ICS 35.240.01
CCS L 67

中华人民共和国国家标准

GB/T 44062—2024

自动化系统与集成　自动化设备安全评估

Automation systems and integration—Safety evaluation for automated devices

2024-05-28 发布　　2024-12-01 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 …… Ⅲ
引言 …… Ⅳ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　缩略语 …… 4
5　安全档案与论证 …… 5
5.1　通则 …… 5
5.2　安全档案样式和格式 …… 7
5.3　声明和论证的充分性 …… 9
5.4　论据的充分性 …… 13
5.5　可接受风险 …… 15
5.6　安全文化 …… 17
5.7　项目范围 …… 18
6　风险评估 …… 20
6.1　通则 …… 20
6.2　故障模型 …… 21
6.3　危害 …… 33
6.4　风险评估 …… 35
6.5　风险消减和消减措施效果评估 …… 38
参考文献 …… 41

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。

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。

本文件由全国自动化系统与集成标准化技术委员会(SAC/TC 159)归口。

本文件起草单位：北京机械工业自动化研究所有限公司、青岛市标准化研究院、优力标准技术服务(上海)有限公司北京分公司、纳恩博(北京)科技有限公司。

本文件主要起草人：郭栋、翟越、常平、姜江、高亚平、张斯光、杨书评、司佳顺、袁望坦、孙逊。

引　言

为了确保在设计过程中以及整个系统生命周期内，以可接受的方式持续全面考虑自动化设备的安全性，为安全自动化设备提供佐证，提出了可用于确定安全档案可接受性的评估标准。本文件主要用于指导制造商、集成商、零部件供应商设计、制造和评估自动化设备时出具的安全档案可以佐证自动化设备的安全性。

本文件采用强制性要素、必备要素、强烈推荐要素、推荐要素和合规性作为规范性要素来规范安全档案各条款。不同类型要素的安全档案偏差方法摘要见表1。

表1　安全档案偏差方法

规范性要素	摘要
强制性要素	不准许出现安全档案偏差
必备要素	安全档案偏差仅适用于因项目的基本性质和/或项目的当前部署状态而本质上不适用的要求。安全档案中记录的所有安全用例偏差均已提供理由。通过影响分析和生命周期跟踪，监控适用性状态变化的可能性
强烈推荐要素	在有可接受理由的情况下，允许出现安全档案偏差。通过影响分析和生命周期跟踪，监控适用性状态变化的可能性。安全档案中记录的所有安全档案偏差均已提供理由
推荐要素	可选项目。无需在安全档案中提及。安全档案偏差不需要论据支持
合规性	通过自我审计和独立评估对各条款的合规性进行评估

自动化系统与集成　自动化设备安全评估

1　范围

本文件规定了建立和评估自动化设备安全论证的合规性要求，主要包括安全档案、风险评估等内容。

本文件适用于指导制造商、集成商、零部件供应商设计、制造和评估自动化设备。

2　规范性引用文件

本文件没有规范性引用文件。

3　术语和定义

下列术语和定义适用于本文件。

3.1

可接受　acceptable

足以达到安全档案中确定的整体项目风险。

示例：“可接受的测试范围”是指在获得声称的风险消减可信度后，测试范围的数量足以支持安全档案对整体项目风险的声明。

注：这是一个与安全档案的有效性和完整性相关的客观术语，而不是与任何特定评估者的个人观点相关的主观术语。

3.2

激发（故障或危害）　activation（of faults or hazards）

导致系统因故障或危害而可能失效的输入或情况。

示例：内存中由单一事件扰乱的损坏位视为故障。读取存储器位置时，故障被激发并导致计算误差，该误差会以不正确或不安全的项目行为造成系统失效。

注：故障消减措施（例如，错误检测编码）能防止激发的故障引起失效。

3.3

人工智能技术　artificial intelligence technologies

计算算法以及其他相关技术（包括归纳学习、故意非确定性行为、基于规则的系统、计算机视觉、启发式搜索以及其他技术）的一般描述。

注：该术语属于从广义上进行解释的描述性术语，以涵盖通常不适用于传统软件安全方法的软件。无论其是否涉及“智能”方面，均不在本文件范围之内。

3.4

论证　argue

构建满足特定要求的**安全档案**（3.32）的过程。

示例：“开发者应论证所有危害均已消减”，即指示开发者需在安全档案中包含每种危害实际上已消减的声明、论据和证据。

3.5

评估员　assessor

开展评估的一名或多名人员。