ICS 25.040
CCS N 10

中华人民共和国国家标准

GB/T 41295.4—2022

功能安全应用指南
第4部分:管理和维护

**Application guide of functional safety—
Part 4:Management and maintenance**

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4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：中国石油集团安全环保技术研究院有限公司、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。

本文件主要起草人：熊文泽、闫伦江、王璐、魏振强、孟邹清、孙文勇、田雨聪、彭其勇、靳江红、任军民、张亚彬、刘晓亮、张雪、朱明露、孙腾。

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。目的在于确立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。目的在于确立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。目的在于确立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。目的在于确立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4部分:管理和维护

1 范围

本文件确立了功能安全系统实现相应安全完整性等级的安全管理和维护活动,包括文档、人员、变更管理,以及维护过程的检验测试等。

本文件适用于从功能安全系统安装、试运行到正常运行过程中的相关管理和维护活动。

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 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

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,包含不同的层次,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、安全管理人员等。

[来源:GB/T 41295.2—2022,3.2]

3.3

功能安全系统维护团队 team for functional safety system maintenance

执行功能安全系统运行维护的责任主体。

注:包括对功能安全系统的检验测试人员、变更管理人员、日常巡检人员、配件更换人员等。

3.4

离线测试 offline test

在受控设备处于安全状态的情况下,开展的测试活动。

4 缩略语

下列缩略语适用于本文件。

HAZOP：危险与可操作性(Hazard and Operability)
HMI：人机接口(Human Machine Interface)
LOPA：保护层分析(Layer Of Protection Analysis)
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 Per Hour)
SIL：安全完整性等级(Safety Integrity Level)
SRS：安全要求规范(Safety Requirement Specification)

5 总则

5.1 从事功能安全系统安装、试运行和正式运行的组织需考虑建立功能安全管理体系，以保证在实施相关工作过程中要求的安全完整性能力得以保持。
5.2 功能安全管理体系可与已经建立的安全/环保管理或质量管理体系相结合，协同实施。

6 文档方面

6.1 在执行安装、试运行和维护之前，需考虑已经获得了足够支持后续安全管理的所有文件和规范，包括但不限于：

——危险与风险分析报告(如 HAZOP 分析报告)；
——安全完整性等级确定报告(如 LOPA 分析报告)；
——所有安全相关系统的安全手册和用户手册；
——整个装置或工艺的安全要求规范(SRS)；
——系统安全集成报告；
——系统工厂验收测试报告；
——项目宜符合的安全相关标准或国家法律法规[如 GB/T 20438(所有部分)，GB/T 21109(所有部分)等]。

6.2 编制安装、试运行和维护工作计划，完成工作之后需要形成技术报告。
6.3 相关文档妥善保存便于功能安全审计和功能安全评估时查阅，文档在特定的安全相关系统停用之后可不再保存。

7 人员方面

7.1 执行功能安全系统运行维护的人员，在上岗前需经过独立的第三方功能安全培训，培训内容宜涵盖 GB/T 20438(所有部分)、GB/T 21109(所有部分)和本文件的相关内容。
7.2 需考虑对负责开展活动的所有人员、部门和组织(包括对验证和功能安全评估负责的人员，以及相关的批准权威机构或安全法规机构)进行识别，并完整清楚地告知其责任。
7.3 清楚的定义出每个人员从事安全活动的范围、职责、应具备的能力(即培训、技术知识、经验和资格)和限制条件等。
7.4 需考虑对执行特定功能安全活动的人员能力进行规定和限制，包括：

——所有人员经过专业机构的功能安全培训，具备从事功能安全活动的资质；
——团队负责人具备相关项目的经验，并对功能安全标准和技术具有深入理解；
——所有人员经过定期的培训，以获知最新的功能安全标准和技术进展。

7.5 不同岗位的人员之间宜建立适当的沟通交流机制。

8 变更管理和配置管理

8.1 需保证采用了适当的配置管理和变更控制规程。

8.2 构建符合特定项目要求的配置项，配置项宜涵盖可能影响安全完整性等级的所有软硬件实体和文档。

8.3 需保证发生变更时要求的安全完整性得以持续满足，这包括针对变更执行影响分析和开发适当的测试计划。

8.4 需保证一个适当的变更批准机制存在并且不会执行非授权的变更。

8.5 配置管理系统需保证所有配置项的配置状态和版本得以识别。

8.6 宜使用一套规范化的系统，保证配置下的所有项目都能单独得以识别。

9 运行和维护过程的安全管理

9.1 总则

功能安全维护管理的核心目标是保证功能安全系统在现场运行过程中要求的 SIL 能力不会降低，导致 SIL 能力降低的原因可能包括：

a) 由于人为的安装、试运行不当，导致功能安全系统从运行开始就存在潜在的缺陷，无法实现预期的所有安全功能（系统性能力不满足）；

b) 由于人为的维护活动不当，导致没有按照系统的要求执行故障处理和维修更换等；

c) 系统的硬件（包括数据传输和软错误）由于环境或人为因素导致比预期的失效率高（硬件安全完整性不满足）；

d) 维护过程中没有执行适当的检验测试，包括检验测试周期过长或检验测试的内容不充分。

a)和 b)的内容需要使用适当的功能安全管理和运行前验收测试来保证，为避免 c)和 d)的发生需要考虑 9.2～9.4 的内容。

9.2 运行过程的在线安全分析

9.2.1 考虑在维护过程中开展对功能安全系统的现场失效分析和在线安全管理。

9.2.2 在功能安全系统运行过程中，现场运维人员需要对功能安全系统出现的故障情况进行记录。

9.2.3 宜采用专用记录工具进行自动化的故障统计。自动化的记录工具可实现对功能安全系统各个组件故障信息通过通信网络自动获取、汇总、分类和显示。

9.2.4 基于故障收集的情况，对所有的故障记录需要进行定性和定量分析，确定这些故障的出现是否超出系统的预期运行目标、规则或失效率。设备失效模式及数据采集方法可见 GB/T 20172—2006、GB 28526—2012、GB/T 15969.6—2015。

9.2.5 对于关键的安全功能回路需要考虑采用专用的安全特性在线分析工具。在线分析工具可与记录工具可以成套使用。安全特性在线分析工具至少具备安全回路设备状态监测、实时故障预警、要求率分析和风险动态评价等功能。

9.2.6 当故障分析结论为功能安全系统当前的运行状态与安全要求规范、系统用户手册和安全手册中规定的不符时，宜采取适当的措施对系统进行修改，可选的措施包括：

——更换故障率高的组件，并排查导致故障率升高的原因，保证从根源上避免故障发生；

——调整内部的管理措施，加强人工的巡检和维护；

——重新开展一次完整的危险与风险分析和安全完整性确定评估，提出新的安全防护需求。

9.3 检验测试

9.3.1 一般原则

9.3.1.1 实际开展的检验测试的时间间隔不超过 PFDavg 或 PFH 计算中规定的间隔时间，如采用更长的间隔时间，重新开展适当的 PFDavg 或 PFH 计算，以证明符合要求的 SIL。

9.3.1.2 实际开展的检验测试达到的测试覆盖率不小于 PFDavg 或 PFH 计算中假设的测试覆盖率。

9.3.1.3 执行检验测试的人员需经过培训，对功能安全系统及现场工艺等都有足够的认识。

9.3.1.4 执行检验测试的工具需考虑经过定期的校核，以保证测量精度和溯源性。

9.3.1.5 制定检验测试计划，在完成测试后编制检验测试报告。

9.3.1.6 理论上，检验测试可在线或离线开展，具体选用何种方式取决于具体的工艺要求、生产要求和功能安全系统特性。

9.3.1.7 宜采用自动化的工具对检验测试的执行情况进行记录和动态分析，并基于测试要求提出改进措施。

9.3.2 离线测试时间

9.3.2.1 最常用的用于揭露导致安全功能丧失功能的失效或故障的安全功能测试是离线功能测试。执行该测试时，受控设备处于停产的状态，可对安全功能的所有特征进行确认。该测试的主要目的是检测安全功能中危险未被揭露的故障。

9.3.2.2 对安全相关系统中的每个安全功能进行辨识。与每个安全功能相关的所有输入、输出和逻辑均得到辨识。测试规范需要考虑定义如何对每个安全功能进行确认。对所有执行测试的必要设备进行辨识，并验证其是否适应于该测试，包括具有可追溯特性的校准设备。

9.3.2.3 考虑以下因素以确定离线测试的时间间隔：

——测试间隔由对安全功能的性能计算确定；

——当逻辑发生变更，对安全功能产生影响的时候；

——当过程或设备由于计划的维护活动停止工作；

——公司关于对安全功能进行完整测试的政策；

——在功能安全系统长时间停机之后。

9.3.2.4 在执行修改（改变下述中的任何一项）之前，执行相应的审查以保证变更不会降低防护等级，并需要执行适当的测试以确认修改后的安全功能仍正常运行，改变包括：

——一个基于原始设计意图的安全保护层的性能；

——结构的材料；

——运行模式；

——运行的规程；

——报警和联锁设置；

——响应速度；

——测试间隔或方法；

——设备类型，除非是同型更换；

——架构或表决逻辑；

——诊断。

9.3.3 传感器子系统的离线测试

9.3.3.1 开关在正常工作过程中，状态不经常发生改变，为确认其功能的有效性，需考虑周期性进行离

线测试，测试周期提前给予确定。

9.3.3.2 变送器能够提供如超范围高/低诊断和超出控制范围显示，故根据变送器的诊断功能酌情降低对变送器的测试频率。

9.3.3.3 输入设备的校准稳定性可能要求其测试频率要低于完整的安全功能。考虑设备会由于环境改变(如温度)而漂移，可能要求更加频繁的测试和校准，以保证正确的过程变量输入到安全功能。时漂大或者工作环境比较恶劣的变送器，需考虑增加其测试频率。

9.3.3.4 组件的冗余可能会影响测试频率。如果冗余变送器有输出监视，并且彼此比较，一致则意味着对测量量不需要频繁的测试或校准。如果输出漂移分离，表示需要对所有冗余组件进行测试和校准。

9.3.3.5 对危险条件检测的多样性是一种在不增加冗余组件的情况下提高安全功能的可用性。例如，对于压力的测量可以通过对工艺过程条件的温度测量来表示。通过对温度、压力值与预计的热力学数据进行比较，对过程测量的有效性进行诊断，降低要求的测试间隔。

9.3.3.6 对于特定传感器和服务的用户经验可用于确定设备的测试频率，以保证传感器的性能。

9.3.4 逻辑控制子系统的离线测试

9.3.4.1 当对逻辑解算器进行变更之后，对这些变更的潜在影响进行评估以确定需要对多少安全功能进行测试。如果程序的变更可以与某些区域明确隔离开，并且可以明确地证明变更不会影响逻辑解算器中执行的其他逻辑，仅有该区域需要被完全测试(完整功能测试)。这可应用各种技术的逻辑解算器，包括机电继电器、固态继电器、气动或可编程电子。

9.3.4.2 诊断功能作为逻辑解算器的外部诊断，宜对其采用与逻辑解算器同样的频率进行测试。

9.3.4.3 宜对逻辑解算器的功能方面特性按照计划进行验证，根据与过程相关的风险情况、逻辑的复杂性和公司使用该逻辑解算器的经验，确定测试频率从一年到几年。

9.3.5 最终执行单元子系统的离线测试

9.3.5.1 当执行全系统功能测试的时候，需要对最终执行组件(如阀门)进行测试。测试频率宜根据安全功能计算中的性能情况进行。每当过程停止工作之后，都宜对最终执行组件进行测试。

9.3.5.2 作为最终执行组件的测试频率取决于很多因素：

——作为最终执行组件的类型；

——应用的环境情况；

——作为正常运行的使用还是当安全功能动作后作为一个备用组件；

——最终执行组件的性能要求，如阀门是需要提供最小的泄漏隔离还是泄漏可以容忍。

9.3.5.3 当测试最终执行组件的时候，附件如阀门定位器、限位显示器/传感器、空气压力器等宜与最终执行器按照同等频率测试。

9.3.6 人机接口的离线测试

对人机接口(HMI)按照与安全功能同等的频率进行测试。当对 HMI 中的信息显示进行变更时，对变更进行测试以确认显示的正确状态。如果 HMI 用于初始化安全功能逻辑，所有与初始化相关的设备都应该进行测试，包括 HMI、输出电路和最终执行组件。

9.3.7 安全通信的离线测试

对于在安全功能采用安全通信总线进行数据交换时，对通信采用与安全功能同等的频率进行测试。当开展对安全功能的全功能测试时，测试包括到所有其他设备的通信，如到基本过程控制系统的通信。当在安全功能和任何其他设备之间发生通信连接变更时，确认对正确的信息进行了传递。

9.4 在线测试

9.4.1 在线测试可保证工艺的连续性，但需要考虑到可能产生导致过程误停车的风险。

9.4.2 为尽可能地避免误停车，在测试开始前宜对测试规程进行一次复审，复审人员包括来自设备、电气和操作维护的技术人员。这个团队考虑审核以下内容：

——讨论功能安全系统中操作员的重要性情况；

——对功能安全系统的功能描述进行复审；

——对功能安全系统的功能测试规程进行复审；

——讨论是否在线测试会影响其他系统，如基本过程控制系统，报警或其他安全功能；

——讨论工作范围，具体到待考虑的参数是什么，压力、温度或是液位等；

——讨论当产生每个报警时，为什么需要告知操作人员；

——讨论当旁路系统时，哪些设备将不再起作用；

——与操作人员复审在测试时那些特别需要注意的事项；

——当输入处于旁路测试时，讨论当安全功能发生非计划停车时宜采取什么动作。

9.4.3 在线测试注意提前做好旁路，并确保旁路后不会产生附加影响。

9.4.4 对于最终执行组件（如阀门）可采用如部分行程测试的方式来开展在线测试，部分行程测试的有效性或取代全行程测试的合理性需通过专门的分析论证。

参 考 文 献

[1] GB/T 15969.6—2015 可编程序控制器 第6部分:功能安全
[2] GB/T 20172—2006 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] GB/T 41295.2—2022 功能安全应用指南 第2部分:设计和实现