ICS 25.040
CCS N 10

中华人民共和国国家标准

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

Application guide of functional safety—
Part 1:Hazard identification and requirements analysis

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1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、中国软件评测中心(工业和信息化部软件与集成电路促进中心)、中国石油大学(北京)。

本文件主要起草人：熊文泽、魏振强、刘晓亮、田雨聪、史学玲、郭永振、姜涛、靳江红、张雪、董绍华、孟邹清、张亚彬、王璐、安健、李世斌、罗方伟、刘瑶、朱明露。

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。目的在于规定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。目的在于规定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。目的在于规定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。目的在于规定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1部分:危害辨识和需求分析

1 范围

本文件提供了功能安全系统应用指南中危害辨识和需求分析指导。

本文件适用于功能安全系统开发的概念阶段。

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 20438.1—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

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

危害辨识 hazard identification

受控设备、工艺过程、运行环境及功能安全系统本身中潜在危险的发生风险,通过理论推导和经验总结等方法分辨并标识风险的可接受程度。

3.2

需求分析 requirements analysis

根据危害辨识(3.1)的结论,制定功能安全系统的安全需求;根据功能安全系统的架构将安全需求分解到组件的过程。

3.3

系统相关人员 system related personnel

在功能安全系统的整个生命周期中,可能与系统发生直接关系的人员。

注:包括系统的定义、需求、设计、实施、测试、操作、维护、商务等人员。

3.4

运行场景 operation scenario

功能安全系统运行时,相关的自然环境、工艺过程、受控设备以及功能安全系统所组成的集合。这个场景是具象化的,能够通过实体仿真观察研究的。

3.5

安全需求　safety requirements

功能安全系统为了降低风险到可容忍级别，而需要满足的功能安全完整性等级要求。

注：安全需求在 GB/T 20438 中被称之为安全要求，两者具有相同的含义。

3.6

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。

4　缩略语

下列缩略语适用于本文件。

DC：诊断覆盖率(Diagnostic Coverage)

EMC：电磁兼容性(Electromagnetic Compatibility)

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

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　危害辨识和需求分析所处生命周期的阶段

本文件所提供的危害辨识和需求分析是指在功能安全系统研发设计前，基于系统的预期用途和工作环境对系统失效可能造成的危害情况进行充分的辨识，从而获得系统预期要实现的安全功能需求。

功能安全系统应用的整体生命周期宜按照 GB/T 20438.1—2017，功能安全系统生命周期宜按照 GB/T 20438.2—2017，功能安全系统软件生命周期宜按照 GB/T 20438.3—2017。

5.2　危害辨识和需求分析的基本考虑

在危害辨识和需求分析时，一般遵循如下的基本通则。

——重点关注会导致人员生命和健康受到伤害的危害。

——危害辨识需要综合考虑各要素的相互影响，需要系统相关人员共同提出辨识意见，系统相关人员包括：

- 工艺设计人员；
- 现场操作人员；
- 系统开发人员；
- 维修维护人员；
- 商务人员等。

——安全需求制定时，需要兼顾系统的基本控制功能。

——安全需求不会产生新的危害，并且需要进行迭代分析。

5.3　危害辨识和需求分析的过程考虑

在危害辨识和需求分析时，需要遵循如下的实施过程：

——选择功能安全系统需要运行场景以及需要控制的范围；
——收集同类场景已经发生过的危险事件数据，包括已确定的危险事件和导致该危险事件的事件序列；
——征询系统相关人员对危险事件的意见和对系统的需求；
——记录危害辨识结果，并对不可接受危害，逐一制定安全措施；
——分析安全措施的有效性，总结编制安全需求；
——征询系统相关人员对安全需求合理性的意见；
——安全需求经过审批后作为功能安全系统的开发的依据；
——根据系统的架构设计，将安全需求的实现方法分配到每一个子系统或者组件中。

5.4 危害辨识和需求分析的变更考虑

在危害辨识和需求分析时，需要考虑如下的变更：
——变更一般由系统开发人员发起；
——需要进行变更影响分析，重点是变更前后运行场景的差异对比；
——变更具有足够的合理性，合理的变更具有如下几个特征：
- 所有系统相关人员均不强烈反对此项需求变更，
- 此项需求变更能够获得审批授权签字人的认可，
- 变更有具体的原因，这些原因包括：危害辨识的错误或疏漏，市场竞争原因，现有技术条件无法满足此项需求，需求完全无法被验证等；

——变更需要通知所有引用危害辨识记录和安全需求的人员。

5.5 危害辨识和需求分析的文档化考虑

在危害辨识和需求分析时，需要文档化的内容包括：
——运行场景的内容和特征；
——危害的特征；
——安全需求；
——危害与需求的关联关系；
——变更影响分析；
——变更的审批记录；
——发布的审批记录。

6 危害辨识

6.1 危害辨识的一般过程

危害辨识从分析自然环境和工艺过程开始，到获得风险记录为止，一般过程如图 1 所示。

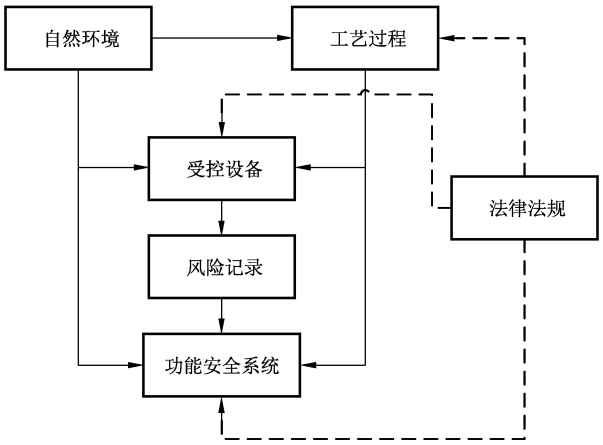

图 1　危害辨识的一般过程

6.2　自然环境在危害辨识过程中的影响分析

危害辨识中的自然环境包括：气候、天气、地理、生物环境、人类社会等，对于自然环境的影响，需要从如下方面进行分析：

——重大自然灾害影响，如地震、海啸、洪水、飓风、泥石流、雪崩；

——轻度自然灾害的影响，如冰雹、暴雨、大风、雷电、太阳活动异常、沙尘暴、雾霾；

——气候的影响，如温度、风沙、盐雾、潮湿、日照；

——生物活动影响，如动物闯入、飞鸟、昆虫、植物发芽、发霉；

——与工艺无关的人类活动影响，如违规闯入、施工、人为破坏电力或通信线路；

——公共服务影响，如停水、停电、停气、交通中断、通信中断。

6.3　法律法规在危害辨识过程中的影响分析

法律法规的影响分析，重点不在于技术层面，而在于组织管理层面，需要从如下方面进行分析：

——明文规定的关于工艺、设备、系统的要求；

——条文中对于人员生命财产的安全保护规定；

——对环境保护的规定；

——对伤害程度的定级。

6.4　工艺过程在危害辨识过程中的影响分析

工艺过程是运行场景存在风险的直接原因，这是生产生活不可避免的环节，为了辨识危害，需要从如下方面进行分析：

——原料和产品在运输和存储过程中有毒物质泄漏，易燃易爆品被引燃引爆，意外的接触导致的剧烈化学反应，例如，金属钠与水，长期大量堆放引发的自燃；

——高温工艺的温度控制、超温保护、异常热传导；

——高压工艺的压力控制、超压保护、压力泄漏；

——高速工艺的速度控制、超速保护、速度骤降；

——爆炸性环境中的静电火花和电源通断时的电火花；

——存在明火的环境中，意外泄漏粉尘或者可燃气体；

——设备运行环境的人员所承受的加速度、温度、噪声、氧气浓度及气压等。

6.5 受控设备的风险

受控设备的风险，需要从如下方面进行辨识：

——自然环境、法律法规及工艺过程对受控设备的影响；

——老化和腐蚀引起的泄漏、堵塞、断裂；

——周边设施坍塌、异动对受控设备的撞击；

——错误的现场人员操控，维修维护。

6.6 安全系统的风险

功能安全系统自身的风险，需要从如下方面进行辨识：

——自然环境、法律法规、工艺过程对安全系统的影响；

——错误的人为操作，例如，在线更新安全逻辑、长时间旁路；

——不正确的维修维护操作，例如，线缆接错、不停车维修；

——配置错误，例如，未明确安全状态、联锁触发条件不合理。

6.7 风险记录

风险记录表示例见表 1。

表 1 风险记录表示例

风险描述	危险源	发生概率	后果严重程度	是否可检测	是否可防御	安全措施
此处描述风险发生的过程以及可能引发的后果	导致危害发生的最终源头，可以简化描述为：自然环境、工艺、受控设备、安全系统	极小：＜1 次/10 年 很小：1 次/年～1 次/10 年 偶尔：1 次/月～1 次/年 经常：1 次/周～1 次/月 频繁：1 次/天～1 次/周	特大：死亡 10 人及以上，或经济损失 5 000 万元及以上 重大：死亡 3 人～9 人或 10 人以上重伤，或经济损失 1 000 万元～5 000 万元 严重：死亡 1 人～2 人或 3 人～9 人重伤，或经济损失 500 万元～1 000 万元 普通：1 人～2 人重伤，或经济损失 100 万元～500 万元 轻微：无重伤死亡但造成停产停工，或经济损失 100 万元以内	是/否	是/否	仅描述安全系统相关的安全措施。其他安全措施可记录为“其他措施”

7 需求分析

制定安全需求的依据是风险记录的安全措施，制定安全需求至少需要考虑如下因素：

——安全需求是针对功能安全系统的要求，需要其他装置完成的安全要求不需要列出；

——安全需求宜考虑信息安全，并进行脆弱性分析；

——安全需求宜考虑实体防护，例如，机柜等；

——每一项对应风险降低的安全需求确定安全完整性等级；

——安全需求能够被验证。

系统安全要求规格书可以包括如下的具体内容。

——遵守产品标准和安全标准，符合的法律、文化、政策要求。

——产品的功能要求，需要考虑区分安全功能和非安全功能，需要对安全需求进行编号，需要描述对操作、维护、启动、重启的要求。

——安全完整性等级的要求，所有安全需求中安全完整性等级要求最高的作为整个系统的安全完整性等级要求。

——结构方面包括：

- 系统的分类，无法明确描述所有失效模式的系统，定义为B类系统；
- 冗余架构，以MooN的形式描述，N是系统的通道数量，M是能够让系统进入安全状态的最少通道数量。

——运行模式方面，包括：

- 低要求模式，仅当要求时才执行将受控设备导入规定安全状态的安全功能，并且要求的频率不大于每年一次；
- 高要求模式，将受控设备导入规定安全状态的安全功能仅当要求时才执行，并且要求的频率大于每年一次；
- 连续模式，安全功能将受控设备保持在安全状态是正常运行的一部分。

——诊断方面，包括：

- 诊断覆盖率(DC)和安全失效分数(SFF)的要求，根据安全完整性等级的要求确定；
- 诊断的范围，需要考虑供电、输入回路、输出回路、时钟、通信通道、存储、可编程组件；
- 故障响应时间，任意一个可被系统自诊断发现的故障，从故障发生到系统针对该故障完成响应处理的时间间隔；
- 平均维修时间，故障被发现，到故障被排除的平均时长；
- 自诊断周期，任何一个可被系统自诊断发现的故障，从故障发生到系统发现该故障的最长时间间隔；
- 检验测试间隔，对功能安全系统所有安全功能的有效性进行全面检验测试的间隔时间，这些检验测试以人工检验为主；
- 检验测试要求，如：检验测试前的准备，检测测试项目，检验测试的通过标准，检验测试需要的工具或设施；
- 故障报警要求：报警的方式，报警的持续时间，报警的消除条件。

——应用场景，需要规定功能安全系统具体应用的领域和工况环境。

——环境方面：安装方式、室内/室外、温度、湿度、所需空间、气压/海拔、运输及存储。

——EMC方面，根据不同的应用现场，参照不同的国家标准或行业标准。

——接口方面：输入输出接口、通信接口、人机操作接口，安全相关组件和非安全相关组件的接口。

——通信方面：速率、节点数、传输距离及抗干扰能力。

——性能方面：响应时间、容量/点数规模、扩展性能、防爆性能及防护性能。

——安全状态：安全状态时的输出、显示，安全状态与其他状态的切换方面。

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