ICS 25.040
CCS N 10

中华人民共和国国家标准

GB/T 41295.2—2022

功能安全应用指南
第2部分:设计和实现

Application guide of functional safety—Part 2:Design and realisation

2022-03-09 发布　　2022-10-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件是GB/T 41295《功能安全应用指南》的第2部分。GB/T 41295已经发布了以下部分：

——第1部分：危害辨识和需求分析；

——第2部分：设计和实现；

——第3部分：测试验证；

——第4部分：管理和维护。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由中国机械工业联合会提出。

本文件由全国工业过程测量和控制标准化技术委员会(SAC/TC 124)归口。

本文件起草单位：上海辰竹仪表有限公司、机械工业仪器仪表综合技术经济研究所、国能智深控制技术有限公司、浙江中控技术股份有限公司、北京康吉森技术有限公司、上海辰竹安全科技有限公司。

本文件主要起草人：熊文泽、周婷、孟邹清、田雨聪、周有铮、裘坤、陈小全、黄之炯、左新、庞欣然、来晓、王璐、张亚彬、刘晓亮、徐神玲、刘瑶、帅冰。

引　言

自 GB/T 20438(所有部分)发布以来,电气/电子/可编程电子系统已经越来越多的应用于国内各个领域的安全控制和安全防护,包括石油、化工、电力、轨道交通、汽车、电梯/扶梯等。近年来随着智能制造的兴起,智能化设备(主要由电气/电子/可编程电子为技术基础)的安全问题逐渐成为一个新的研究方向和焦点,进一步提升了对功能安全技术的需求。

GB/T 20438(所有部分)给出了实现功能安全的基本框架和结构,作为等同转化的标准,与国内企业的管理体系和设计思路未能完全切合,加之很多国内工程技术人员都是初次接触功能安全技术,对于功能安全概念一时难以理解,这就造成虽然国际功能安全标准提出了非常好的安全理念和设计措施,但技术人员难以清楚的理解和认识。GB/T 20438(所有部分)发布 10 多年来,国内一些领先的科研院所和企业已经基于标准要求开展了很多工作,并积累了一定的经验。因此,基于国内目前已有的功能安全评估、功能安全设计、功能安全测试和功能安全管理实践形成本文件,以更好地指导功能安全相关系统的设计、分析、评估和运行维护。

GB/T 41295 拟制定 4 个部分:

——第 1 部分:危害辨识和需求分析。目的在于给出功能安全系统设计初期的危害辨识内容和需求如何产生的方法;

——第 2 部分:设计和实现。目的在于给出功能安全系统的软硬件设计和实现方法和实施指南;

——第 3 部分:测试验证。目的在于给出功能安全系统在生命周期过程各个阶段的测试导则和测试方法解读;

——第 4 部分:管理和维护。目的在于给出功能安全系统管理和维护过程的导则。

功能安全应用指南
第2部分:设计和实现

1 范围

本文件给出了设计和实现功能安全系统的指导措施,面向的对象包括安全传感器、安全逻辑控制器、安全通信总线和安全执行器等。

本文件适用于功能安全系统研发团队(如制造商),就开发出符合相应安全完整性能力的安全产品给出规范性指导;系统集成商、评估机构和用户用于对适当功能安全系统的选型和评价参照执行。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 19001—2016 质量管理体系要求

GB/T 20438.1—2017 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

GB/T 20438.2—2017 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

GB/T 20438.3—2017 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

GB/T 20438.4—2017 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

GB/T 20438.6—2017 电气/电子/可编程电子安全相关系统的功能安全 第6部分:GB/T 20438.2和GB/T 20438.3的应用指南

GB/T 34040—2017 工业通信网络 功能安全现场总线行规 通用规则和行规定义

GB/T 41295.3 功能安全应用指南 第3部分:测试验证

IEC 61508-3-1 电气/电子/可编程电子安全相关系统的功能安全 第3-1部分:软件要求 重复使用预先存在的软件元素来实现全部或部分安全功能(Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 3-1:Software requirements—Reuse of pre-existing software elements to implement all or part of a safety function)

3 术语和定义

GB/T 20438.4—2017界定的以及下列术语和定义适用于本文件。

3.1

功能安全系统 functional safety system

执行安全相关功能的系统,具有功能安全相关的特性,满足特定的安全完整性等级(SIL)。

注:这里的系统是一个广义的概念,包括不同的层次,如安全部件、安全设备或安全控制系统等。在实际的工业过程中,功能安全系统可能是一个变送器、继电器、安全可编程序控制器或安全仪表系统。

[来源:GB/T 41295.1—2022,3.6]