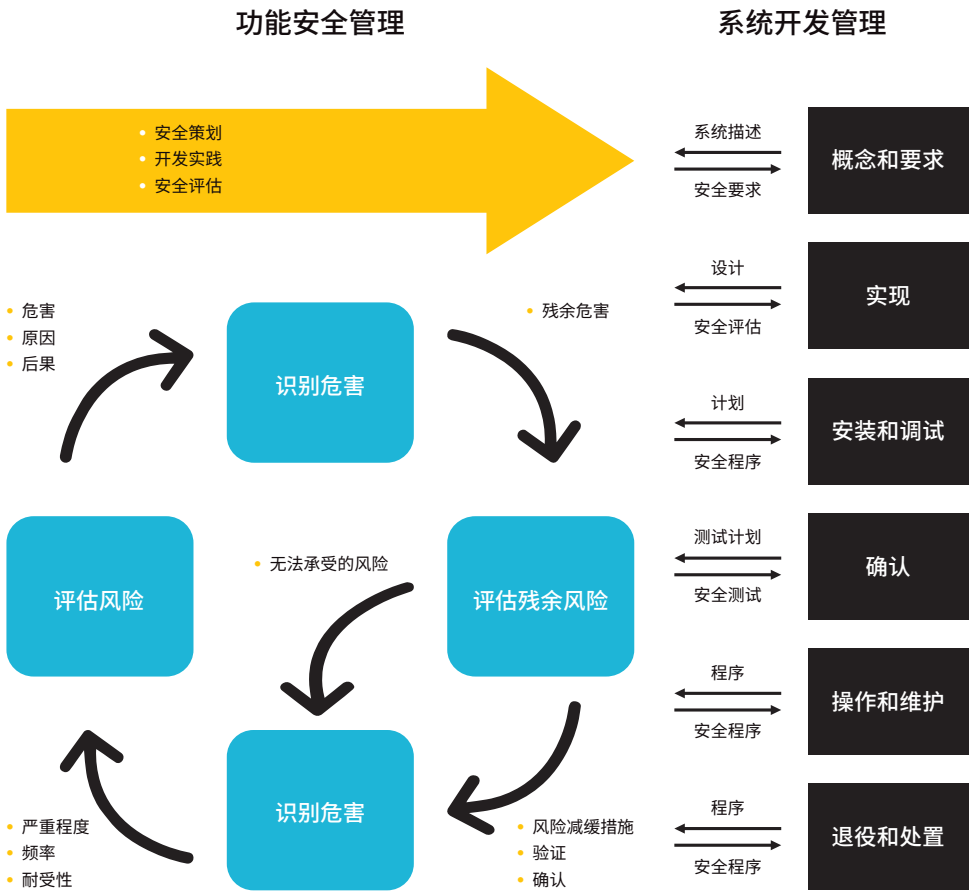


图1.12（功能安全管理流程）

第10条

常见
缩略语

缩略语	含义/说明
SIL	**安全完整性等级** 详细说明设备或元件必然要求的四个等级之一。
CCF	**共因故障** 一项特定事件或根本原因致使设备两个或多个元件出现故障。共因故障是指不属于连锁故障（CF）的从属故障（DF）。
CF	**连锁故障** 设备元件故障致使该设备另一个或另一些元件发生故障。连锁故障是指不属于共因故障（CCF）的从属故障（DF）。
CMF	**共同模式故障** 多个装置以相同模式发生故障的一种共因故障（ CCF）。分析时，采用故障树分析（FTA）。
DC	**诊断覆盖率** 通过已实施的安全机制探测或控制的硬件元件故障率。
DCLS	**双核锁步处理器** 同时并行同一套操作的处理系统。
DF	**从属故障** 同步发生或连续发生概率不能以每种故障无条件概率的简单乘积表达的故障。从属故障包括共因故障和连锁故障。
DFA	**从属故障分析** 旨在识别可能忽视或废弃必要独立性或给定元件之间无干扰、违反安全要求或安全目标的单一事件或单一原因。
DIA	**开发接口协议** 客户与供应商之间的协议，明确规定对各项活动的责任、证据或各方需要交流的工作成果。
DTI	**诊断测试时间间隔** 通过安全机制执行在线诊断测试间隔的时间。
E/E/PE	**电气、电子和可编程电子** IEC 61508-4在电气和/或电子和/或可编程电子技术基础上对此做出定义。

缩略语	含义/说明
EMI	**电磁干扰：紊乱** 外部来源产生的电磁感应或电磁辐射对电路的影响。
EOS	**电气过应力** 电气过应力故障可分为热诱导故障、电迁移相关故障和电场相关故障。可能造成闭锁短路。
ESD	**静电释放** 电气过应力（EOS）的子类。因相互接触、短路或介质击穿造成两个充电物品之间陡然产生电力流。
FIT	**单位时间故障** 装置运行10亿小时（1x10^9）内预计可能发生的故障次数。 两次故障之间的平均时间（MTBF）= 1,000,000,000 x 1/FIT
FMEA	**失效模式及后果分析** 与故障树分析（FTA）相反，失效模式及后果分析（FMEA）是一种归纳法，重点关注系统的各个零件、这些零件如何会发生故障以及这些故障对系统的影响。从可能导致错误和故障的缺陷开始分析。
FMEDA	**失效模式影响与诊断分析** 详细确定错误原因及其对系统的影响的程序，为了及早识别缺陷，在系统开发早期阶段采用可能会非常有效。
FTA	**故障树分析** 与失效模式及后果分析（FMEA）相反，故障树分析（FTA）是一种演绎法（由上至下），从系统不良行为开始分析，确定可能造成这种行为的原因。
FTTI	**故障容错时间间隔** 故障发生与系统过渡到安全状态、随时可能经历另一种危害之间的时间。 FTTI最大值 = DTI + 故障反应时间 + 安全状态
HSI	**硬件/软件接口** 输入输出信号诊断分析软件/硬件兼容性。
MBU	**多比特翻转** 同一个词内出现两个或多个错误比特。无法通过简单的单比特予以更正。
MPFDI	**多点故障探测区间** 在可能引发多点故障之前检测多点故障的间隔时间。
SEL	**单粒子锁定** 造成瞬时故障的单粒子翻转（SEU）产生的一种单粒子效应（SEE）。这种瞬时故障非常严重，只能通过动力循环予以更正。
TD	**工具错误探测** 对防止软件工具发生故障、产生相应错误输出的措施或者探测软件工具已发生故障、已产生相应错误输出的措施的信心。

第11条

客户提供的
技术文件和技术规范

第11条中的表格列示整机、(全系统)子系统和部件/独立式机器符合ISO 12100输出和设计失效模式影响与分析(FMEA)时为支持控制设备(EUC)风险评估缓解输出而提供的设计和技术文件。

注：以下表格中列出的所有参考文件不可能都适用，但若适用于控制设备，则应提供。

控制设备ISO 12100风险评估技术文件和技术规范(若适用)
控制设备在静态/动态负载(应力/应变负载表)、材料、震动、排放、有害物质、辐射以及对环境的影响等方面的机械设计计算和规范
液压与气动系统、集成或独立式工业机器人、焊接/制作而成的组件、切割系统(研磨、热力、隔音或液压)的设计规范和示意图
与结构稳定性、基础类型及负载应力、环境外力相关的设计规范
结构设计规范和计算 - 控制设备在商品成本(CoG)、负载、SWL/MWL/YWL计算、吊装点等方面的设计规范
与控制设备所用的或释放的任何化学有害物质相关的规范
通过相关安全相关参数，确认设计规范和控制设备计算值
电气安全：符合 IEC 60204的控制设备设计规范，包括电气系统布局、示意图电气布线应力负载计算值/表、已识别的关键部件以及安全认证(若有)。部件 PL和SIL(若有)、电气绝缘分类
控制设备的网格代码连接、可达性/蠕变及间隙考虑事项等技术规范 (若适用)
与控制设备相关的设计和计算(SIL)，控制IEC 61508 -1和-2 (E/E/PE)系统，部件安全设计规范，SIL(若有)计算
与控制设备电子器件：模拟/数字电子系统和部件的设计规范和示意图，包括静态负载/脉冲负载、偏差、时钟排序和PCB人口层面有源控制安全链/安全回路
控制设备软件 - IEC 61508 -3，安全相关功能的设计规范和线性或流式布局，比如安全状态、故障指示、错误处理、传感器故障探测、故障分析监控、在线自诊、软件修订/上传、功能接口、软件通信修订 - 安全状态

控制设备ISO 12100风险评估技术文件和技术规范(若适用) - 续
控制设备软件系统形态能力，包括独立等级、安全数据兼容性、数据接口(外部系统)、非一致数据、已损坏数据、数据未经授权访问及人员未经授权访问
包括硬件的所有运行模式和功能、设置/校准、系统架构、硬件集成和系统能力、性能/响应时间、设备/操作员接口及自诊能力等
人体工程学，与局部环境(照明、出入口、可视显示)相关的规范，访问控制/显示
机器设置、前置机设置、校准、安全措施 - 检查、操作、运行模式、原材料处理、运行控制、运行参数、操作手册、管理控制和最终产品验证等设计规范/指导书
调试、机器装配、调整、连接系统、电源连接、演示(试运行)、准备、预维护、固定件(锚固件)、基础准备、无负载运行、最大负载运行等相关技术文件
维护手册，包括一般内务整理 - 清洁/润滑/液面、拆卸/重新组装、工具更换、重置/调节、修理/改良、故障查找及故障模式流程
指导书，包括运输装载、包装、运输、卸载、拆包、拆卸/解除和处置计划等

条款	控制设备ISO 13489-1技术文件和技术规范
4.4	控制系统安全相关部件的设计布局和结构【部件层面(所有相关机械/电气/电子部件)】
4.5.1	与所有控制系统安全相关部件相关的技术规范，引用 PL、MTTFd、DC、CCF、结构等声称内容
	失效模式及后果分析(FMEA)
	软件ID代码、系统故障、环境状况声称、性能等级定性方法、架构约束。
4.5.2	性能等级计算方法 - 来自制造商资料、附录C和附录D中的表格、生命周期能力(年数)
4.5.5	类别计算/声称性能等级计算
4.7	性能等级验证计算方法得出：PLr和PL(子控制系统安全相关部件) >= PLr
6.2.2	控制系统安全相关部件架构块结构文件
6.3	控制系统安全相关部件组合PL CAT的方法和论证

条款	控制设备ISO 13489-2技术文件和技术规范
4.2	控制设备总体确认计划
4.3	控制设备一般系统故障列表及规定限值
4.4	控制设备特殊故障列表以及每种故障的缓解措施
4.5	控制设备系统确认（整个系统的软件、性能等级计算）
5	控制设备系统确认方法 - 包括所采用的确认技术
6	控制设备最终产品测试/确认计划
7和8	与控制设备安全功能相关的技术文件 - 安全功能要求规范。对安全功能进行测试和分析的确认计划
9	控制设备采用的类别规范确认方法、MTTFd/DCavg/CCF确认、与性能等级和控制系统安全相关部件类别相关的系统故障措施确认。安全相关软件确认、性能等级确认和验证。组合安全相关部件确认
10, 11, 12	提供环境分析、维护、最终用户操作指导书的控制设备确认计划

IEC 62061需要提交的文件	
所需信息	子条款
功能安全计划	4.2.1
SRCF要求规范	5.2
SRCF功能安全要求规范	5.2.3
SRCF安全完整性要求规范	5.2.4
SRECS设计	6.2.5
结构化设计流程	6.6.1.2
SRECS设计文件编制	6.6.1.8
功能块结构	6.6.2.1.1
SRECS架构	6.6.2.1.5
子系统安全要求规范	6.6.2.1. 7
子系统实现	6.7.2.2
子系统架构（元件及其相互关系）	6.7.4.3.1.2
估算故障容许度/SFF时声称的故障排除	6.7.6.1c)/6.7.7.3
子系统组件	6.7.10
软件安全要求规范	6.10.1
基于软件的参数化	6.11.2.4
软件配置管理项	6.11.3.2.2
软件开发工具的适宜性	6.11.3.4.1
应用程序文件编制	6.11.3.4.5
应用软件模块测试结果	6.11.3.7.4
应用软件集成测试结果	6.11.3.8.2
SRECS集成测试文件编制	6.12.1.3
SRECS安装文件编制	6.13.2.2
安装、使用和维护文件编制	7.2
SRECS确认测试文件编制	8.2.4
SRECS配置管理文件编制	9.3.1

条款	控制设备IEC 61508-1技术文件和技术规范
7.3.2	控制设备相关信息、预期运行环境和已识别危害
7.4.2 7.5.2	阐明控制设备代表性危害和风险分析范围的信息
7.6.2 7.7.2	依据安全功能要求和安全完整性要求制定的整体安全要求规范。总体安全功能分配信息，详述目标故障措施以及针对需要在控制设备整个寿命期管理的其他风险降低措施做出的相关安全完整性等级假设
7.8.2 to 7.15.2	总体安全要求分配信息和结果 电气/电子/可编程电子安全相关系统的安装计划；电气/电子/可编程电子系统安全要求规范 电气/电子/可编程电子安全相关系统的安装计划；电气/电子/可编程电子安全相关系统的调试计划 完全安装的电气/电子/可编程电子安全相关系统；电气/电子/可编程电子安全相关系统总体安全确认计划 总体安全要求分配信息和结果，包括安装和维护

条款	控制设备IEC 61508-2技术文件和技术规范
7.2.2	电气/电子/可编程电子系统设计要求和规范，描述电气/电子/可编程电子系统的设备和架构
7.3.2	电气/电子/可编程电子安全相关系统的安全确认计划
7.4.2 to 7.4.11	符合电气/电子/可编程电子系统设计要求规范的电气/电子/可编程电子安全相关系统设计，电气/电子/可编程电子系统集成测试计划，以可编程电子系统架构信息作为软件要求规范输入
7.5.2	符合电气/电子/可编程电子系统设计要求、功能完善的电气/电子/可编程电子安全相关系统；电气/电子/可编程电子系统集成测试结果
7.6.2	针对每个独立电气/电子/可编程电子系统的电气/电子/可编程电子系统安装、调试、操作和维护程序
7.7.2	彻底经过安全确认的电气/电子/可编程电子安全相关系统，电气/电子/可编程电子系统安全确认结果
7.8.2	电气/电子/可编程电子系统改良结果
7.9.2	如上文所述，取决于阶段，每个阶段的电气/电子/可编程电子安全相关系统验证结果
8	电气/电子/可编程电子系统功能安全评估结果
7.2.2	在电气/电子/可编程电子系统安全要求规范（源自 IEC 61508-2）分配（参见 IEC 61508-1）过程中制定的电气/电子/可编程电子安全要求规范

条款	控制设备IEC 61508-2技术文件和技术规范 - 续
7.3.2	控制设备软件安全要求规范
7.4.3	控制设备软件安全要求规范；电气/电子/可编程电子系统硬件架构设计（源自IEC 61508-2）
7.4.4	控制设备软件安全要求规范；软件架构设计
7.4.5	控制设备软件架构设计；支持工具和编码标准
7.4.5	控制设备软件系统设计规范；支持工具和编码标准
7.4.6	控制设备软件模块设计规范；支持工具和编码标准
7.4.7	控制设备软件模块测试规范；源代码列表；代码审查报告
7.4.8	控制设备软件系统集成测试规范；软件
7.5.2	控制设备软件架构集成测试规范；软件/可编程电子集成测试规范（IEC 61508-2也要求提供） 经过集成的可编程电子系统
7.6.2	控制设备设计和验证计划及上述规范
7.7.2	系统安全软件方面的控制设备确认计划
7.8.2	控制设备软件改良程序；软件改良按需更新
7.9.2	控制设备适当验证计划（取决于阶段）
8	控制设备软件功能安全评估