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]

3.2

功能安全系统研发团队　team for functional safety system research and development

执行功能安全系统设计研发的责任主体。

注：包括功能安全系统硬件开发人员、软件开发人员、验证测试人员、功能安全管理人员等。

3.3

功能安全系统制造团队　functional safety system manufacture team

执行功能安全系统生产制造的责任主体，它可能包括功能安全系统制造过程的装配人员、测试人员、管理人员、加工人员等。

注：为保证系统的安全功能正确制造，功能安全系统制造团队需要得到来自功能安全系统研发团队的有效协助。

3.4

故障插入测试　fault injection test

人为地在功能安全系统中产生一种故障模式，验证系统在故障状态下的响应情况是否符合安全要求的一种测试方法。

4　缩略语

下列缩略语适用于本文件。

ASIC：专用集成电路（Application Specific Integrated Circuit）

CMMI：能力成熟度模型集成（Capability Maturity Model Integration）

CPLD：复杂可编程逻辑器件（Complex Programmable Logic Device）

DC：诊断覆盖率（Diagnostic Coverage）

FMEA：失效模式与影响分析（Failure mode and effect analysis）

FMEDA：失效模式、影响与诊断分析（Failure mode，effect and diagnostic analysis）

FPGA：现场可编程门阵列（Field Programmable Gate Array）

FTA：故障树分析（Fault tree analysis）

HFT：硬件故障裕度（Hardware Fault Tolerance）

MooN：N 取 M 通道架构（M out of N channel architecture）

PFDavg：要求时危险失效平均概率（Average Probability of dangerous Failure on Demand）

PFH：危险失效平均频率（Average frequency of dangerous failure）

SFF：安全失效分数（Safe Failure Fraction）

SIL：安全完整性等级（Safety Integrity Level）

5　总则

5.1　功能安全系统的研发设计过程需要按照 GB/T 20438.2—2017 和 GB/T 20438.3—2017 等相关功能安全基础标准的要求开展功能安全系统研发和验证工作。为保证预期的 SIL 目标和要求得以切实实现，本文件给出了相关的应用指南。

注：某些领域有其特定领域的功能安全标准，这些领域的功能安全标准继承了 GB/T 20438.2—2017 和 GB/T 20438.3—2017 的整体架构和核心理念，因此在符合这些领域功能安全要求时，也可参考本文件的相关内容。

5.2　功能安全系统还宜满足其产品标准中关于基本安全（如电气安全）、环境适应性以及可靠性/稳定性的特定要求，这些要求是实现相应安全完整性的前提。

5.3　功能安全系统的生产制造过程需要考虑第 15 章或相关领域功能安全标准中的规定。

6 安全生命周期

6.1 一般原则

6.1.1 功能安全系统研发团队需要在安全研发的初期建立功能安全管理体系和定义安全生命周期阶段。

6.1.2 功能安全管理体系和安全生命周期的建立需要结合功能安全标准要求以及研发团队的已有经验。

6.2 应用考虑

6.2.1 功能安全管理体系需要考虑 GB/T 20438.1—2017 中第 6 章的要求，功能安全研发部门可以参考公司已有的质量/安全管理体系来建立功能安全管理体系。

注：GB/T 19001—2016 或 CMMI 等体系的构建和实施是实现功能安全管理的有力保障。

6.2.2 功能安全管理体系需要包含系统或软件变更的需求，需要考虑 GB/T 20438.2—2017 中 7.8 和 GB/T 20438.3—2017 中 7.8 的要求。当变更发生后，宜按照制定的变更规程执行影响分析，留存变更记录。

6.2.3 典型的安全生命周期过程需要考虑 GB/T 20438.2—2017 和 GB/T 20438.3—2017 中第 7 章的要求，功能安全系统研发团队按照该章的要求建立满足自己研发特性的安全生命周期。

6.2.4 功能安全系统实现过程的安全生命周期需求包括：系统设计要求规范（包括软件安全要求规范）、系统的架构设计、系统的详细设计和实现、软件设计和实现、系统集成（包括子系统软硬件集成和子系统间集成）、系统运行和维护规程（包括用户手册、安全手册等）、系统的安全确认（包括软件确认）、系统的制造。功能安全系统的安全生命周期见图 1。

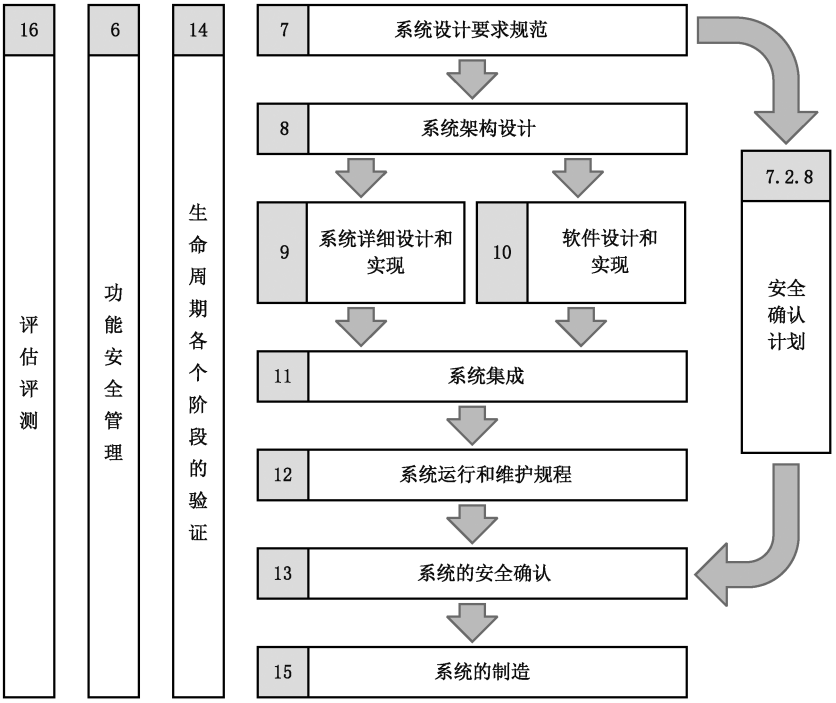

图 1 系统实现过程的安全生命周期

6.2.5 对系统的修改和验证的要求贯穿于以上生命周期的所有阶段。

7 系统设计

7.1 一般原则

7.1.1 功能安全系统设计要求规范的基本要求需要考虑 GB/T 20438.2—2017 中 7.2 和 B.1 的要求。

7.1.2 系统设计要求规范中需要包括系统的所有设计要求，包括安全相关要求和非安全相关要求。宜将安全相关要求和非安全相关要求明确区分开来，对于非安全相关要求可以不必按照生命周期后续活动执行。

7.1.3 对与某些与应用联系非常紧密的产品（例如，轨道交通产品，汽车电子产品），安全要求和非安全要求的界定需要根据具体的应用加以分析，并将分析过程文档化。

7.1.4 宜对所有的安全要求保持追溯，典型的追溯方法包括：采用专业的要求管理工具，采用特定的编号系统等。

7.1.5 在系统设计要求规范和软件安全要求规范编制完成后，需要按照 GB/T 20438.2—2017 中图 2 和 GB/T 20438.3—2017 中图 6 的 V 模型，在每一阶段开展对其的验证，验证形式包括内部测试、外部测试、会议审查、专家评定或建模分析等。验证完成后形成正式的验证记录。

7.1.6 需要按照 GB/T 20438.2—2017 中 7.3 编制系统安全确认计划。

7.2 应用考虑

7.2.1 系统设计要求与系统安全要求的关系，如图 2 所示。

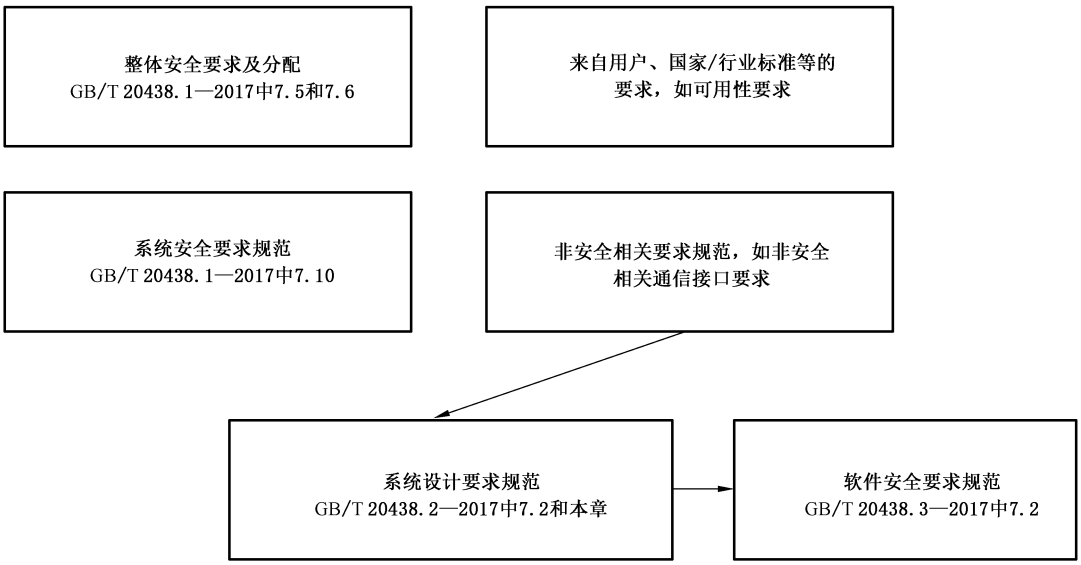

图 2 系统设计要求规范与系统安全要求规范的关系

7.2.2 一般情况下，系统设计要求规范可以包括功能级的要求和单独的硬件要求，对于复杂的系统也可以单独编制硬件安全要求规范。

7.2.3 系统设计要求规范宜进行如图 3 的分解。

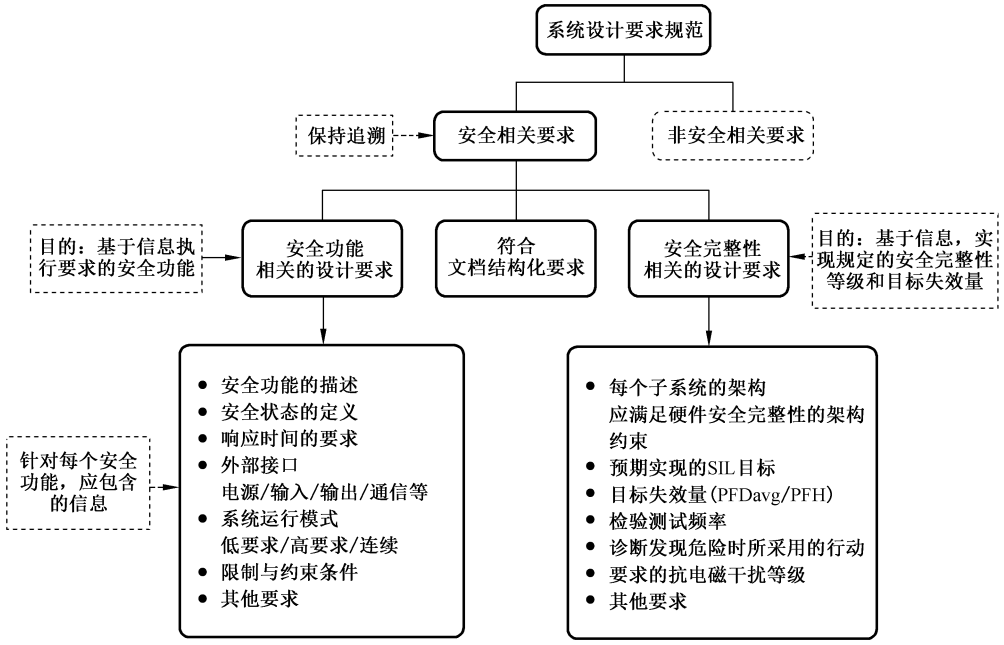

图 3　系统设计要求规范的分解

7.2.4　对于所有要求规范的描述避免直接进入具体的软硬件设计细节(这些设计细节将在后续架构设计和详细设计完成)。

注：要求规范规定系统预期要实现的安全要求，而不给出设计方案，例如“系统应对寄存器单元进行周期性自诊断”是一项安全要求，“系统将采用漫步位方法对寄存器单元进行周期性自诊断”是一项设计方案。

7.2.5　规定功能安全系统预期实现的 SIL 目标(SIL1/SIL2/SIL3/SIL4)。如果系统内的安全功能有不同的 SIL 目标宜分别详细规定。

7.2.6　如果整个安全回路是由多个功能安全系统组成，对于预期的 SIL 目标，每个功能安全系统的目标失效量(PFDavg 或 PFH)宜不超过规定的百分比，这个百分比规定下的 PFDavg 或 PFH 目标应作为要求规范中一条要求明确提出，这个百分比可来自：

——在整体要求规范或安全要求规范中已经明确的了对各个部分功能安全系统的目标失效量，特定功能安全系统研发单位直接采用该数值；

——如果在整体要求规范或安全要求中没有明确给出，则需要按照行业的通常做法，例如，在典型过程工业中会有图 4 的推荐分配。

注 1：例如，逻辑控制器保证不超过 10%的回路目标失效量，假设要求的 SIL 目标是 SIL3，按照 SIL3 在低要求运行模式下满足 PFDavg 小于 10E-3，那么对于预期实现 SIL3 应用的逻辑控制器其 PFDavg 目标至少小于 10E-4。

注 2：图 2 更加适用于过程工业，不同行业可能可能安全回路的构成有显著差异，其他行业宜结合自身的行业特性确认 SIL 分配目标。

图 4　过程工业 SIL 目标分配示例

7.2.7　其他部件也是执行整个安全回路的必要组成部分，如安全栅、安全继电器等；其他部件不包括与安全功能执行没有直接相关的部分。

7.2.8 安全确认计划宜包含的内容见图 5。

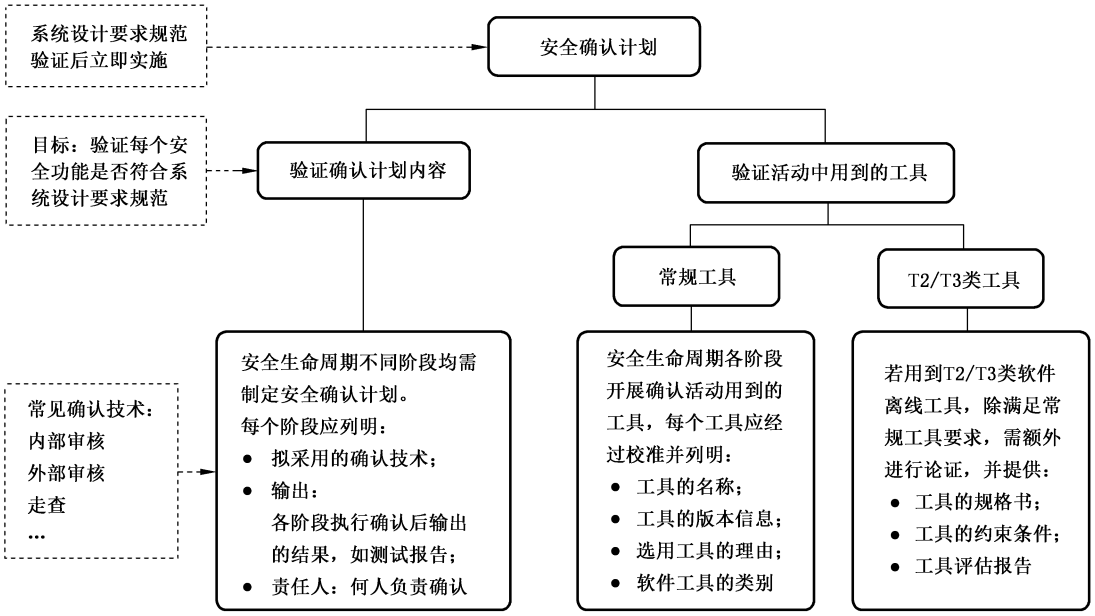

图 5 安全确认计划内容

7.2.9 确认计划在系统设计要求规范和软件安全要求规范验证完成后立即实施，需要针对要求规范的每一条要求规划确认策略。典型的确认策略包括：

——建模分析；

——内部测试；

——外部测试；

——会议审查；

——专家评定。

8 系统架构设计

8.1 一般原则

8.1.1 需要基于系统设计要求规范开展系统(硬件)架构设计。

8.1.2 对于相对简单的功能安全系统，系统架构设计可以合并到系统设计要求规范阶段实施，但单独的软件架构设计是必要的。

8.1.3 对于相对复杂的功能安全系统，宜建立单独的系统架构设计阶段。

8.1.4 架构设计需要考虑 GB/T 20438.2—2017 中 7.4 的适用要求。

8.1.5 需要考虑对架构设计开展验证。

8.1.6 需要考虑基于架构设计内容编制集成测试计划。

8.2 架构设计应用考虑

8.2.1 架构设计在保障功能安全上面需要考虑如下方面：

——保证系统足够的健壮性；

——保证不同模块之间适当的独立性，避免复杂的耦合关系和共因失效；

——保证非安全相关模块不会对安全相关模块造成负面影响。

8.2.2 需要对架构设计的静态特性进行规范性描述(例如,架构框图),对组成系统架构的每个模块和模块间接口进行描述。

8.2.3 架构设计宜避免对每个模块内部的实现细节进行描述,这些细节是后续详细设计的内容。

8.2.4 可以考虑采用多通道的 MooN 表决结构来实现高安全或高可用设计。可以在不同层次上实现多通道表决,在设备层、模块层、板卡层,甚至芯片层。

8.2.5 需要明确区分 MooN 表决结构和备用结构之间的差异,一般情况下备用结构是用于提高可用性而非安全性。

8.2.6 需要在完成架构设计验证之后,制定集成测试计划,其中包括对所有架构特性和接口特性的测试策略。

9 系统详细设计和实现

9.1 一般原则

9.1.1 功能安全系统设计和研发的基本要求需要考虑 GB/T 20438.2—2017 中 7.4、附录 A 和 B.2 的要求。

9.1.2 需要考虑编制硬件详细设计相关文件,并基于详细设计实现硬件电路。

9.2 应用考虑

9.2.1 随机硬件失效的要求

9.2.1.1 功能安全系统最终的随机硬件失效量小于或等于第 7 章所规定的目标(PFDavg 或 PFH 数值),并通过合理的建模和计算证明该目标得以实现。

9.2.1.2 随机硬件失效估算的范围是功能安全系统中所有安全相关的部分。

9.2.1.3 需要考虑按照 GB/T 20438.6—2017 中附录 B 开展 PFDavg 或 PFH 的估算,如果采用该方法,确保实际的待分析系统满足规定的所有假设条件。如果采用其他方法,宜有符合数学逻辑的合理性证明。

注:某些文献资料给出了非常简化的公式,对于简化公式的应用要更加小心,因为简化条件可能和当前实际的项目要求不符,这会导致简化公式的错误。

9.2.1.4 需要考虑使用适当的元器件失效率/失效模型数据库作为计算的输入,可以来自:

——国际标准或国家标准、行业标准,如 ISO 13849-1;

——领域内广泛认可的商用数据库;

——具有专门收集系统的现场反馈数据,保证统计置信度≥70%。

9.2.1.5 同一系统的计算宜使用一个同一来源的失效率/失效模式数据库。只有能证明数据在共同条件下得到时,才能使用多个来源的数据。

9.2.1.6 某些计算的输入参数,如检验测试周期(T1)、平均修复时间(MTTR)和平均维修时间(MRT)等不是由功能安全系统研发设计单位决定的,因此需要基于产品预期的应用情况预设一个数值参与计算,数值的合理性需要经过专门的分析和论证,在功能安全系统后续的产品手册中宜明确说明这些预设的数值。

9.2.1.7 当系统架构包含多个通道,如 1oo2 或 2oo3 架构时,需要考虑共因失效对随机硬件失效的影响,宜采用 GB/T 20438.6—2017 的方法对共因失效因子进行估算。

9.2.1.8 如果使用第三方的软件工具开展计算,需要对工具的适用性进行分析,并开展完备的工具验证。

9.2.1.9 为尽可能减小元器件发生随机硬件失效的可能性,需要对安全相关的元器件开展降额设计,电

气特性的降额因子不宜高于67%，对于温度的降额宜不小于10 ℃。

9.2.1.10 需要形成文档性的分析材料，以证明降额设计的合理性，宜开展测试对降额的实现情况进行验证。

9.2.2 硬件失效分析要求

9.2.2.1 为对9.2.1所要求的随机硬件失效进行PFD/PFH估算，需要开展元器件级的硬件失效分析，常用的分析方法包括FMEDA、FTA等。

9.2.2.2 基于元器件失效后对模块的影响以及是否能够被诊断到，失效分析宜将每种失效分类为以下几种类别之一：

——可诊断到的安全失效(λ_{SD})；

——不可诊断到的安全失效(λ_{SU})；

——可诊断到的危险失效(λ_{DD})；

——不可诊断到的危险失效(λ_{DU})；

——无影响失效。

注：对于架构设计阶段已经界定为安全无关的模块，可以不对其元器件开展详细的失效分析，这些部件的失效在GB/T 20438(所有部分)中被定义为无关失效。

9.2.2.3 对于复杂的子系统或元器件，如果其失效后安全或危险难以判定，可以将其按照50%安全，50%危险的方式进行划分。

注：在一个有效的分析过程中，不宜简单的将大部分的元器件按照50%的方式划分，这会导致最终的PFDavg，PFH，SFF等参数非常差，甚至连SIL1都达不到，这样的分析是没有意义的。

9.2.2.4 需要注意区分安全失效和无影响失效，不能将无影响失效纳入安全失效之中。

9.2.2.5 基于硬件失效分析的结论需要对已有安全设计进行复审，确保所有关键故障都得到有效控制或避免。

9.2.2.6 需要仔细判断每个诊断功能的有效性，无效的诊断不能将对应的失效归类为可诊断的，无效的诊断包括但不限于：

——诊断测试间隔过长，不满足过程安全时间的要求；

——如果采用多通道设计，单纯的通道间表决不能作为单个通道内器件失效的诊断措施；

——诊断到故障后没有适当的故障响应或报警。

9.2.3 诊断覆盖率的判定

需要仔细判断每个诊断功能的覆盖率，一般按照如下考虑进行判定。

——对于简单元器件，如果诊断测试能够诊断到它的某种失效模式，则该器件这种失效模式的诊断覆盖率为100%，否则为0%，简单器件例子：电阻、电容、三极管、二极管、光耦等。

——对于复杂的器件，原则上基于GB/T 20438.2—2017中A.1～A.14的要求。如果有更高诊断覆盖率的申明或者采用了GB/T 20438.2—2017中附录A没有规定的技术，采用测试的方法证明所实现诊断覆盖率的真实性。复杂元器件的例子：中央处理器(CPU)、模数转换(ADC)芯片、存储单元等。

——对同一器件或模块，可使用两种或更多种诊断方法来诊断相同的失效模式，这种方式可以实现比GB/T 20438.2—2017中附录A规定的更高诊断覆盖率。但这些不同方法一定是独立的，且不具有共因失效的可能。

9.2.4 诊断功能及诊断覆盖率(DC)

9.2.4.1 对于功能安全系统设计的足够的自诊断措施，设计是否足够的判定需要考虑如下：

——系统遵循了单一失效原则；

——PFDavg/PFH 满足了目标失效量的要求；

——SFF 满足了架构约束的要求。

注：足够的诊断功能可以更加利于以上要求的实现，但并不是单单依靠诊断功能，例如，失效率高低和检验测试间隔长短对于 PFDavg/PFH 是否满足要求也有重大影响。当这些要求无法满足时，可以考虑是否通过提高诊断能力进行改善。

9.2.4.2 诊断功能的设计满足检测到故障后系统的行为要求。

9.2.4.3 需要但不限于在如下两个阶段执行诊断：

——在系统初始化时，诊断重点是所有的硬件，内部或外部数据通路等；

——正常运行时周期中执行诊断功能，诊断重点包括硬件、软件、软错误、数据通路等。

9.2.4.4 宜基于系统的运行周期和所有诊断功能实现的时间，确定所有诊断的间隔时间，即诊断测试间隔（T_D）。

9.2.4.5 诊断测试间隔要足够小，以满足 GB/T 20438.2—2017 中 7.4.5.3 和 7.4.5.4。

9.2.4.6 某些诊断功能为避免频繁的误动作，可能会采取多次判断后诊断决策的机制，需要考虑到这种多次判断和重试可能会导致进入到某种死循环或无法实现所规定的诊断能力。

9.2.5 架构约束

9.2.5.1 架构约束的基本要求需要考虑满足 GB/T 20438.2—2017 中 7.4.4。

9.2.5.2 宜优先选用 GB/T 20438.2—2017 中 7.4.4 的路线 1(1H)，即通过硬件故障裕度（HFT）和安全失效分数（SFF）的确定来给出架构约束满足的 SIL 目标。

9.2.5.3 HFT 的确定需要仔细分析采用的冗余方式，某些冗余的方式不能保证硬件故障裕度的提升。

注：例如采用一用一备的方式实现冗余，正常时只有一个通道执行要求的处理功能，故障时切换到另一个通道，这种情况下的 HFT=0。

9.2.5.4 合理的估算系统的 SFF 需要考虑：

——不将无影响失效纳入 SFF 的计算之中；

——诊断部分失效导致误动不能纳入 SFF 的计算之中。

9.2.5.5 安全失效分数的确定需要考虑到某些失效率很大的部件，如果该部件是安全失效，那么可能会导致在没有执行足够的诊断情况下，SFF 指标满足架构约束要求，这个是不符合安全准则的。

9.2.6 硬件部分系统性失效的避免和控制

9.2.6.1 为了避免硬件开发期间的系统性失效，需要考虑使用 GB/T 20438.2—2017 中附录 B 的技术和措施。

9.2.6.2 在验证和确认阶段，需要有足够的证据证明这些技术和措施的确在研发过程得到了实施，并对证据文档化。

9.2.6.3 为控制系统性故障，系统设计需要考虑 GB/T 20438.2—2017 中 A.15～A.18 的要求，以满足安全数据通信过程中对于系统性故障控制。

9.2.6.4 在设计和开发活动中需要考虑可维护性和可测试性，以便在组合的最终安全相关系统中实现这些特性。系统的设计需要考虑人员的能力和限制，并且能够分配给操作员和维护人员实施。所有接口的设计宜考虑人员因素，并适应操作员可能具有的培训或意识等级，例如，大批量生产应用中操作员可能仅接受过有限的培训。

注：设计目标是通过可能的设计或在完成前进行再次确认，来防止或消除由操作员或维护人员产生的可预见的关键错误。

9.2.7 检测到故障时系统行为

9.2.7.1 需要考虑 GB/T 20438.2—2017 中 7.4.8 的所有内容。

9.2.7.2 在系统初始化时检测到危险故障，需要停止启动并给出相应的报警指示。

9.2.7.3 在系统运行期间检测到关键性危险故障，需要导致：

——在制造商规定的故障响应时间内，通过内置措施（如硬件或嵌入式软件）将所有受故障影响的输出切换到定义的安全状态；或

——在制造商所规定的故障响应时间内，向应用措施（如应用程序）通知（报警）故障，从而应用措施（如应用程序）可采取适当的动作来保持安全；

——当以上任何一种情况发生后如果还没有进入安全状态，就意味着系统已经处于降级运行，系统是否设计为当降级运行后在规定的时间内如果没有维修处理好需要自动的输出安全值，将过程导入安全状态，降级后自动进入安全状态的功能不能被现场运行人员手动关闭；规定的时间作为平均维修时间（MTTR）的影响因素之一纳入失效计算。

注 1：关键性危险故障的定义在危险和风险分析时确定，通常来说是指那些无法执行安全功能且短时间内无法自动恢复的危险故障。

注 2：何种动作合适取决于应用，功能安全系统研发团队可以将其设计为可配置的方式。

9.2.7.4 故障需要被检测并通知（报警）给应用程序，除非以下两种情况：

——通过设计，该故障不可能在系统中发生；

——由书面的技术评估证明故障可忽略。

9.2.8 安全数据通信

9.2.8.1 系统一般有两种类型的数据通信，一种是安全相关通信，另一种是非安全相关通信，对于安全相关通信需要考虑符合 GB/T 20438.2—2017 中 7.4.11 的要求。

9.2.8.2 可以采用黑色通道和白色通道两种方式实现安全通信，对于工业控制领域宜按照 GB/T 34040—2017 的要求采用黑色通道的方式。

9.2.8.3 除了对残余差错率进行估算之外，还需要考虑通过测试的方式证明安全通信的检错能力，具体的测试方法按照 GB/T 41295.3 的规定。

9.2.8.4 内部通信路径可以不按照 GB/T 34040—2017 的要求实施，但也需要有足够的传输错误检测能力。

注：典型的内部通信路径包括：内部芯片之间的数据通信（如 I^2C 等）、同一个模块内两块板卡之间接口通信。

9.2.8.5 实现安全通信协议的安全层软件需要考虑符合第 10 章。

9.2.8.6 ASIC 组件安全设计：如果系统中包含 ASIC 组件（如 FPGA、CPLD 等），其开发过程需要考虑符合 GB/T 20438.2—2017 中附录 F 的要求。

9.2.8.7 需要考虑基于硬件详细设计对硬件进行实现。

10 软件设计和实现

10.1 一般原则

10.1.1 软件设计和实现包括软件安全要求规范、软件架构设计和软件详细设计和实现。

10.1.2 安全相关软件包括：系统的嵌入式固件、系统所应用的操作系统、系统所应用的安全数据库、在线支持工具等。

10.1.3 安全软件设计和实现的一般原则宜符合 GB/T 20438.3—2017。

10.1.4 基于已经完成的软件安全要求规范和软件架构设计来实施软件详细设计和实现。

10.1.5 按照 GB/T 20438.3—2017 中 7.3 的要求编制软件确认计划。

10.2 应用考虑

10.2.1 软件安全要求规范

10.2.1.1 需要考虑基于系统设计要求规范编制软件安全要求规范。

10.2.1.2 需要考虑对软件安全要求规范进行持续追踪以确保所有要求得以正确实现。

10.2.2 软件架构设计

10.2.2.1 需要对软件架构设计的静态特性进行规范性描述(例如,架构框图),宜对组成系统架构的每个模块和模块间接口进行描述。

10.2.2.2 软件架构设计需要避免对每个模块内部的实现细节进行描述(如函数的参数),这些细节是后续详细设计的内容。

10.2.2.3 需要对软件的动态特性进行规范性描述,包括软件可能处于的运行状态描述,以及状态之间的转移关系。

10.2.2.4 在软件架构设计中,宜适当的对数据规范、数据流、内存分配及存储空间余量方案等进行描述。

10.2.2.5 在对架构设计进行验证时,需要考虑至少采用一种规范性的分析方法(如系统级/模块级 FMEA),通过该方法以证明:

——非安全相关的模块不会对安全相关模块造成负面影响;

——足够的健壮性以保证在数据传输错误等情况发生时,系统不会进入危险状态。

10.2.3 离线支持工具

10.2.3.1 软件相关的离线支持工具包括:代码编辑器、编译器和连接器、模型化设计工具、软件文档编辑工具、软件测试工具、配置管理工具等。

10.2.3.2 需要按照 GB/T 20438.3—2017 中 7.4.4 的要求考虑对离线支持工具的分类,包括:

——T1:不产生可直接或间接影响安全相关系统的可执行代码(包括数据)的输出;

——T2:支持设计或可执行代码的测试或验证,工具中的错误不能发现可执行软件的缺陷,但不会在可执行软件中直接产生错误;

——T3:产生可直接或间接影响安全相关系统的可执行代码的输出。

注 1:T1 的示例包括:文本编辑器或没有自动代码生成能力的需求或设计支持工具;配置控制工具。

注 2:T2 的示例包括:测试装置生成器;测试覆盖度量工具;静态分析工具。

注 3:T3 的示例包括:源代码程序和生成的目标代码之间的关系不明显的优化编译器;将一个可执行运行时软件包组合到可执行代码的编译器。

注 4:此分类基于 GB/T 20438.4—2017 中 3.2.11。

10.2.3.3 对于按照 GB/T 20438.3—2017 已经开展了符合性评估的离线支持工具,设计人员可以考虑直接按照工具手册的要求应用工具。

10.2.3.4 对于没有按照 GB/T 20438.3—2017 开展符合性评估的离线支持工具,设计人员需要对工具的适用性和正确性进行论证,并形成论证报告。

10.2.4 编程语言

10.2.4.1 选用符合产品特性和适于软件设计人员的编程语言。

10.2.4.2 针对特定的编程语言需要考虑编制适当的编码规则来规范和约束代码的实现,编码规则需要考虑至少规定规范化的编码风格和可以使用和不能使用的编码形式。

10.2.4.3 编码规则的内容宜来自：

——企业的已有类似项目的编码经验，公司规定等；

——国际和国内通用的且被认可的编码规则或标准，如 Mirsa C/C++等；

——待实施项目的特殊情况，如编译环境或测试工具的特殊情况。

10.2.5 软件失效分析

10.2.5.1 对 SIL1 和 SIL2 的软件宜开展软件失效分析，对于 SIL3 和 SIL4 的软件需要考虑开展软件失效分析。

10.2.5.2 软件失效分析的典型方法有：软件 FMEA、软件危险与可操性分析（HAZOP）、软件形式化建模分析等。

10.2.5.3 软件失效分析的结果保证所有安全相关模块的可预见故障都能得到相应的安全控制。

10.2.6 组件复用

10.2.6.1 对于某些软件模块，在执行本次功能安全系统设计之前就已经存在，并一直良好运行（例如，应用在之前类似系统上的通用软件模块），如果将这些软件模块复用于本次功能安全系统执行特定的组件安全功能，这些软件模块符合 GB/T 20438.3—2017 中 7.4.2.12。

10.2.6.2 对于复用的软件组件为了保证其安全性，采用以下三种方式之一进行安全设计和论证。

——路线 1s：符合性开发。按照 GB/T 20438.3—2017 和第 10 章的所有内容对该已有软件组件进行一次完全符合性的设计开发。

——路线 2s：经使用证明。符合 IEC 61508-3-1 的相关要求。

——路线 3s：非符合性开发。符合 GB/T 20438.3—2017 中 7.4.2.13。

10.2.6.3 如果采用路线 2s，最高适用于 SIL2 的安全组件，并需要足够的已有运行经验。

10.2.7 组件组合提高系统性能力

10.2.7.1 可以考虑通过组合安全组件来提高系统性能力，见 GB/T 20438.2—2017 中 7.4.3。

10.2.7.2 组合组件提高系统性能力的前提是组件之间具有足够的独立性，例如，两个通道之间的软件是异构配置的。

10.2.8 软件验证

10.2.8.1 可以考虑通过分析或测试的方法来对软件开展验证。

10.2.8.2 采用走查或审查等方式对软件代码或详细设计文件进行检查。

10.2.8.3 开展软件测试。

10.2.9 软件部分避免系统性失效

10.2.9.1 为了避免软件开发期间的系统性失效，使用 GB/T 20438.3—2017 中附录 A、附录 B 和附录 C 的相关技术和措施。

10.2.9.2 在验证和确认阶段，需要有足够的证据证明这些技术和措施的确在研发过程得到了实施，对证据文档化。

11 系统集成

11.1 一般原则

11.1.1 不同复杂度的系统可能有不同的集成考虑，对于简单的系统可能只有软硬件集成，对于复杂的

系统还存在一个到多个层次的子系统集成，宜在生命周期早期阶段明确系统的集成方式。

11.1.2 功能安全系统集成考虑符合 GB/T 20438.2—2017 中 7.5(子系统集成)和 GB/T 20438.3—2017 中 7.5(软硬件集成)。

11.1.3 在硬件和软件架构设计阶段编制集成测试计划。

11.2 应用考虑

11.2.1 在集成阶段执行故障插入测试。

11.2.2 故障插入测试用例的设计和执行参考 GB/T 41295.3。

11.2.3 故障插入测试的执行得到第三方独立机构见证，并产生基于见证结论的故障插入测试报告。

12 系统运行和维护规程

12.1 一般原则

12.1.1 功能安全系统研发团队宜基于产品的基本功能和应用特性编制用户手册，包括安装、维护要求等；功能安全系统研发团队还需要基于产品的功能安全属性编制安全手册，包括安全配置方式、危险失效参数等。

12.1.2 用户手册和安全手册从形式上可以是一个或多个文档。

12.1.3 安全手册的内容至少需要考虑 GB/T 20438.2—2017 和 GB/T 20438.3—2017 中附录 D 的要求。

12.1.4 用户手册和安全手册需要考虑随功能安全系统在发货时移交给集成单位或用户单位。

12.2 应用考虑

12.2.1 安全手册中对于安全应用的限制条件需要在手册中详细说明，包括安全模块的应用范围，响应时间约束等；

12.2.2 除了 12.1.3 的规定外，安全手册还需要考虑如下适用内容：

——安全功能可使用的那些功能和接口的规范，如应用限制、通信限制；

——可导致危险的系统失效，并能被诊断测试检测到的随机硬件失效率的估计；

——可导致危险的系统失效，并不能被诊断测试检测到的随机硬件失效率的估计；

——对保持失效率有效性的环境限制；

——预期系统所处的机械和气候环境(如振动、冲击、温度、湿度)；

——制造商声明的系统最大使用寿命，该寿命应等于或小于 20 年，除非系统制造商能提供证据证明更长的寿命，这些证据基于计算，表明其可靠性数据对于更长寿命是有效的；

注：系统中的有些单个元件已知寿命小于 20 年。典型示例包括：电池、电解电容、LED 等。如有必要，对这些元件的定期更换作为系统制造商规定的常规维护规程的一部分。定义最大 20 年使用寿命是为了覆盖大部分未知寿命的系统元件。

——定期检验测试方法、时间间隔和/或维护要求；

——系统内部的诊断覆盖率；

——系统内部的诊断测试间隔；

——如适用，平均恢复时间(MTTR)和平均维修时间(MRT)；

——安全失效分数(SFF)；

——硬件故障裕度；

——为避免系统性失效建议的应用限制；

——所用元件的降额；

——适宜使用系统的安全相关系统的可声明 SIL；
——系统的硬件版本；
——系统已得到确认的文档证据。

13 系统的确认

13.1 一般原则

13.1.1 系统的确认需要符合 GB/T 20438.2—2017 中 7.7 和 GB/T 20438.3—2107 中 7.7。
13.1.2 系统的确认方法可以考虑包括分析或测试。

13.2 应用考虑

13.2.1 保证安全要求规范中的所有内容都得到了确认，宜建立确认项与安全要求规范条款的对应关系矩阵，以清楚的显示所有的确认关系。
13.2.2 确认的部分项目可以考虑在功能安全系统研发团队内部进行（如功能测试），也可以考虑通过外部第三方实验室开展（如型式试验）。与确认相关的功能安全测试按照 GB/T 41295.3 进行。

14 生命周期各个阶段的验证

在执行以上功能安全系统生命周期过程中，在每个阶段的工作完成后，需要考虑开展对该阶段的验证工作。

每个系统生命周期阶段交付内容的验证工作需要计划、执行和文档化。这些验证需要考虑到基于生命周期各阶段输入的规定。验证所使用的技术/工具包括，例如：

——阶段性文档的复审；
——设计复审；
——功能测试；
——环境测试。

注：验证不要与校准和确认相混淆。

15 制造

15.1 对功能安全系统制造的主要目的是保证制造过程的功能安全目标能够得到保持。
15.2 功能安全系统制造团队宜符合 GB/T 19001—2016 的质量管理体系要求，包括设定质量负责人等岗位，编制质量计划等文档。

注：本文件中对于功能安全系统的制造要求其核心在于所有的安全功能和安全完整性在制造过程能够保持，而不是对于单纯制造质量或生产效率提升的考虑，虽然 GB/T 19001—2016 是对于质量体系的规定，但是很多基于良好工作实践的规定可以避免制造过程的错误。

15.3 功能安全系统制造团队编制功能安全系统的制造计划，并至少考虑以下内容：

——基本的生产要求，如工艺流程、装配方案等；
——安全相关的要求，如为了保证器件失效率而采取的筛选或老化测试的措施；
——开发过程最后发布的产品配置情况；
——预期制造装备、测试设备和相关人员能力的要求；
——对系统或系统内的组件的追溯方法（例如，编号、二维码等）。

15.4 对于存在嵌入式软件的系统，需要考虑制定相应规程，以保证在制造时将正确版本的嵌入式软件

下装到系统中，包括下装前的人工核对，下装后的一致性检查等。

注：可以采用的措施包括校验和比对，回读比较等。

15.5 对于 SIL3 和 SIL4 应用的功能安全系统生产过程，需要考虑开展适当的失效分析，分析生产过程中可能出现的合理可预见的失效情况，并采取适当的措施来避免或控制这些失效[典型的方法如过程失效模式与影响分析(PFMEA)]，在正式生产前需要考虑对相应的控制措施进行验证。

15.6 功能安全系统制造团队需要制定变更管理计划，以保证当制造过程发生了变化后不会造成新的制造风险。

15.7 变更管理计划需要考虑到功能安全系统本身出现变更的情况，例如，如果制造过程发现了功能安全系统本身的设计问题，需要协同研发团队执行变更过程。

15.8 面向生产制造相关人员对所有以上要求开展培训。

15.9 所有测试设备都应在适当的管理体系受控下，包括定期的核查、校准和维护等。

15.10 制定程序来规定对于功能安全系统内关键元器件的有效检验，以保证系统的失效率不会因为元器件的偶发问题出现异常而大幅度升高，关键元器件由研发团队基于失效分析结论确定。

15.11 制定详细的程序来规定制造后端的检验和测试，包括例行检验、确认检验和工厂验收测试。除了常规的功能和性能测试之外，还需要对系统的典型故障反应开展测试。

15.12 检验和测试需要保证不会对系统的安全性造成负面影响，如果不确定这种影响应对测试方法开展适当的论证，并将论证结论详细的告知给操作人员。

16 功能安全系统评估评测

16.1 对于特定的功能安全系统，为证明第 5 章～第 15 章内容的有效实施，需要考虑开展独立的功能安全评估评测。

16.2 功能安全评估评测机构来自独立于功能安全系统研发制造单位的第三方组织，评估评测机构是经相关机构授权的具有功能安全标准认可能力的实验室、检验机构或认证机构。

16.3 功能安全评估评测机构需要建有满足功能安全评估评测技术的实验场地，配置有适当的测试设备、软件和工具。

16.4 功能安全评估评测的人员需具备足够的资质，包括对于功能安全技术的理解和对于待评估产品的理解。

16.5 具备必要的测试设备、软件和工具，至少包括：

——专用的功能安全失效分析工具；

——专用的故障模拟或仿真工具以实现适当的故障插入测试；

——安全功能和性能测试的必要环境条件。

16.6 功能安全系统的评估评测至少包含以下适用内容：

——对建立的安全生命周期和功能安全管理开展评估；

——对形成的所有安全相关证据文档开展评估；

——对系统和硬件设计的安全性进行评测；

——对软件设计的安全性进行评测；

——基于安全机制的设计和失效分析结论，评估评测人员设计故障插入测试用例，执行或现场目击故障插入测试，完成故障插入测试报告；

——对功能安全系统研发团队执行的系统、硬件和软件测试的合理性和完备性开展评测(参见 GB/T 41295.3)，检查所有的测试计划、测试记录和测试报告；

——必要的测试需在功能安全评估评测机构授权的实验室内开展，至少包括：关键的故障插入测试、环境条件下的关键功能和性能测试、安全通信检错能力测试、关键软件模块的单元测试；

——对形成的用户手册和安全手册开展评估；

——对功能安全系统的制造能力开展评估；

——形成基于以上评估评测结论的过程记录和标准符合性检查表；

——编制评估评测报告。

16.7 在完成评估评测工作之后，形成面向特定功能安全系统的评估评测报告，报告中至少包括：

——评估评测的对象，包括详细的软硬件模块、系统结构、版本和文档；

——评估评测的实施周期和人员；

——评估评测依据的标准规范，采用的方法和策略；

——特定生命周期阶段的符合性结论；

——评估评测的约束条件和有效期。

16.8 功能安全系统在其他第三方机构开展的测试（如型式试验）需要首先经过功能安全评估评测机构的认可。

参 考 文 献

[1] GB/T 15969.6—2016 可编程序控制器 第6部分:功能安全

[2] GB/T 20172 石油天然气工业 设备可靠性和维修数据的采集与交换

[3] GB/T 20438(所有部分) 电气/电子/可编程电子安全相关系统的功能安全

[4] GB/T 21109(所有部分) 过程工业领域安全仪表系统的功能安全

[5] GB 28526—2012 机械电气安全 安全相关电气、电子和可编程电子控制系统的功能安全

[6] GB/T 41295.1—2022 功能安全应用指南 第1部分:危害辨识和需求分析

[7] ISO 13849-1 Safety of machinery—Safety-related parts of control systems—Part 1: General principles for design

[8] ISO 26262:2018 (all parts) Road vehicles—Functional safety

[9] IEC 61800-5-2 Adjustable speed electrical power drive systems—Part 5-2: Safety requirements—Functional safety