intertek
Total Quality. Assured.

功能安全

安全控制的最佳工程实践

功能安全目的在于确保系统正常发挥其性能并良好运作。Intertek提供的功能安全服务覆盖从差距分析、功能安全管理，到安全确认、验证、功能安全评估及认证，能够在整体/系统/软件的全生命周期为您提供支持，从而使您的产品得到优化和安全保障。

功能安全是一种全面分析，评估产品开发的全生命周期，由此确定产品的硬件及软件如何相互作用，以及确定产品如何响应用户输入信息和预期的运行环境。

这些系统通常涵盖传感元件、逻辑控制元件以及执行元件。

这些系统通常以以下几种指标进行评价：安全完整性等级(SIL)、性能等级(PL)、声明的安全完整性等级(SILCL)、硬件故障裕度(HFT)、安全失效分数(SFF)、类别架构(Category)、软件分类(software Class)等。

涉及的相关标准可能包含：

- IEC 61508 电气电子可编程电子安全相关系统的功能安全
- IEC 62061 机械安全 - 安全相关的电气电子可编程电子控制系统的功能安全
- ISO 13849 机械安全 - 控制系统的安全相关部件
- IEC 61800-5-2 可调速的电驱动系统 - 第5-2部分：安全要求 - 功能
- ISO 25119 农林拖拉机和机械 - 控制系统的安全相关部分
- IEC 60730-1 家用和类似用途电自动控制器第1部分：通用要求
- IEC 60335-1 家用电器及类似电器的安全 第1部分：通用要求等等

功能安全适用于所有行业，并且，随着制造商和终端用户期望进一步的降低产品/系统的风险，功能安全方面的需求逐渐增加：

- 产品设计师以及企业都希望确保以安全并且成功的方式创造和经营产品
- 制造商希望自己生产的产品能满足具体的欧洲指令及要求，或者满足由贸易协会、保险公司或监管机构(例如：美国职业安全与健康管理局(OHSA))在功能安全方面的建议
- 嵌入式系统的技术发展及其应用普及，覆盖其软硬件开发过程的功能安全逐渐成为产品基本要求
- 不断更新的产品标准将功能安全要求纳入其中
  - 工业机器人 ISO 10218
  - 自动导引车(AGV) ISO 3691-4, UL 3100
  - 分布式发电用电力变换器 UL 1741
  - 电动自行车助力车 EN 15194, UL 2849
  - 个人轻型交通工具 UL 2272
  - 电池 IEC 62619, UL 1973, UL 2271
  - 储能系统 UL 9540
  - 电动工具 EN 62841
  - 制冷系统和热泵 EN 378-2
  - 自动扶梯 EN 115等

Intertek竭诚助您开发、创建、实施和运行优质的功能安全体系。一个稳健、高效的系统离不开以下文档及其体系整合：

- 功能安全文化与企业级管理
- 人员的授权与分派
- 风险及危害分析
- 安全需求规格
- 确认及验证的计划与实施
- 软硬件详细设计文档与测试
- 失效模式及影响分析
- 质量管理措施
- 配置/变更管理
- 安全手册
- 功能安全复审、审核与评估

功能安全是整体安全的一部分，它依赖于一个系统或设备对其输入的正确响应。

- IEC 61508-4 章节3.1.12

Printed in Shanghai, 08/2020

功能安全

Intertek在开发和指导功能安全系统方面积累了丰富的专业知识和经验，可以为您提供无与伦比的精湛知识，从而助您满足以下需求。

相关服务包括：

- 差距分析
- 流程整改建议与技术支持
- 具备独立性的功能安全评估及认证
- 流程及文档的组织完善
- 安全链管理(审核、检验、质量管理、生产效率/卓越运营、文件支持)
- 系统级别的计划开发，包括：从功能安全概念，到软硬件开发
- 产品及测试设计故障排除与建议
- 法规及认证要求的识别及相关解决方案

您的业务及运营将获益如下：

- 更深入地了解流程及产品可行性，从而更迅速地进入市场
- 通过减少故障和返工，以此降低价格成本及时间成本
- 使得产品符合所有相关的以及必须遵守的标准和规范
- 使公司持续拥有具有相关技能及洞察力的员工。通过现场培训、虚拟培训和定制培训，培训员工更顺畅、更迅速地推出产品
- 以更少的产品型号进驻更多市场，从而扩大并且简化全球扩张的难度

关于Intertek天祥集团

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。

标准体系简介

标准号/标题	应用范围
IEC 61058 电子电气可编程电子安全相关系统的功能安全	为其他功能安全标准的基础。针对由电气/电子/可编程电子部件构成的、起安全作用的电气/电子/可编程电子系统的整体安全生命周期，建立了一个基础的评价方法。
ISO 13849 机械安全 - 控制系统的安全相关部件 IEC 62061 机械安全 - 安全相关的电气电子可编程电子控制系统的功能安全	规定了机械设备中安全相关控制系统在设计和确认方面的要求。在机械领域，实现的方式可能包含复杂电子/电气，也可能涉及接触器/继电器以及流体动力系统(气动、液压)等。
IEC/EN 61800-5-2 可调速的电驱动系统 - 第5-2部分：安全要求 - 功能	针对伺服控制系统的安全开发生命周期提供了指导，是安全伺服产品的功能安全评估指南。标准定义了集成安全驱动的各类安全功能，如安全扭矩关断(STO)、安全停车1(SS1)、安全停车2(SS2)等。
ISO 25119 农林拖拉机和机械 - 控制系统的安全相关部分	特别针对农林拖拉机和机械的控制系统，结合车辆与机械行业的功能安全理念，建立了覆盖功能安全计划直至确认验证与生产的软硬件全生命周期的综合评价方法。
IEC 60730-1 家用和类似用途电自动控制器第1部分：通用要求 IEC 60335-1 家用电器及类似电器的安全 第1部分：通用要求	应用于家用和类似用途控制器。尤其在软件功能安全方面提出了细致的分类与要求。

联系我们

400 886 9926

service.china@intertek.com

intertek.com.cn

Printed in Shanghai, 08/2020