

Research on Testing Technology of System Functional Safety

王春喜 欧阳劲松

(机械工业仪器仪表综合技术经济研究所, 北京 100055)

摘要: 介绍了功能安全的定义和现有国际、国内功能安全标准, 分析了进行系统功能安全测试的必要性。总结了系统功能安全测试的关键技术, 包括基于功能安全的安全标准体系、安全完整性等级、整体安全生命周期。正在筹建的系统功能安全测试实验室将是一家开展系统功能安全测试的实验室。

关键词: 功能安全 安全完整性等级 风险 安全生命周期

中图分类号: TP302

文献标识码: A

Abstract: The definition of functional safety, the international and national functional safety standards and the necessity of system functional safety test are introduced. Key technologies of system functional safety test are summarized. These include safety standard architecture, integrated safety level and integrated safety lifecycle. The "Testing Lab for System Functional Safety" which is being established by ITEI (instrumentation technology and economy institute) will be the national lab to proceed the system functional safety test.

Keywords: Functional safety Safety Integrated level Risk Safety life cycle

0 引言

安全技术的目标是通过应用和使用适当的技术, 把对人类和环境存在的潜在危险降至最低。今天, 安全技术经常应用于许多不同的领域, 比如机械、煤矿、石化、电力和和铁路领域。在这些场合, 人员的健康和安全的、工厂设备的保护、环境的保护都依靠实现安全技术的自动控制产品和系统能够正确执行其功能, 这就是系统功能安全所要实现的目标。为了达到设备和工厂安全功能, 受保护的和控制设备的安全相关部分必须正确执行其功能, 而且, 当失效或故障发生时, 设备或系统必须仍能保持安全条件或进入到安全状态。同时, 为了实现这一点, 还需要采用系统功能安全测试技术, 使系统满足相关标准的要求。

1 功能安全定义

从保护对象的观点来看, 安全性是不可分割的一部分。造成危险的原因和避免危险的技术方法有很大区别。通过弄清潜在危险的原因, 针对不同的安全类型有不同的适用方法。例如: 术语“电气安全”被用于需要防护电气危险的安全性; 而术语“功能安全”被用于依赖正确功能的安全性。如图 1 所示。

在 IEC 61508 中, 功能安全被定义为“与 EUC (控制设备) 和 EUC 控制系统有关的整体安全的组成部分, 它取决于 E/E/PE (电气/电子/可编程电子) 安全相关系统、其它技术安全系统和外部风险降低设施功能的正确执行。”

衡量达到功能安全等级的方法是事件发生的概率, 这些事件包括: 危险的失效、故障容错性、危害程度和通过避免系统故障来保证的质量等。在不同标准中, 会使用不同的术语来表示: 在 IEC 61508 中使用“安全完整性等级 (SIL)”, 在 EN 954 中使用“类 (categories)”, 在 DIN V 19250 和 DIN V VDE 0801 中使用“需求等级 RC (requirement class)”。

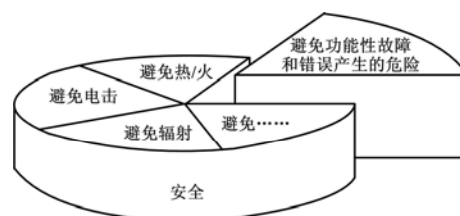


图1 安全分类示意图

2 功能安全标准

2.1 功能安全国际标准

现有的功能安全国际标准有:

ISO/FDIS 12100-1 & ISO 14121 Safety of machinery-Principles for design and risk assessment (基础标准, 用于安全相关的电气、电子和可编程电子控制系统设计和风险评估);

ISO 13849-1,-2 Design of safety-related parts of machinery control systems (用于非电气子系统设计);

IEC 60204-1 Safety of electrical equipment of machinery (用于通用电器安全方面);

IEC 62061 Functional safety of SRECS for machinery (用于机械的电气控制系统设计);

IEC 61508 Functional Safety of E/E/PE safety-related systems (用于复杂子系统设计);

IEC 61511 Functional safety-safety instrumented systems for the process industry sector (用于过程工业安全测量系统设计);

IEC 61784-3 Data communications for measurement and control-Part3: Profiles for functional safety communications in industry networks （用于工业网络功能安全通信）（制定中）。

2.2

现有的功能安全国内标准有：

- ① 《电气/电子/可编程电子安全相关系统的功能安全》系列标准（已报批）；
- ② 《PROFIsafe 安全技术行规》（制定中）；
- ③ 《过程工业部门仪表型安全系统的功能安全》系列标准（制定中）。

3 系统功能安全测试的必要性

功能安全是保障工业自动化网络正常运行的基础，如何有效地保证系统的各个部件在整体安全生命周期中可靠工作，是目前工业自动化领域面临的新课题。目前国内还没有科学的标准规范在自动化控制系统的“全安全生命周期”内对系统进行有效的安全保证。

进行系统功能安全测试的主要目的为：

- ① 用最先进的技术手段改进国家安全和经济安全功能；
- ② 使用一种基于风险分析来确定安全完整性等级的方法使安全要求和安全设计量化、规范化；
- ③ 提供一个在产品和系统设计时，可以从整体安全生命周期、E/E/PES 安全生命周期以及软件安全生命周期的各阶段确定安全相关系统安全功能要求的方法；
- ④ 针对飞速发展的技术，建立一个足够完善并能广泛满足未来发展要求的工业控制网络安全技术框架，使其既可直接应用于工业，也可指导各领域安全标准的制定，使将来其它相关安全标准的起草具有一致性（如基本概念、技术术语和对规定安全功能的要求等）；
- ⑤ 建立一个协调一致的安全标准，以增进各领域产品和系统的安全功能，改进安全通信及安全要求（如增加对实际安全要求的透明度），发展用于各领域的安全技术、安全测试和安全认证，提供产品和系统安全一致性评价服务。

4 系统功能安全测试关键技术

功能安全测试的目标在于增加工业自动化系统功能安全方面的测试设备及测试软件，使之能够对基于先进控制网络的控制系统进行系统功能安全方面的测试，为工业自动化产品的用户提供产品功能安全评估报告，降低用户使用先进技术风险。因而根据现有现场总线技术和功能安全标准，建立一套针对自动化产品（系统）的整体安全生命周期的功能测试系统将是其最终目标。

综合功能安全实现的三个关键要素（功能安全管理、技术规范、人员竞争力）、安全生命周期概念和安全完整性等级(SIL)，系统功能安全测试方法如图2所示。

从图2可以看出，系统功能安全测试是基于功能安全技术标准的制定、安全完整性等级（SIL）的计算和安全生命周期的划分来实现的；另外，该测试方法也可以进一步发展作为工业控制网络系统功能安全设计方法，据此基于给定的安全需求等级和用户现场条件设计合适的工业安全应用系统。

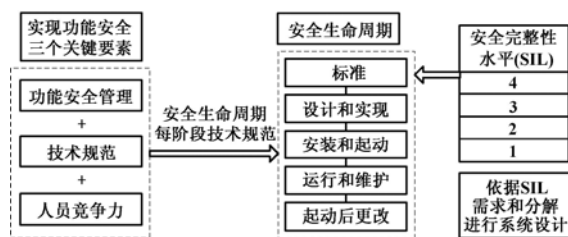


图2 系统功能安全测试方法

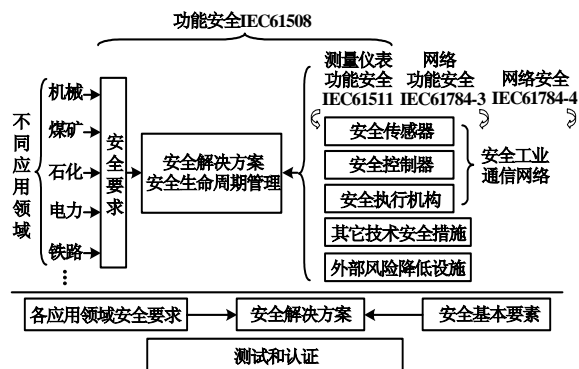


图3 安全标准体系

4.1 基于功能安全的安全标准体系

功能安全标准引出了一种非常重要的新技术，它是可靠性技术在系统功能安全领域的延伸，解决了困扰工业界多年的对系统要执行的功能进行安全评价和管理的理论和实践问题，在系统安全性与部件（软硬件）、子系统、网络的可靠性之间建立了量化关系。功能安全标准为国家进行工业生产的安全监管提供了理论依据，为企业进行安全控制提供了手段和方法。

全国工业过程测量和控制标准化技术委员会（SAC/TC124）正在将 IEC 61508 系列标准转化为中国国家标准。同时国内迫切需要针对功能安全在各工业领域的应用制定相应标准，最终形成我国基于功能安全的安全标准体系，其基本框架如图3所示。

如图 3 所述, 相关的安全标准、安全产品及行业经验组成了基于功能安全的工业安全标准体系的基础, 这三者的结合产生了不用应用领域的安全解决方案, 进而, 要保证这个应用框架下的安全产品、安全系统和安全解决方案能够正确执行和持续完善, 那么就必须提供系统功能安全测试。

4.2 安全完整性等级 (SIL)

安全完整性等级 (SIL) 被定义为在规定的周期内的所有规定的条件下, 安全相关系统成功完成所需安全功能的概率。该概率是由风险作为度量指标的。风险定义为危害发生的概率和危害严重性的组合。

风险的表达式为

$$\text{风险}(R) = \text{严重性}(S) \times \text{频度}(P)$$

式中: 严重性表示发生一次事故造成的损失数值; 频度表示在一定时间或生命周期内事故发生的次数。

IEC 61508 定义了被控装置风险、可容忍的风险、残余的风险和必须的风险降低等 4 种风险指标, 如图 4 所示。

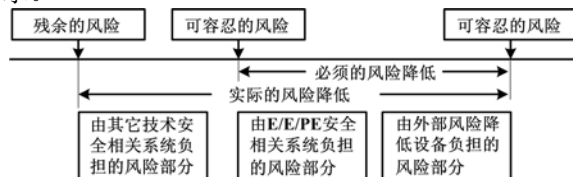


图4 风险指标关系

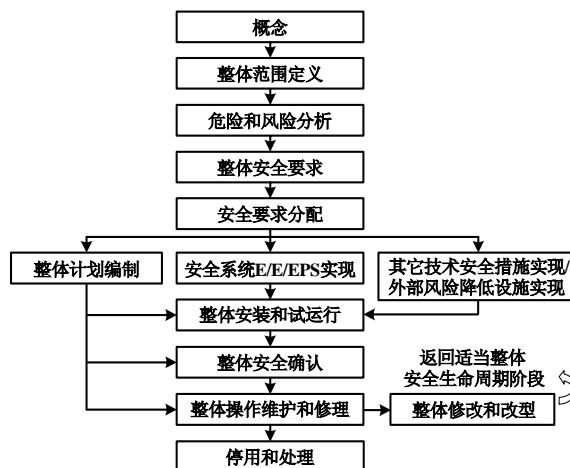


图5 整体安全生命周期技术框架

4.3 整体安全生命周期

安全生命周期被定义为从方案的确定阶段开始到所有的电气/电子/可编程电子安全相关系统、其它技术的安全相关系统、外部风险降低设备不再可用时为止, 这个时间周期叫安全生命周期。为了系统地实现达到要求的 E/E/PE 安全系统安全完整性水平所需的全部活动, 需采用一种整体安全生命周期的技术框架, 如图 5 所示。

5 结束语

世界标准化机构 (如 IEC、ISO、EN 等) 在过去几年中相应地制定了多项系统功能安全标准; 另外, 各发达国家 (如德国、英国、美国、日本等) 为了保证其工业控制网络安全、人员安全以及环境安全, 都制定了相应的安全法规和措施。

这些功能安全标准的制定使得现场总线开发商们为用户提供安全现场总线和相关解决方案成为可能。因此, 近年来多家国际自动化领域的大公司都提出了符合国际功能安全标准的现场总线功能安全技术, 如西门子公司的 PROFIsafe、罗克韦尔公司的 CIP Safety、三菱公司的 CC-Link Safety、菲尼克斯公司的 Interbus Safety 等。同时这些大公司致力于开发相应的功能安全产品, 在原有的现场总线及工业以太网基础上形成安全集成的工业控制网络系统。这些功能安全技术、产品和解决方案已成为当今自动化领域的新热点和核心竞争力。

以前, 我国的安全技术主要关注的是单一产品的安全性能。但是, 不同生产厂商的单一安全产品集成成为系统后的安全性, 以及当某些设备出现故障时系统整体的安全性, 都没有确切的评价依据。系统功能安全技术在世界工业自动化领域是最先进的技术, 其相应测试设备和测试环境要求也很严格。目前, 机械工业仪器仪表综合技术研究得到国家重点课题资金资助, 正在筹建“系统功能安全测试实验室”。该实验室的建设将可以依据国际标准和相关的国家标准, 为由国内外不同安全产品组成的系统进行功能安全的量化评估, 并指出在不同状态下系统可以达到的安全等级, 对重大装备以及有较高安全要求的厂矿安全运行具有十分重要的意义。

参考文献

- 1 IEC. Functional Safety of Electrical/Electronic/Programmable Electronic Safety - Related Systems.
- 2 王春喜, 王玉敏. 工业安全技术研究[J]. 仪器仪表标准化与计量, 2004, (6).
- 3 王春喜. 功能安全标准及应用研究[J]. 山东大学学报 (工学版), 2005, (6).
- 4 王春喜. 过程工业部门仪表型安全系统的功能安全[J]. 仪器仪表标准化与计量, 2005, (6).

收稿日期: 2006-03-22。

第一作者王春喜, 男, 1974 年生, 2004 年毕业于北京交通大学获博士学位, 工程师; 主要从事工业自动化功能安全的研究及现场总线标准的制定等工作。