ICS 25.040
CCS N 10

中华人民共和国国家标准

GB/T 41295.3—2022

功能安全应用指南
第3部分:测试验证

Application guide of functional safety—Part 3:Testing and verification

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3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：机械工业仪器仪表综合技术经济研究所、国家管网集团西南管道有限责任公司、国能智深控制技术有限公司、浙江中控技术股份有限公司。

本文件主要起草人：熊文泽、陈小华、田雨聪、徐德腾、裘坤、史学玲、孟邹清、李旺、张亚彬、王璐、刘晓亮、朱杰、刘志勇、帅冰、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测试验证。

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3部分:测试验证

1 范围

本文件确立了功能安全系统的测试验证,包括执行安全相关功能的硬件、软件、集成和系统级的测试。

本文件适用于功能安全系统研发阶段、制造阶段、系统集成阶段、试运行阶段或现场确认阶段。测试活动包括功能安全系统研发团队内部测试和外部测试。

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

IEC 61326-3-1 测量、控制和实验室用电气设备 电磁兼容性(EMC)的要求 第3-1部分:与安全相关的系统和用于与执行安全相关的功能设备(功能安全)用抗扰度要求 一般工业应用[Electrical equipment for measurement,control and laboratory use—EMC requirements—Part 3-1:Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety)—General industrial applications]

IEC 61326-3-2 测量、控制和实验室用电气设备 电磁兼容性(EMC)的要求 第3-2部分:与安全相关的系统和用于与执行安全相关的功能设备(功能安全)用抗扰度要求 带指定电磁环境的工业应用[Electrical equipment for measurement,control and laboratory use—EMC requirements—Part 3-2:Immunity requirements for safety-related systems and for equipment intended to perform safety-related functions (functional safety)—Industrial applications with specified electromagnetic environment]

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、功能安全管理人员等。

[来源：GB/T 41295.2—2022，3.2]

3.3

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。

[来源：GB/T 41295.2—2022，3.4]

4　缩略语

下列缩略语适用于本文件。

EMC：电磁兼容性(Electromagnetic Compatibility)

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)

HDL：硬件描述语言(Hardware Description Language)

MC/DC：修订的条件/判定覆盖率(Modified Condition/Decision Coverage)

SIL：安全完整性等级(Safety Integrity Level)

5　总则

5.1　需考虑在功能安全系统研发安全生命周期的适当阶段开展测试，以证明所确立的安全功能和安全完整性得以实现，基于安全生命周期典型阶段的测试如图 1 所示。

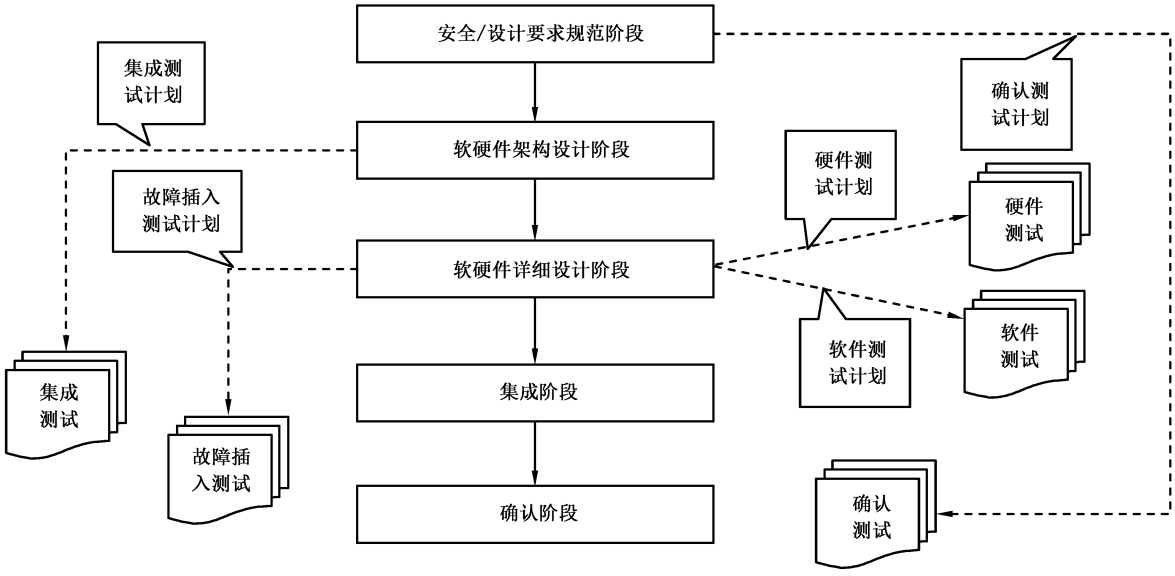

图 1　基于安全生命周期典型阶段的测试

5.2　一般功能安全系统实现安全研发过程所开展的测试内容如图 1 所示，对于更加复杂的系统，或在更严格的安全研发管理下，可能有更多的测试项。

5.3　对测试的总体考虑如表 1 所示。

表 1　各个测试的总体考虑

测试类型	输入文件	测试计划	测试输出	测试不通过的处理
硬件测试	硬件详细设计相关文件(设计规范、原理图、降额分析等)	硬件测试计划	硬件测试记录/报告	对硬件详细设计进行修改，并重新执行硬件测试
软件测试	软件详细设计相关文件(设计规范、编码规则等)	软件测试计划	软件测试记录/报告(静态测试报告、单元动态测试报告、单元集成测试报告等)	对软件详细设计进行修改，并重新执行软件测试
集成测试	软硬件架构设计相关文件	集成测试计划(在架构设计完成之后编制)	集成测试记录/报告	对设计进行修改，开展影响分析和适当的重新测试
故障插入测试	软硬件相关设计相关文件(设计规范、原理图、失效分析报告等)	故障插入测试计划	故障插入测试记录/报告	对设计进行修改，开展影响分析和适当的重新测试
确认测试	安全/设计需求规范	确认测试计划	确认测试记录/报告	对设计进行修改，开展影响分析和适当的重新测试

5.4　测试过程的文档需包括：

a)　在测试前宜编制测试规范，详细规定测试内容、方法、采用的设备、步骤和预期结果等；

b)　在测试过程中宜形成测试记录；

c)　在测试完成后宜编制测试报告；

d)　所有测试相关的文档宜按照功能安全管理体系的规定进行编制、维护和存档。

5.5　所有测试设备宜有相应的设备管理制度，宜在执行测试之前进行功能完好性检查，宜经过定期的校准。

5.6　宜采用自动化测试工具，将手动操作的步骤降到最低。

5.7　测试之前，需清楚的定义出功能安全系统通过测试时应达到的状态和性能指标，宜考虑如下情况：

a)　硬件的损坏；

b)　嵌入式程序和应用程序出现非预期的修改或意外的改变；

c)　应用数据的存储和交换过程出现非预期的修改；

d)　模拟输入/输出接口精度出现不允许的偏差；

e)　通信过程的响应时间超过允许的限值；

f)　组件/系统内的扫描周期和响应时间超过允许的限值；

g)　时钟错误；

h)　不能正常初始化或复位；

i)　组件/系统不能在不同运行模式之间进行转换，如“初始化”“正常运行”“故障”等。

5.8　如在相关的产品标准里面已经定义了适当的性能判据，宜采用该性能判据。

6　硬件测试

6.1　硬件测试可由功能安全系统硬件研发小组成员开展，执行测试的人员宜不同于该部分硬件的研发人员。

6.2 考虑基于硬件详细设计来规划硬件测试用例。

6.3 如果使用数字专用集成电路，需要考虑开展以下测试：

a) 模块级的功能测试，如：使用(V)HDL 测试平台；

b) 顶层功能测试；

c) 嵌入式环境的功能测试；

d) 通过对门级网表的仿真进行测试，包括时序、参考模型等。

7 软件测试

7.1 软件测试可由功能安全系统软件研发小组成员开展，执行测试的人员需考虑不同于该部分软件的研发人员。

7.2 基于软件架构和软件详细设计来规划软件测试用例。

7.3 开展软件静态测试，包括：

a) 对采用的编码规则进行符合性检查，确保代码符合所有的编码规则，对于出现不符合的情况，有相应的论证以说明不符合不会导致潜在的安全隐患，所有的不符合情况及其论证宜文档化；

b) 对软件的结构化和模块化特性进行度量，包括圈复杂度等；

c) 宜采用专业化工具开展软件静态测试。

7.4 开展软件动态测试，宜考虑以下内容：

a) 至少从模块(函数)和模块(函数)集成两个层面开展软件动态测试；

b) 软件动态测试的测试用例生成方法和覆盖率程度满足表 2；对于某些模块如果达不到 100％覆盖率有合理性论证，例如，调用了第三方已有的安全库、防御性编程等，不符合情况及其论证宜文档化；

c) 宜采用专业化工具开展软件动态测试。

表 2 软件动态测试

技术/措施[a]		参考	SIL1	SIL2	SIL3	SIL4
1	根据边界值分析执行测试用例	C.5.4	R	HR	HR	HR
2	根据错误推测执行测试用例	C.5.5	R	R	R	R
3	根据错误植入执行测试用例	C.5.6	—	R	R	R
4	根据基于模型测试用例的生成执行测试用例	C.5.27	R	R	HR	HR
5	性能建模	C.5.20	R	R	R	HR
6	等价类和输入划分测试	C.5.7	R	R	R	HR
7a	结构测试覆盖率(入口)100％[b]	C.5.8	HR	HR	HR	HR
7b	结构测试覆盖率(语句)100％	C.5.8	R	HR	HR	HR
7c	结构测试覆盖率(分支)100％	C.5.8	R	R	HR	HR
7d	结构测试覆盖率(条件、MC/DC)100％	C.5.8	R	R	R	HR

测试用例分析在子系统级进行并基于规范和代码。

注 1：第三列中的参考(属于资料性的，而非规范性的)“C.x.x”显示了 GB/T 20438.7—2017 中附录 C 给出的技术/措施的详细描述。

注 2：HR 表示强烈推荐，R 表示推荐，—表示不推荐也不反对。

注 3：该表引用自 GB/T 20438.3—2017 中表 B.2，并进行适当修改。

[a] 根据安全完整性等级选择适当的技术/措施。

[b] 当 100％覆盖率不能实现时(比如防御性代码的语句覆盖率)，给予适当的说明。

8 集成测试

8.1 集成测试宜由功能安全系统研发团队的测试人员完成，测试人员宜不同于硬件和软件设计人员。

8.2 基于功能安全系统架构设计和系统级失效分析的结论设计集成测试的用例。

8.3 执行功能、黑盒和性能测试，以证明集成后的组件或系统满足预期的目的，宜至少满足表 3 的相关内容。

表 3 功能和性能测试

测试子项	内容	执行要点
功能测试	在正常室内没有增加额外的环境应力下，对产品设计中定义的所有安全相关功能进行测试	充分考虑以下方面开展功能测试： ——系统级失效分析报告； ——所有正常和异常的输入输出情况； ——所有组件之间的接口
黑盒测试	在一个规定的环境中，利用规定的测试数据执行一个系统或者程序的功能。这将揭露出系统的行为是否符合设计规范	开展黑盒测试，考虑如下设计测试用例： ——边界值分析； ——等价类划分； ——根据因果图，结合在极限运行边界的临界状况等
通用性能测试	在正常室内没有增加额外的环境应力下，对产品设计中定义的所有安全相关性能进行测试	充分考虑以下方面开展通用性能测试： ——输入输出的电气性能测试； ——结构的机械性能测试； ——测试设备的精度要高于待测系统的精度
性能测试-响应时间测试	任何输入点的阶跃变化到任何输出点阶跃变化的最大持续时间，以及通过点到点通信的某一个系统输入点阶跃变化到任何其他系统输出点的阶跃变化	开展响应时间测试，以尽可能地反映最坏情况下的响应时间：迅速改变输入和输出、持续外部通信、持续点对点通信等。考虑对以下可能影响响应时间的情况开展测试： ——条件打印语句；条件浮点计算或数组处理； ——突发事件，多个输入/输出接口同时变化； ——源自外部的通信报文突发性出现； ——输入/输出接口出现突发变化时，远程监控导致内部生成信息的增长； ——因开路、短路或 EMI 导致丢失通信连接，造成内部超时或故障响应； ——单一随机硬件故障造成内部超时或故障响应的情况
性能测试-系统容量测试	从硬件扩展和软件存储等方面对系统设计中规定的容量进行测试	宜开展系统性能测试，按照最大配置或最多存储占用等方式开展测试
性能测试-压力过载测试	设置在极端情况下，极端输入条件或输入速度情况下开展压力过载测试	——对于 SIL3 以上的应用，开展压力过载测试； ——压力过载后允许系统损坏，但要合乎安全行为，例如，实现了安全输出

表 3　功能和性能测试（续）

测试子项	内容	执行要点
性能测试-统计测试	采用足够的样品、足够的测试输入和足够的测试实验，实现多次的批量化测试以证明系统的可靠性能力（包括硬件可靠性和软件可靠性）； 统计测试的目的是验证系统的动态行为是否符合预期目标，包括功能上的和健壮性上的。统计测试必须基于某些应用场景或失效分析假设，通过模拟给安全相关组件/系统的大量不同输入的统计分布来进行测试	——对于 SIL3 以上的一般软硬件系统，宜采用统计测试； ——对于简单的具有重复性功能的机械组件（例如，机械继电器、阀门、开关等）应采用统计测试； ——输入组合可以来自硬件和软件失效分析的结论，或来自预期应用现场可能出现的输入条件统计分布； ——由于需要进行大量较长时间的测试，因此可能需要配置专用的测试工具以产生测试信号和接收记录输出情况；对输出情况的记录可能包括输出信号的时间戳、值和保持时间等

9　故障插入测试

9.1　故障插入测试宜由独立于研发团队的第三方功能安全评估机构完成，或由第三方功能安全评估机构现场见证下完成。

9.2　故障插入测试的用例宜由第三方功能安全评估机构根据设计文档和失效分析记录等形成，并在测试前与功能安全系统研发团队沟通确定；故障插入测试可在器件级、组件级和系统级开展。

9.3　故障插入测试的执行程度如表 4 所示，在低测试程度下，测试至少在组件或系统级，包括不同单元间的数据连接。在中等或高程度下，测试应用于元器件级，并以足够的严格度来验证声明的诊断覆盖率。

表 4　故障插入测试的程度

该部分声明的诊断覆盖率	SIL1	SIL2	SIL3	SIL4
＜90％	低	低	中	高
≥90％	高	高	高	高

9.4　故障插入测试的目的如下：

a）　验证硬件失效分析（例如：FMEA 或 FMEDA）和软件失效分析（例如：软件 HAZOP，软件 FTA）对于故障影响判定的正确性（例如：安全失效、危险失效的划分）；

b）　验证初始化时/运行时执行的诊断测试是否切实有效，以及在诊断到故障后是否采取了正确的动作（包括进入安全状态，指示灯变化，上位监控软件报警等）；

c）　验证组件/系统的故障响应是否符合设计意图；

d）　验证允许的在线维护过程，如模块的更换，运行是否符合设计意图；

e）　验证安全通信设计的正确性。

9.5　故障插入测试的流程考虑如下过程：

a）　收集所需的输入材料，包括软硬件详细设计、软硬件失效分析报告等；

b）　设计故障插入测试用例，并形成故障插入测试计划；

c）　准备故障插入待测系统、测试环境和测试设备，对待测系统进行功能和性能检查（见第 5 章的性能判据），确保测试前系统无异常；

d) 执行故障插入测试，并记录测试时间、现象和人员等信息；如在测试过程中发现问题宜执行设计修改，并返回到第三步重新开始测试，已完成的测试是否需要重复取决于设计修改后的影响程度；

e) 编制故障插入报告。

9.6 在确定故障插入测试点时考虑以下方面：

a) 在失效分析中对于失效影响判定不明晰的地方，包括对安全还是危险能不能诊断到的判定；

b) 失效模式的失效率较大；

c) 系统运行时用于故障揭露的所有诊断措施；

d) 完成特定功能的专用复杂器件(如模数转换芯片)；

e) 对于某些复杂器件的内部依靠软件实现的诊断措施；

f) 安全通信过程的故障诊断措施。

注：由于功能安全系统的元器件/模块较多，一般情况对所有元器件/模块的失效模式进行故障模拟是不现实的，需筛选出具有代表性的测试点，通过对代表性测试点的故障插入可证明对该部分信号链路的诊断能力是否确实发挥作用。

典型故障插入测试用例如表5所示，对于功能安全系统考虑表5中的适用测试用例。

表5 故障插入测试的测试项

测试对象	故障插入测试用例
机电装置(如继电器、开关等)	1) 继电器线圈阻值变化； 2) 继电器开/关触点粘黏； 3) 继电器开/关触点动作时间延迟
分立硬件	
数字I/O	1) 输入/输出通路的开路和短路； 2) 表示高/低电平的电压变化； 3) 由于器件故障导致输入/输出卡死在固定状态
模拟I/O	1) 输入/输出通路的开路和短路； 2) 负责采样器件的异常，如开路、短路和值变化； 3) 负责信号转换器件的异常，如模数转换，加法器等； 4) 由于器件故障导致输入/输出卡死在固定状态
电源	1) 外部/内部电源欠压/欠流； 2) 外部/内部电源过压/过流； 3) 外部/内部电源波动； 4) 外部意外掉电重启
总线	
通用	1) 模拟数据/地址错误； 2) 模拟传输超时
内存管理单元(MMU)	1) 模拟数据/地址错误； 2) 模拟使用的寄存器软错误
直接内存访问(DMA) 总线仲裁	1) 模拟无或连续的访问错误； 2) 模拟使用的寄存器软错误； 3) 模拟仲裁信号固定； 4) 模拟无或连续仲裁信号

表 5　故障插入测试的测试项（续）

测试对象	故障插入测试用例
安全通信协议	1）　模拟传输过程中的数据完整性受损； 2）　模拟传输过程中的重复、删除、插入、重新排序； 3）　模拟传输过程中的误用、延时和伪装
中央处理器(CPU)	
寄存器	1）　模拟数据或地址错误； 2）　模拟寄存器内的软错误
内部 RAM	1）　模拟数据或地址错误； 2）　模拟内存的软错误； 3）　模拟寻址错误
编码和执行，包括标志寄存器 地址计算 程序计数器，堆栈指针	1）　模拟运算码的执行错误； 2）　模拟固定错误； 3）　模拟数据的软错误； 4）　模拟指向地址固定； 5）　模拟软错误
中断处理 中断 复位电路	1）　模拟无中断或连续中断； 2）　模拟中断的交叉； 3）　模拟电路可能产生的直流故障； 4）　模拟电路的震荡
不可变内存	1）　地址线或管脚错误； 2）　数据线或管脚错误； 3）　不可变内存器件上其他管脚的开路和短路
可变内存	1）　地址线或管脚错误； 2）　数据线或管脚错误； 3）　可变内存器件上其他管脚的开路和短路； 4）　模拟数据的软错误
时钟[石英、振荡器、锁相环(PLL)]	1）　无时钟； 2）　时钟频率过快； 3）　时钟频率过慢； 4）　时钟频率振荡
通信和大容量存储器	1）　模拟数据或地址错误； 2）　模拟传输错误
传感器	1）　模拟固定故障； 2）　模拟直流故障； 3）　模拟漂移或振荡
最终元件	1）　模拟固定故障； 2）　模拟直流故障； 3）　模拟漂移或振荡

10 确认测试

10.1 确认测试一般由功能安全系统研发团队内部和第三方测试机构共同完成。

10.2 宜基于系统、硬件和软件的安全需求开展确认测试，一般包括：

a) 针对安全需求中规定的，在上面已经完成的测试中没有覆盖到的安全功能和安全完整性（性能），开展测试（具体描述按照表 3）；

b) 开展环境条件下的功能测试，环境条件下的功能测试一般也称为型式试验；

c) 对 SIL2 以上的系统，开展扩展的功能测试，即测试安全需求描述内容以外的意外发生时，或极端情况下，组件/系统能否进入或保持安全状态；

d) 根据功能安全系统的应用情况，宜开展黑盒测试、最坏情况测试和统计测试（具体描述按照表 3）。

10.3 对于环境条件下的功能测试（型式试验），宜考虑以下内容：

a) 测试项目能够证明在安全需求中定义的应用环境条件得以满足；

b) 满足特定功能安全系统领域应用标准或产品标准中的型式试验[如安全可编程序控制器符合 IEC 61131（所有部分）中关于试验的要求]，典型的包括气候试验、机械试验；

c) 通过第三方的符合 GB/T 27025—2019 认可规则的测试实验室开展型式试验。

10.4 功能安全系统需要考虑开展加强的电磁兼容性测试（EMC），包括：

a) 相对于常规的系统，功能安全系统需要考虑开展加强的电磁兼容性测试，这些测试是在国家或行业强制的基础考虑上进行适当的强度增加，例如，测试的时间、次数等；

b) 以 IEC 61000-1-2:2016 作为针对电磁现象保障功能安全的方法指导；

c) 对于在国际标准或国家标准中没有特殊规定功能安全 EMC 测试内容的系统，电磁兼容试验的等级强度遵循 IEC 61326-3-1 和 IEC 61326-3-2 的相关内容；

d) 对于在国际标准或国家标准中有特殊规定功能安全 EMC 测试内容的系统，电磁兼容试验的等级强度可按照这些产品或领域标准的要求实施[例如，对于可编程序控制器符合 IEC 61131（所有部分）的相关内容]；

e) 通过第三方的符合 GB/T 27025—2019 认可规则且具有 IEC 61000-1-2、IEC 61326-3-1 和 IEC 61326-3-2 等安全相关系统 EMC 标准试验资质的测试实验室开展 EMC 试验。

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—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/T 27025—2019 检测和校准实验室能力的通用要求

[6] 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

[7] 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

[8] GB/T 41295.2—2022 功能安全应用指南 第2部分:设计和实现

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

[10] IEC 61000-1-2:2016 Electromagnetic compatibility (EMC)—Part 1-2:General—Methodology for the achievement of functional safety of electrical and electronic systems including equipment with regard to electromagnetic phenomena

[11] IEC 61131(all parts) Programmable controllers

[12] IEC 61800-5-2:2016 Adjustable speed electrical power drive systems—Part 5-2:Safety requirements—Functional