ICS 29.020
CCS K 09

中华人民共和国国家标准

GB/T 34924—2024/IEC GUIDE 116:2018
代替 GB/T 34924—2017

低压电气设备安全风险评估和风险降低指南

Guidelines for safety related risk assessment and risk reduction for low voltage equipment

（IEC GUIDE 116:2018,IDT）

2024-04-25 发布　　2024-11-01 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。

本文件代替GB/T 34924—2017《低压电气设备安全风险评估和风险降低指南》。与GB/T 34924—2017相比,除结构调整和编辑性改动外,主要技术变化如下:

a) 更改了第1章,细化为“范围”“目的”和“排除和限制”(见第1章,2017年版的第1章);

b) 增加了“3.1.7”、“3.1.9”、“3.1.11”、“3.1.12”、“3.1.13”、“3.1.14”、“3.1.24”、“3.1.27”、“3.1.28”、“3.1.29”、“3.1.30”等术语的定义,更改了“3.1.2”、“3.1.3”、“3.1.4”、“3.1.5”、“3.1.6”、“3.1.15”、“3.1.16”、“3.1.17”、“3.1.18”、“3.1.20”、“3.1.23”、“3.1.25”等术语的定义(见3.1);

c) 增加了缩略语(见3.2);

d) 增加了风险不可容许的重复迭代过程(见图2);

e) 增加了“使用限制”的考虑因素(见第5章);

f) 增加了“防护措施失效或没起到有效防护”的原因(见8.2.3);

g) 增加了“关于残余风险的使用信息”(见8.3);

h) 增加了“安全相关的信息安全风险”(见A.8)。

本文件等同采用IEC GUIDE 116:2018《低压电气设备安全风险评估和风险降低指南》,文件类型由IEC的指南调整为我国的国家标准。

本文件做了下列最小限度的编辑性改动:

——将标准名称更改为《低压电气设备安全风险评估和风险降低指南》。

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。

本文件由全国电气安全标准化技术委员会(SAC/TC 25)提出并归口。

本文件起草单位:国网浙江省电力有限公司嘉兴供电公司、中国能源建设集团江苏省电力设计院有限公司、机械工业北京电工技术经济研究所、国网北京市电力公司、厦门恺成精密机械有限公司、国网浙江省电力有限公司杭州市钱塘区供电公司、国网陕西省电力有限公司、西门子(中国)有限公司、中天电气技术有限公司、中韶电气股份有限公司、广东华南家电研究院、中国电器工业协会、广东光达电气股份有限公司、杭州之江开关股份有限公司、广东正诚电气科技有限公司、中山市深中标准质量研究中心、南阳市一通防爆电气有限公司、广东粤电新会发电有限公司、温州昌泰电气有限公司、金杯电工衡阳电缆有限公司、广安电气检测中心(广东)有限公司、莱芜鲁能开源集团电器有限公司、广州长川科技有限公司、珠海沃顿电气有限公司、兴盛电器股份有限公司。

本文件主要起草人:马红、钱国良、殷超、李彬、冯凯、金建华、李立鹏、马嘉菲、方晓燕、周永军、曾雁鸿、杨四化、赖静、于良中、仲超、陈益栓、陈伟亮、宗林才、梁昕、路用军、夏君山、陈烨、李旭、冯玉花、郑纯、龚利武、苏嘉彬、张哲、范莹、方忠昉、胡少中、傅进、梁子俊、夏向阳、李康、贾东强、夏文红。

本文件及其所代替文件的历次版本发布情况为:

——2017年首次发布GB/T 34924—2017;

——本次为第一次修订。

低压电气设备安全风险评估和风险降低指南

1 范围和目的

1.1 范围

本文件基于ISO/IEC Guide 51提供了实现低压电气设备安全的指导。这些指导包括风险评估，集合了低压电气设备相关的设计、使用、事件、事故及伤害的知识和经验，用于评估设备生命周期相关阶段风险(见第6章)，以及执行降低风险措施的基本原则。各技术委员会宜在适当情况下采用本文件。

本文件在实施风险评估方面给出了ISO/IEC Guide 50、ISO/IEC Guide 51和ISO/IEC Guide 71的附加指导信息。确立了危险识别、风险预估和风险评价(包括风险比较)和必要风险降低的程序。本文件涉及的伤害包括对人员、财产或牲畜的潜在伤害。各技术委员会不必使用本文件的结构。

本文件还包括涉及充分的设备安全使用信息的设备文件要求。

1.2 目的

本文件旨在为各技术委员会制定低压电气设备安全决策及验证进行风险评估所需文件时提供指导。

本文件适用于交流电压1 000 V及以下，直流电压1 500 V及以下的各类电气设备。额定电压指电气输入或输出的电压，而不是设备内部可能出现的电压。

附录A给出了适用于低压电气设备的基本健康和安全要素。

风险评价参考的文件见附录B。危险相关示例见附录C。技术委员会自我评估的记录见附录D。

1.3 排除和限制

本文件不适用于设备、电气系统或装置的基本部件，这些基本部件的风险评估很大程度上取决于在电气系统或装置中的使用和装配情况。对于拟并入其他电气设备并能根据本文件进行风险评估的电气部件，通常需要对此类部件的并入方式的安全做进一步评估。

注1：宜正确认识基本部件的排除范围，不能将其扩展到灯具、启动器、熔断器、家用开关、电气装置元件等。即使经常与其他电气设备一起使用，且必须正确安装以实现功能的部件，也属于本文件适用范围。

注2：产品使用者所采取的降低风险措施取决于各国的法律规定，特别是职业健康和安全体系的要求。

本文件不适用于安全认证。当产品标准的技术内容不能覆盖领域内设备的所有潜在危险，尤其是伴随新兴技术可能出现新的危险时，鼓励在产品标准中增加与风险评估有关的安全条款。

如果风险评估给出了与健康和安全不直接相关的方面，如环境保护、能源消耗、气候变化等，则健康和安全相关风险的风险降低，特别是对于人员的风险降低将优先于其他方面。其他方面能由法规定义。

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。

ISO/IEC Guide 51：2014 安全方面 标准中考虑安全方面的编写指南(Safety aspects—

Guidelines for their inclusion in standards)

注：GB/T 20002.4—2015 标准中特定内容的起草 第4部分：标准中涉及安全的内容(ISO/IEC Guide 51：2014，MOD)

IEC Guide 104:2010 安全出版物的编写及基础安全出版物和多专业共用安全出版物的应用导则(The preparation of safety publications and the use of basic safety publications and group safety publications)

注：GB/T 16499—2017 电工电子安全出版物的编写及基础安全出版物和多专业共用安全出版物的应用导则(IEC Guide 104:2010，NEQ)

IEC Guide 117：2010 电气设备 可接触热表面的温度(Electrotechnical equipment—Temperatures of touchable hot surfaces)

注：GB/T 34662—2017 电气设备 可接触热表面的温度指南(IEC Guide 117:2010，IDT)

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

ISO与IEC维护以下用于标准化的术语数据库，网址如下：

——ISO：http://www.iso.org/obp/

——IEC：http://www.electropedia.org/

3.1.1

低压电气设备 low voltage equipment

电源或输出电压不超过交流1 000 V和直流1 500 V的用于发电、输电、配电及用电等用途的电气设备或装置。

示例：电气设备包括发电机、电气开关设备和控制设备及成套装置、电气布线系统、空调机组、储能机组、可编程电子设备等。

3.1.2

伤害 harm

对人体健康的损害或损伤，对财产或环境的损害。

[来源：ISO/IEC Guide 51:2014，3.1]

3.1.3

危险 hazard

可能导致伤害(3.1.2)的潜在根源。

[来源：ISO/IEC Guide 51:2014，3.2]

3.1.4

危险区域 hazard zone

产品、过程或服务内部和/或周围的任何空间，在该空间人员或牲畜可能暴露于危险(3.1.3)中。

3.1.5

危险事件 hazardous event

能导致伤害(3.1.2)的事件。

注：危险事件在短时间内或长时间内都会发生。

[来源：ISO/IEC Guide 51:2014，3.3]

3.1.6

危险情况 hazardous situation

人员、财产或环境暴露于一种或多种危险中的情形。

[来源:ISO/IEC Guide 51:2014,3.4]

3.1.7

电弧 arc

设备内由不同电势的带电部件之间和/或带电部件与其他导电部件之间故障引起的空气自放电短路。

[来源:IEC 61641:2014,3.5]

3.1.8

事件 incident

过去的危险事件(3.1.5)。

注:已发生并且造成伤害的事件视为意外事故。已发生但未造成伤害的事件视为未遂事件。

3.1.9

事故 accident

造成伤害(3.1.2)的事件(3.1.8)。

3.1.10

故障 malfunction

由于下述各种原因,电气设备不能发挥预期功能的情况,例如:

——加工材料或加工件特性或尺寸的变化;

——一个(或多个)零部件或服务的故障;

——外部干扰(例如:电击、振动、电磁干扰);

——设计错误或缺陷(例如:软件错误);

——电源干扰;

——周围环境(例如:因温度变化而导致的凝结)。

3.1.11

风险指数 risk index

用于衡量风险(3.1.18)发生的可能性、广度和严重程度的综合得分。

[来源:ISO 17666:2016,3.1.3]

3.1.12

固有安全设计 inherently safe design

通过更改产品或系统的设计或操作方式,消除危险(3.1.3)和/或降低风险(3.1.18)而采取的措施。

[来源:ISO/IEC Guide 51:2014,3.5]

3.1.13

安全防护 safeguarding

使用安全防护装置保护人员和牲畜的防护措施(3.1.20),使其免受那些不能合理消除的危险(3.1.3)或者通过固有安全设计(3.1.12)措施无法充分降低的风险(3.1.18)。

[来源:ISO 12100:2010,3.21,有修改]

3.1.14

补充防护措施 complementary protective measure

涉及防护装置(非安全防护装置)的降低风险措施(3.1.20)。

防护装置示例:急停装置、联锁装置、使能装置等。

3.1.15

预期的使用 intended use

按产品和/或系统提供的信息使用,无此类信息时,按通常理解的模式使用。

[来源:ISO/IEC Guide 51:2014,3.6]

3.1.16

可合理预见的误使用　reasonably foreseeable misuse

由容易预见的人的行为所引起的,未按供方提供的方式对产品或系统的使用。

注 1:容易预见的人的行为包括全部类型的用户行为,例如老人、儿童和残疾人士。更多信息见 ISO 10377。

注 2:在消费者安全方面,术语"可合理预见的使用"越来越多地被用作"预期的使用"和"可合理预见的误使用"两者的同义词。

[来源:ISO/IEC Guide 51:2014,3.7,有修改]

3.1.17

残余风险　residual risk

在实施降低风险措施(3.20)后仍然存在的风险(3.1.18)。

注:区分为:

——在设计者采取防护措施(3.1.20)后的残余风险;

——在用户实施所有防护措施(3.1.20)后的残余风险。

[来源:ISO/IEC Guide 51:2014,3.8,有修改]

3.1.18

风险　risk

伤害(3.1.2)发生概率和伤害严重程度的组合。

注:发生概率包括暴露在危险情况(3.1.6)中、发生危险事件(3.1.5),以及避免或限制伤害(3.1.2)的可能性。

[来源:ISO/IEC Guide 51:2014,3.9]

3.1.19

风险评估　risk assessment

包括风险分析和风险评价的全过程。

[来源:ISO/IEC Guide 51:2014,3.11]

3.1.20

降低风险措施　risk reduction measure

防护措施　protective measure

消除危险(3.1.3)或降低风险(3.1.18)的行动或手段。

示例:固有安全设计(3.1.12);防护装置;个体防护装备;使用和安装信息;工作安排;培训;设备应用;监督。

[来源:ISO/IEC Guide 51:2014,3.13]

3.1.21

安全　safety

免除了不可接受的风险(3.1.18)的状态。

[来源:ISO/IEC Guide 51:2014,3.14]

3.1.22

可容许风险　tolerable risk

可接受风险　acceptable risk

按当今社会价值取向在一定范围内被接受的风险(3.1.18)。

[来源:ISO/IEC Guide 51:2014,3.15,有修改]

3.1.23

安全整合　safety integration

运用"三步骤方法"(见图 1)将低压电气设备的残余风险(3.1.17)降至可容许风险(3.1.22)水平。

注:A.2 给出了更多信息。

3.1.24

功能安全　functional safety

整体安全的一部分,取决于功能和物理单元对响应其输入功能的正确行使。

注：见 IEC TR 61508-0 和 IEC 61508。

[来源：IEC 60050-351:2013,351-57-06]

3.1.25

充分防护　adequate protection

将风险(3.1.18)降至可容许水平的防护。

3.1.26

单一故障状态　single fault condition

指单一防护措施失效，或单个组件或设备发生故障的状态。

注 1：如果一个单一故障状态不可避免地会导致一个或多个其他故障状态，则所有故障状态均被视为单一故障状态。

注 2：加强防护定义见 IEV 903-02-08。

[来源：IEC Guide 104:2010,3.8]

3.1.27

安全相关的安全风险　Safety-related security risk

特定安全威胁(3.1.28)利用特定安全漏洞(3.1.30)导致危险情况(3.1.6)的风险(3.1.18)。

[来源：IEC/TS 62443-1-1:2009,3.2.87，有修改]

3.1.28

安全威胁　security threat

当有违反安全并引起伤害(3.1.2)的环境、能力、行动或事件出现时，存在安全违规(3.1.29)的可能性。

[来源：IEC TS 62443-1-1:2009,3.2.125，有修改]

3.1.29

安全违规　security violation

来自外部入侵或内部无意的违反或其他方式破坏安全策略的行为或事件。

[来源：IEC/TS 62443-1-1:2009,3.2.116，有修改]

3.1.30

安全漏洞　security vulnerability

系统设计、实现或运行和管理中的缺陷或弱点，能被利用来扰乱系统的完整性或安全策略。

[来源：IEC/TS 62443-1-1:2009,3.2.135，有修改]

3.2　缩略语

下列缩略语适用于本文件。

HMI：人机界面(Human machine interface)

LAN：局域网(Local area network)

TCP：传输控制协议(Transmission control protocol)

USB：通用串行总线(Universal serial bus)

WLAN：无线局域网(Wireless loal area network)

4　基本原则

4.1　安全整合原则

安全整合原则见图 1。最低的必要风险降低是指：特定情况下风险被降低至实现可容许风险。必要风险降低的概念对制定电气设备安全要求是至关重要的。确定具体危险事件的可容许风险旨在说明

就风险的两个组成要素而言哪些是合理的(见 3.1.18、7.2 和图 2)。

风险取决于许多因素(例如:伤害的严重程度、财产损失、暴露在危险下的人员数量、一人或多人暴露在危险下的频度和暴露持续时间)。

如果需要在产品标准中的不同降低风险措施中进行选择,这些标准宜清楚地表明制造商如何通过对自身设备的详细调查来实施包括安全整合在内的风险评估原则。制造商通过这种方式在确定适当的防护措施方面将更具灵活性和自由创新性,并从中获益。制造商对所属设备的详细规格和有关内容最为了解时,当产品更复杂时这种方式尤为重要。下列信息来源也可做进一步考虑:

——来自各种来源的要求,包括一般要求和与具体应用直接相关的要求;

——来自各种来源的指导;

——与应用相关的不同方面之间的讨论和协定;

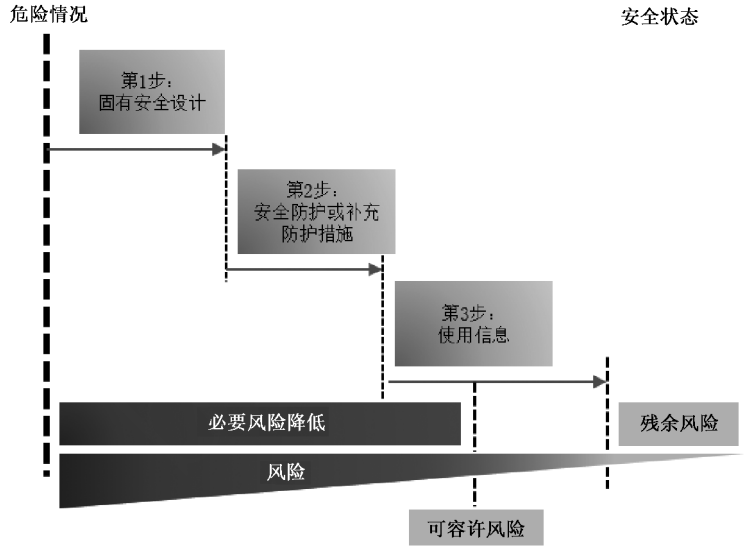
——国际研讨和协定(国家标准和国际标准在实现应用案例的可容许风险水平方面变得日益重要);

——行业标准和指南;

——顾问机构提供的第三方行业、专家和科学建议;

——所有相关利益方确定的当前社会价值;

——用户规范。



注:某些时候,通过第 1 步或第 1 步和第 2 步已达到可容许风险。

图 1 安全整合原则

4.2 基本概念

安全风险评估是一系列逻辑步骤,从判定低压电气设备的限制条件开始。下一步需要系统地识别与低压电气设备相关的危险。在风险预估、风险评价和/或风险比较之后,进行风险评估,必要时风险降低。反复这一过程,给出了尽可能消除危险和实施额外降低风险措施(防护措施)的迭代过程。

风险评估包括以下程序(见图 2)。

a) 风险分析

1) 判定低压电气设备的限制条件(见第 5 章);

2) 危险识别(见第 6 章);

3) 风险预估(见第 7 章)。

b） 风险评价/风险比较(见第 8 章)。

风险分析为风险评价提供了用于判断低压电气设备安全性的信息。

风险评估依赖于判断性决策。这些决策应以定性方法为依据,并尽可能辅以定量方法。当伤害的潜在严重程度和范围较大、并且资源或数据可用,定量方法是合适的。定量方法有助于评估供选择的降低风险措施,以确定哪种降低风险措施提供更好的防护。

注 1：定量方法的应用受到可用有用数据量的限制,在许多应用中只能进行定性风险评估。

注 2：低压电气设备的风险评估过程能按以下步骤进行：

——确定低压电气设备的适当范围和目标用户(见第 5 章)；

——确定低压电气设备的预期的使用和可合理预见的误使用(见第 5 章)；

——识别低压电气设备每个生命周期阶段的危险,例如:设计、制造、安装、维护、修理和处置(见第 6 章)；

——预估每个已识别危险所造成的风险(见第 7 章)；

——评估已识别危险引起的风险(见第 8 章)；

——如果低压电气设备的风险评估结果表明残余风险处于可容许水平,不必采取进一步措施(见第 8 章)；

——如果残余风险不可容许,有必要实施风险降低(见第 9 章)；

——重复迭代,直到残余风险降至可容许水平。

风险评估应记录已遵循的程序和所取得的结果(见第 10 章)。

风险评估决定了是否需要降低风险。降低风险过程见第 9 章。

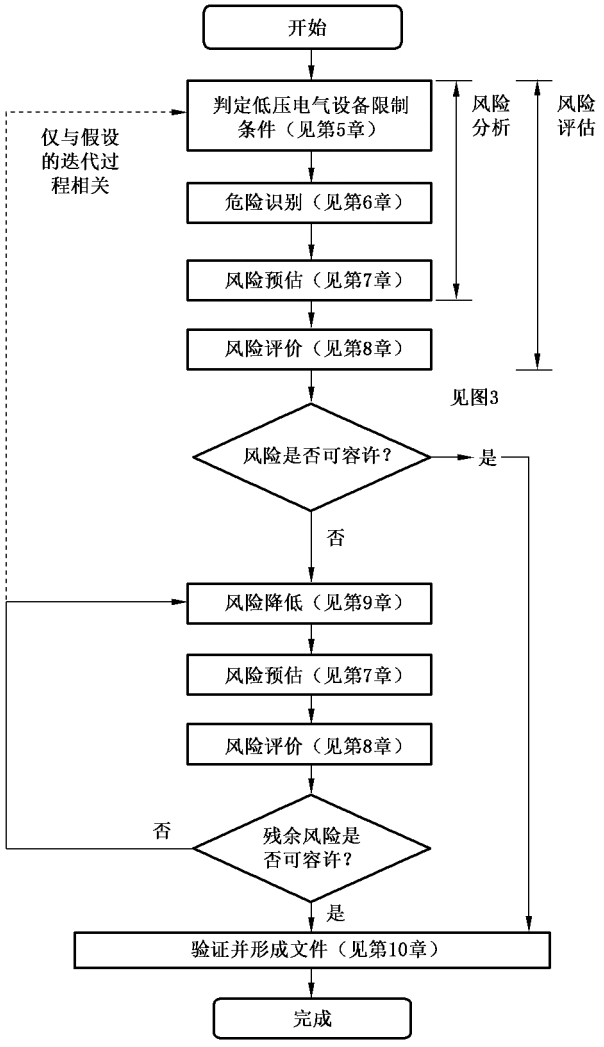


图 2 风险评估和风险降低的迭代过程

4.2.1 风险评估信息

用于风险评估及定性和定量分析的信息宜包括以下内容：

a) 低压电气设备的限值条件(见第5章)；

b) 低压电气设备整个生命周期各个阶段的描述(例如：运输、组装和安装、调试和使用)；

c) 构成低压电气设备特性的设计图样或其他方案；

d) 现有或类似低压电气设备的任何事故、事件或故障记录(如果可用)；

e) 由于排放(噪声、振动、尘埃、烟雾等)、低压电气设备使用的化学品或加工的材料等导致的可能风险的信息；

f) 随低压电气设备交付的可用使用信息；

以上信息应随着设计改进或修改而更新。

如果有足够的关于不同类型设备的危险和事故情况的信息，通常可对与这些情况相关的类似危险情况进行比较。

不应直接将无事故历史、只有少数事故或事故后果不严重这三种情况视为低风险。

对于定量分析，如果确定相关数据适用，可使用数据库、手册、实验室和制造商说明中的数据。文件中应说明这些数据的不确定性(见第10章)。

4.2.2 有关低压电气设备描述的信息

有关低压电气设备描述的信息宜包括以下方面。

a) 低压电气设备预期规范，包括：

1) 对设备整个生命周期各个阶段的描述(例如：运输、组装和安装、调试、维护和使用)；

2) 构成设备特性的设计图样或其他方案；

3) 所需能源和供应方式。

b) 关于设备使用的可用信息。

4.2.3 相关标准和其他可用文件

相关文件包括：

a) 相关出版物，例如国际标准；

b) 安全数据表或其他相关技术规范。

4.2.4 关于使用经验的信息

设备使用经验的信息宜包括：

a) 现有或类似设备的任何历史记录(如果引用的是制造商收集的数据，这些数据仍归制造商所有)；

b) 健康损害记录。

4.2.5 相关人类工效原则

应包括与健康相关的信息：

a) 随着设计不断改进，或；

b) 随着必要的修改。

5 判定低压电气设备的限制条件

风险评估从判定低压电气设备的限制条件开始。本文件将低压电气设备的限制条件分为了四类。

它们用于定义预期的使用和可合理预见的误使用。该分类并不详尽,前后顺序无关重要性或相关性。

a) 使用限制,包括预期的使用和可合理预见的误使用,考虑以下因素。
   1) 低压电气设备的不同操作模式和用户的不同干涉程序(包括对使用低压电气设备的可预见故障的干预)。
   2) 用户的培训、经验或能力的预期等级,例如:操作人员、维护人员或技术人员、实习人员和学徒、社会公众。

注:考虑使用低压电气设备(例如:工业用、非工业用和家用)人员的性别、年龄、惯用手或身体缺陷(例如:视力或听力损伤、身高、力量)。

   3) 用于使用的不同附件和连接设备。
b) 空间限制,考虑以下因素。
   1) 移动范围。
   2) 低压电气设备安装和维护的空间要求。
   3) 人机交互,例如:“人机”界面。
   4) “机器—电源”接口。
c) 时间限制,考虑以下因素。
   1) 低压电气设备和/或其零部件(例如:工具、耐磨件)的可用寿命,考虑其预期的使用和可合理预见的误使用。
   2) 建议的使用周期。
d) 其他限制,考虑以下因素。
   1) 环境,建议的最低、最高温度,能否在户内或户外、干燥或潮湿、阳光直射下操作,对尘埃和湿度、振动、冲击等的耐受性。
   2) 清扫,所需清洁程度。

判定低压电气设备的限制条件时,应考虑低压电气设备生命周期的相关阶段。

6 危险识别

系统地识别低压电气设备生命周期中所有阶段的潜在危险、危险情况和危险事件是任何风险评估的重要步骤。区分所考虑的危险、危险情况或危险事件是否会对人员和/或牲畜或财产造成损害。暴露在危险情况下能够立即或在一段时间内造成伤害。需考虑以下电气设备生命周期的所有阶段:

a) 运输;
b) 组装和安装;
c) 试运行;
d) 使用,用户的维护和服务人员的服务;
e) 尽可能安全地终止运行、拆解和处置。

注:许多国家在危险物使用处理以及电气电子设备回收方面有着国家或区域的法律要求。

从低压电气设备执行的操作以及与设备互动人员执行的任务中完成危险识别是十分重要的。

任务识别宜考虑与上述低压电气设备生命周期所有阶段相关的所有任务,包括但不限于:

a) 设置
b) 测试;
c) 编程;
d) 启动;
e) 所有操作模式下的任务;
f) 拆除低压电气设备的一个或多个部件;

g） 正常停止；
h） 紧急停止；
i） 意外启动；
j） 故障查找/故障排除(操作人员干涉)；
k） 清洁和清扫；
l） 计划内维护和维修；
m） 计划外维护和维修；
n） 可合理预见的误使用。

应识别出与各项任务和安全威胁相关的所有危险、危险情况或危险事件。

还应识别出与任务无直接关联的可合理预见的附加危险、危险情况或危险事件(例如：地震、雷击、过多的雪载荷、噪声、低压电气设备倒塌或解体等)。

危险、危险情况和危险事件的示例见附录C，这些示例有助于危险识别。

用于识别和记录被评估低压电气设备相关危险的工具见附录D。根据附录A中描述的安全原则和基本安全要求，识别这些危险并记录在附录D的“是否相关”一栏中。

7 风险预估

7.1 一般原则

危险识别(见第6章)后，通过判定7.2中的各项风险要素，应对每种危险情况进行风险预估。判定风险要素时，考虑7.3中的因素是十分必要的。由此完成风险分析。

7.2 风险要素

7.2.1 风险要素组合

与特定情况或技术过程相关的风险来源于下列要素的组合。

a） 伤害的严重程度。
b） 伤害发生的可能性，取决于：
   1） 暴露在危险情况的可能性；
   2） 危险事件发生的可能性；
   3） 技术和人员能力避免或限制伤害发生的可能性。

这些要素的组合见图3。具体要求见7.2.2、7.2.3和7.3。

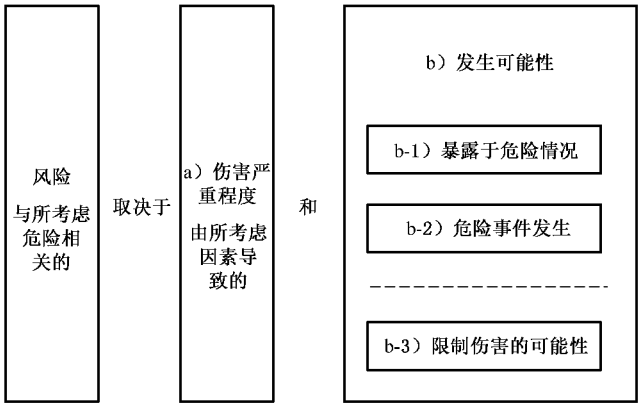


图3 风险预估的要素

7.2.2 伤害的严重程度

通过考虑如下因素预估伤害的严重程度。

a) 伤害的严重程度包括：

1) 轻微(正常可逆或短期内可修复)，见图 4 中的 S_1；

2) 高度(正常可逆或长期内可修复)，见图 4 中的 S_2；

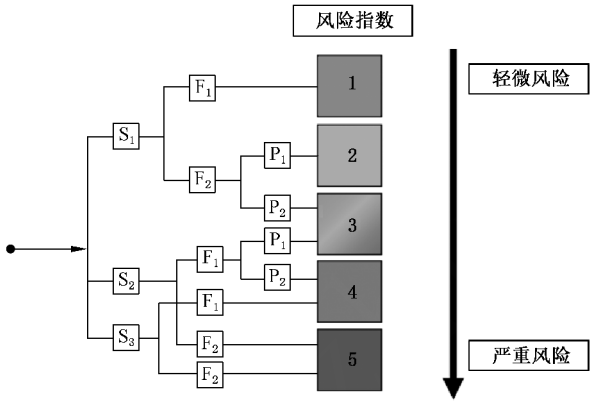
3) 严重(正常不可逆或不可修复)或死亡，见图 4 中的 S_3。

b) 伤害的广度包括：

1) 涉及一个人员或设备本身或周围环境的财产；

2) 涉及多个人员或较广环境(例如：影响整个建筑或更大范围)。

如果预计不止一人受伤害或死亡，发生的概率为 F_2。



标引序号说明：

S_1——轻微伤害(正常可逆或短期内可修复)，见 7.2.2；

S_2——高度伤害(正常可逆或长期内可修复)，见 7.2.2；

S_3——严重伤害(正常不可逆或不可修复)或死亡，见 7.2.2；

F_1——极少、较少暴露和/或短时间暴露，见 7.2.3.2；

F_2——频繁、持续暴露和/或长时间暴露，见 7.2.3.2；

P_1——可能避免或限制，见 7.2.3.4；

P_2——不大可能避免或限制，见 7.2.3.4。

图 4 风险预估图

7.2.3 伤害发生的概率

7.2.3.1 通则

风险预估过程中，正常条件和单一故障状态都应考虑。通常不考虑两种独立且不相关故障同时发生的情况，因为此类事件的可能性很低，风险通常处于可容许水平。第一故障引起的第二故障被视为单一故障。当无法自动检测到第一故障时，一定要考虑两种独立且不相关故障发生双重故障的情况。这种情况下，技术委员会也可对绝缘、隔离、组件或防护装置等提出规范、检查或测试要求。

事故数据能用于显示与使用特定类型低压电气设备和/或特定类型防护措施相关的伤害发生概率和严重程度。

伤害发生概率能按 7.2.3.2～7.2.3.4 的规定进行预估。

7.2.3.2 暴露在危险情况

图 4 的 F_1 和 F_2 表示人员、牲畜或财产暴露在危险的情况，危险事件的发生见 7.2.3.3。

人员、牲畜暴露在危险下的评定准则包括以下方面：

a) 需要接近危险区域[例如：正常操作(F_2)、修正故障(通常为 F_1)、维护或维修(通常为 F_1)]；

b) 触及危险区域的情况[例如：手动操作设备(F_2)或自动控制(通常为 F_1)]；

c) 在危险区域暴露的时间；

d) 需要进入危险区域的人员数量；

e) 进入危险区域的频率；

f) 已采取的防护。

7.2.3.3 危险事件的发生

危险事件发生的评定准则包括以下方面：

a) 可靠性和其他统计数据；

b) 事故记录；

c) 健康损害记录；

d) 风险比较(见 8.3)。

注：危险事件的发生可能是技术原因或人为原因。

7.2.3.4 避免或限制伤害的能力

图 4 的 P_1 和 P_2 表示避免或限制伤害的可能性。

避免或限制伤害的评定准则包括以下方面。

a) 操作低压电气设备的人员：

- 技术人员；
- 非技术人员；
- 无人操作。

b) 人员避免或限制伤害的能力(例如：反应动作、敏捷性、逃离的可能性)：

- 可能；
- 特定条件下可能；
- 不可能。

c) 风险意识：

- 通过一般信息；
- 通过直接观察；
- 通过警示标志和指示装置。

d) 实际经验和知识：

- 关于低压电气设备；
- 关于类似低压电气设备；
- 无经验。

e) 危险情况下导致伤害的速度：

- 突然；
- 快速；
- 缓慢。

f) 不同暴露人员对伤害的敏感程度及伤害能够降低的程度。

7.2.4 风险指数

风险指数是风险评价的第一步，可表示从“轻微风险”到“严重风险”的程度。也有助于电气、电子和编程控制系统进行分类。如果需要进一步降低风险（见第 8 章和第 9 章），风险预估结果不能作为最终决策的唯一根据。

风险指数描述了风险等级。风险等级受可预见伤害严重程度和以下因素的影响。

a） 发生伤害的可能性，和

b） 避免伤害的可能性。

注：风险要素和避免伤害的可能性的不同组合会得出同样的风险指数，例如：$S_1/F_2/P_2$ 和 $S_2/F_1/P_1$。

7.3 风险预估中考虑的因素

7.3.1 人员和牲畜的暴露

风险预估应考虑暴露在危险下的所有人员或牲畜。

7.3.2 暴露的类型、频率和持续时间

对考虑中的危险暴露（包括对健康的长期损害）的预估，应分析和考虑低压电气设备的所有操作模式和工作方法。尤其是在设置、教学、改变或修正、清洁、勘障和维护期间会影响到进入危险区域的需要。

风险预估应考虑到有必要暂停安全功能的情况（例如：维护期间）。

7.3.3 积聚效应和协同增效影响

还应考虑暴露在危险下的积聚效应和协同增效影响。风险预估时应尽量基于适当的数据考虑这些影响。

8 风险评价

8.1 一般原则

风险预估后，应通过风险评价判定是否需要风险降低或是否已达到可容许风险。风险大小的第一信息给出了风险指数，见图 4。根据产品类型、风险评价中考虑的因素（见 8.2）和当前社会价值（见 8.2.6），结合风险降低原则（见第 9 章），判断是否需要风险降低。如需要，应选择并实施适当的防护措施，并重复风险评估过程（见图 2），直至每种危险都达到可容许风险。这个重复的过程中，技术委员会检查在应用新的风险降低措时是否引起了附加危险是十分重要的。如果引起了附加危险，应列入危险识别列表。

评价风险时能参考公认的基础安全出版物和多专业共用安全出版物，列表见附录 B。

必要风险降低的实现（见 8.3）和风险比较的良好结果（见 8.4），表明风险已充分降低。

风险评估的一般原则包括：

a） 根据风险预估中考虑的因素（见 7.3）进行风险评价，识别轻度风险和严重风险；

b） 采用“三步骤方法”判定风险降低水平；

c） 对于严重风险采用第 9 章中的风险降低措施。

8.2 风险评价中考虑的因素

8.2.1 人员因素

风险评价应考虑人员因素对风险的影响，包括但不限于：

a) 人员与低压电气设备的互动，包括故障修正；

b) 人员之间的互动；

c) 压力相关的因素；

d) 人类工效影响；

e) 人员在特定情况下感知风险的能力，该能力取决于其经历的培训、经验和自身能力。

对暴露人员能力的评价应考虑下列因素：

——在低压电气设备设计中应用人类工效原则；

——执行要求任务的先天或后天能力；

——对风险的感知；

——在无有意或无意偏离的情况下执行所需任务的信心水平；

——偏离规定和必要安全操作规程的诱因。

培训、经验和能力能影响风险，但它们不应替代在设计、安全防护或补充防护措施阶段实施的消除危险、降低风险的防护措施。

8.2.2 降低风险措施的可靠性

风险评价应考虑部件和系统的可靠性，应包括：

a) 识别能造成伤害的环境(例如：部件故障、电力故障、环境参数、电磁兼容、电气干扰、振动)；

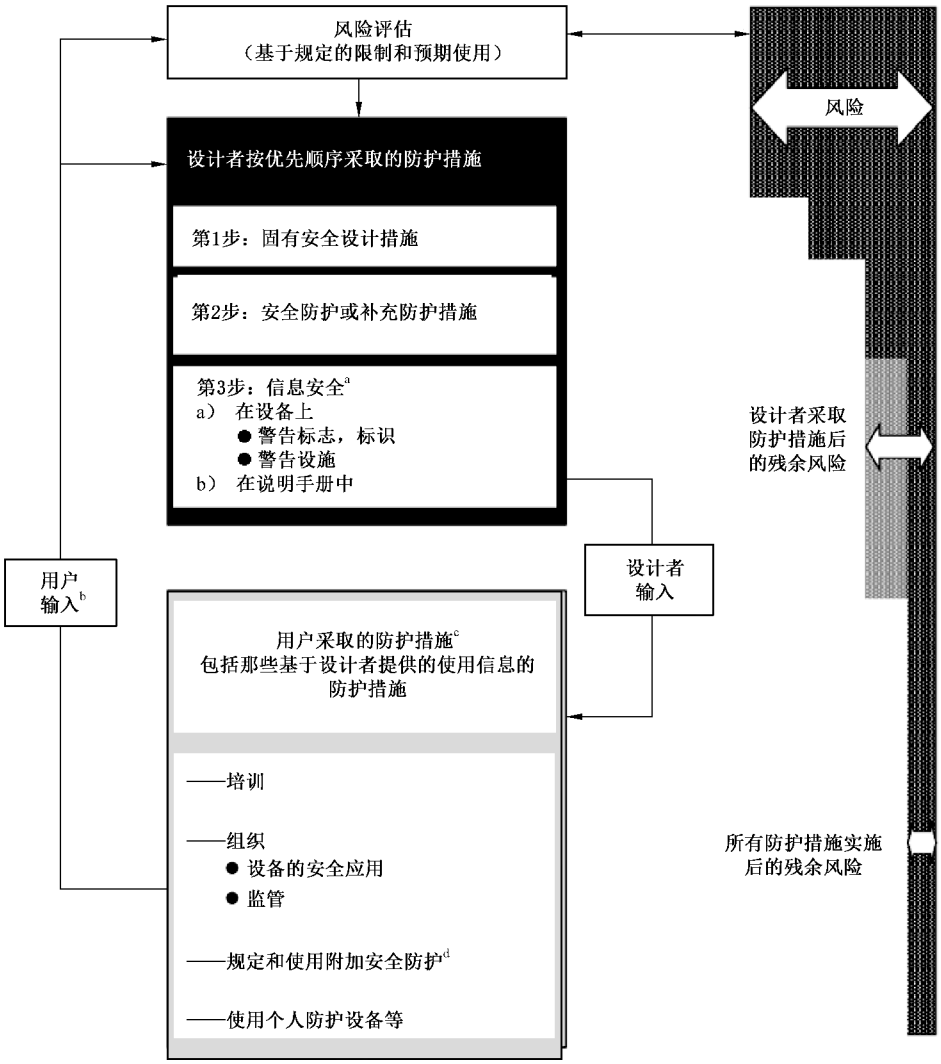
b) 适当情况下，使用定量方法和已验证的使用过程来比较替代的降低风险措施；

c) 提供信息以便选择适当的安全功能、部件和装置。

需要特别注意那些有助于提升安全功能的部件和系统，例如：相关的可靠性、测试、环境条件耐受性。

当不止一个安全相关装置都提供安全功能时，选择这些装置时应考虑可靠性和性能的一致性，例如：必须正确选择传感器、可编程逻辑控制器(PLC)和激励器，以实现特定安全功能。

与技术或培训、工作组织、正确行为、注意事项、使用个人防护设备等相关防护措施相比，设计阶段实施的固有安全设计措施和补充防护措施更为有效。与经验证的技术防护措施相比此类措施(与技术或培训、工作组织、正确行为、注意事项、使用个人防护设备等相关防护措施)的可靠性相对较低，风险评价应做考虑。



[a] 提供适当使用信息是设计者在风险降低过程中工作的一部分，但防护措施只有在用户实施时才会有效。

[b] 用户输入是指，从用户群体收到的低压电气设备预期使用信息，或从具体用户收到的信息。

[c] 用户采取的各种防护措施之间没有任何等级之分。

[d] 由于低压电气设备预期的使用中未预见到的特定过程或设计师无法控制的特定安装条件而需要采取的降低风险措施。

图 5　风险降低过程

8.2.3　防护措施失效的可能性

风险评价应考虑防护措施失效或没起到有效防护的可能性。还应考虑防护措施失效或没起到有效防护的原因，例如：

a）　防护措施影响生产效率，或干扰用户的任何其他活动或习惯；

b）　防护措施难以实施；

c）　涉及操作人员以外的人员；

d）　防护措施不被用户认可，或被认为不适用于其功能；

e）　防止安全措施对安全操作产生不利影响，反之亦然。

防护措施失效的可能性取决于防护措施的类型（例如：可调节防护）及其设计细节。

使用未能恰当设计、控制和监督安全软件的可编程电子系统会增加防护措施失效或没起到有效防护的可能。风险评估应识别低压电气设备中安全相关功能与其他功能关联的情况，并应确定进行评估的程度。当用于诊断或过程校正目的的远程访问时，这一点至关重要。

8.2.4 降低风险措施的维持能力

风险评价应考虑在保证所需防护等级的条件下降低风险措施是否能维持。

注：如果在正确工作状态下降低风险措施无法轻松维持，为了继续使用低压电气设备鼓励不采用或规避使用该降低风险措施。

8.2.5 使用信息

风险评价应考虑使用信息。

注：使用信息的结构和表示见 ISO/IEC 82079-1。

应向用户提供关于产品预期使用的信息，包括设备的所有操作模式。

信息应包括确保低压电气设备安全和正确使用的指导内容。并应告知和警告用户注意残余风险。

使用信息对以描述信息以外的方法使用低压电气设备产生的风险也应进行警告，特别是考虑可合理预见的误使用和相关安全威胁。

使用信息应通过单独或组合方式提供有关运输、组装和安装、试运行、使用(设置、教学/编程或工艺转换、操作、清洁、勘障和维护)以及必要的终止运行、拆解和处置等信息。

8.2.6 当前社会价值

仅当社会对风险的非自愿影响容忍度远低于相同风险的自愿影响容忍度。社会对一些人群提供特殊保护，例如：儿童和残疾人。相关法律和法规也能反映社会需要。也宜考虑被科学证明的事实和实例。社会舆论和观点宜是次要的。

8.3 通过降低风险措施消除危险或降低风险

应依据下面“三步骤方法”(见图 1、图 2 和图 5)的顺序应用用于达到目标的所有降低风险措施。

——固有安全设计措施；

注：这是唯一能消除危险的阶段，从而避免了额外的防护措施，例如安全防护或补充防护措施。

——安全防护或补充防护措施；

——关于残余风险的使用信息(见 8.2.5)。

关于残余风险的使用信息可包括：

a) 设备的正确操作；

b) 推荐操作和相关培训要求；

c) 设备生命周期的残余风险；

d) 个人防护设备的需求和相关培训的要求；

e) 安全相关的安全风险的要求或建议补救措施。

8.4 风险比较

风险评价过程中，低压电气设备的风险能与类似的低压电气设备或类似的产品的风险进行比较，一般原则如下：

——依据公认的国际标准，类似的低压电气设备是安全的；

——产品的预期的使用、设计和构造的方式都是可比的；

——危险和风险要素是可比的；

——技术规范是可比的；

——使用条件是可比的。

使用风险比较方法，也要按照本文件给出的风险评估过程对具体使用条件进行评估（例如：将家用洗碗机与印刷电路板清洗机进行比较时，应评估使用不同材料的风险）。

9 风险降低

风险降低的目标可通过消除危险或单独或同时减少决定风险的两个要素中的某一个来实现：

——考虑中的危险的伤害严重程度；

——发生伤害的可能性。

按优先顺序（见图5）使用“三步骤方法”将表明残余风险已充分降低，以判断低压电气设备在哪个阶段被认为是安全。

a) 危险已经消除或风险已经降低，例如：通过设计或使用危险性较小的替代材料和物质、或依据人类工效原则。

b) 通过应用安全防护或补充防护措施降低了风险，这些措施充分降低了预期的使用风险并适于操作。

c) 如果步骤a)和b)不能充分降低风险，宜给出使用信息，但不应替代步骤a)和b)。使用信息应包括以下对任何残余风险的提示，但不限于：

- 低压电气设备的操作程序与使用该设备的人员能力或其他可能暴露在低压电气设备相关危险下的其他人员能力一致；
- 已充分描述了低压电气设备使用的推荐安全工作规范；
- 已充分告知用户关于低压电气设备生命周期不同阶段的残余风险。

以下原则有助于判断附录D列出的具体危险的残余风险是否可容许。

——是否考虑到固有安全设计措施（见图1）实施的所有可能性。

——如果安全防护或补充防护措施（见图2）一定要实施，是否有包含了相关要求的横向安全标准、多专业共用安全标准、其他IEC标准或其他组织（例如：ISO）开发的国际标准。如果没有，IEC、ISO或其他标准制定组织的适当规范性要求及其他安全出版物可能有帮助。

——如果上述标准中没有可适用的要求，根据第7章和第8章规定的原则起草具体要求。应按照图2的迭代过程和图4的风险指数确定执行，直至风险得到充分降低。

在风险降低程序结束前，应检查下列事项：

——已考虑所有操作条件和所有干预程序；

——采取的措施不会带来其他新的危险；

——已充分告知并警告用户注意残余风险；

——用户的工作条件和低压电气设备的使用能力未受到所采取的降低风险措施的影响；

——采取的降低风险措施相互兼容；

——已充分考虑在非专业/非工业背景下使用专业/工业用途设计的设备所带来的后果。

10 文件

风险评估文件应说明所采取的程序和所实现的结果。文件内容包括（如相关）以下方面。

a) 已评估的低压电气设备（例如：规格、限制、预期的使用）：

- 已做出的任何相关假设条件（例如：负载、压力、安全要素）。

b) 已识别的危险：

- 识别的危险情况；
- 评估中考虑的危险事件。

c) 风险评估所依据的信息(见 4.3)：
- 使用的数据和资源(例如：事故历史情况、类似低压电气设备的风险降低经验)；
- 使用数据相关的不确定性及其对风险评估的影响。

d) 通过降低风险措施实现的目标。

e) 为消除识别危险或降低风险实施的降低风险措施(例如：来自标准或其他规范)。

f) 低压电气设备相关的残余风险。

g) 包括安全方面的最终风险评价结果(见图 2)。

附 录 A
（规范性）
低压电气设备的安全因素

A.1 通则

下列安全因素能视为制定安全出版物的基本要求。这些要求是否与具体产品相关，能通过本文件描述的风险评估过程进行判定。在某些情况下可存在本附录未识别的其他危险。这种情况也应根据本文件确立的风险评估过程采取适当的降低风险措施。

注：本附录依据 IEC Guide 104 附录 A 制定。

A.2 初步观察

技术委员会有义务对负责领域内与设备有关的潜在危险进行识别和评估。技术委员会应在制定文件时考虑以下因素：

——安全整合原则，见 A.3；

——评估 A.4～A.8 列出的危险；

——对信息提出的要求，见 A.9。

A.3 安全整合

电气设备的设计和制造应为人员和财产（如适用）提供充分防护。

应对本附录中列出的设备使用过程中产生的所有危险提出防护，考虑设备的功能性和特殊性，以及由于外部影响对设备本身造成的危险。

本附录中的对危险的评估应考虑到预期的使用和可合理预见的误使用两种情况。

技术委员会所采用的解决方案应符合安全原则，并考虑到广泛认可的技术知识。

在选择最适当的解决方案时，技术委员会应尽量合理地按照给定顺序应用以下原则：

——通过固有安全设计措施消除危险或降低风险；

——对无法通过固有安全设计措施降低的风险，采取必要的降低风险措施；

——将残余风险告知预期用户和其他人（如适用），说明是否需要特殊培训以及是否需要使用个人防护设备。

设备应设计和制造为在正常条件和单一故障状态下可提供充分防护。

单一故障状态下的防护能通过使用双重防护方式（例如：双重绝缘）或足够的安全裕度（例如：加强绝缘）来实现。

A.4 电气危险防护

除非特别允许的功能性原因，设备的可接触导电部分不应带电。

降低风险措施应考虑设备正常使用过程中绝缘可能受到的电气、机械、化学和物理应力。

设备应对电气危险提供充分防护，防止由于以下原因引起的电气危险：

——漏电（例如：绝缘故障）；

——供电；

——累积电荷；

——电弧；

——电击；

——起火。

具体要求见 IEC 61140。

A.5 机械危险防护

如适用,出版物应包括由设备或作用在设备上的预期外力引起的或以下原因引起的机械危险的相应要求:

——不稳定性;

——运行时断电;

——跌落或弹出的物体;

——不合适的表面、边缘或棱角;

——运动部件,包括转速可变的地方;

——振动;

——零件安装不当。

A.6 其他危险防护

A.6.1 概述

如适用,出版物应包括 A.6.2 至 A.6.9 中所涉及的危险的相关要求。

A.6.2 爆炸

爆炸危险能由设备自身引起,例如:由开关设备中的蒸汽金属部分引起,或可能由设备使用或产生的或可能存在于设备使用位置的气体、液体、尘埃、蒸气或其他物质引起。

注:在爆炸性环境中,要关注具体风险评估、危险场所分类和设备防护等级。

A.6.3 电场、磁场和电磁场,其他电离和非电离辐射危险

设备的设计和制造应保证将产生的电场、磁场、电磁场以及其他非电离辐射限制在运行要求范围内,确保设备安全运行。

设备的设计和制造应保证任何电离辐射发射限制在运行要求范围内,不存在对暴露人员的影响,或影响可降至无危险水平。

A.6.4 电场、磁场或电磁场干扰

设备的设计和制造应保证在预期的生命周期内不产生可合理预见的电场、磁场和电磁场干扰。设备的设计应限制磁场和电磁场干扰的发射,避免影响其他设备并产生危险。

A.6.5 光辐射

设备的设计和制造应避免暴露在危险的光辐射(包括 LED、激光、红外线和紫外线辐射等)下。

A.6.6 着火

应规定适当的要求以确保设备内引燃风险和火焰蔓延受到限制。

包括限温装置、限流装置、漏电检测装置、防火外壳、减少火灾蔓延的方法以及选择适当的材料的规定。

注 1:使用阻燃剂可能造成的环境损害宜与通过降低火灾风险所获得的好处相平衡。

注 2:电工产品火灾隐患评估指南的一般原则见 IEC 60695-1-10。

A.6.7 温度

需考虑的两个主要方面如下：

——可接触表面的温度，见 IEC Guide 117；

——温度对材料和组件的影响。

A.6.8 噪声

设备的设计和制造应将噪声尽可能限制在可接受水平。如果噪声达不到可接受水平，制造商的说明书应规定采用外部噪声降低措施（例如：挡板、防护罩或使用个人防护设备）。

A.6.9 生物和化学影响

以下情况能造成危害，应规定避免危害的措施：

a) 微生物因素，如病菌、腐败物，微生物或毒素；例如：细菌、孢子、病毒、酵母和霉菌的浸入或滞留；

b) 化学因素，包括清洁剂或消毒物质，例如：润滑油和清洁液；

c) 从原材料、设备或其他原因带来的外来物，例如：过敏源、有害生物、金属以及设备制造时使用的材料。

A.6.10 排放、生产和/或使用有害物质（例如：气体、液体、尘埃、雾气、蒸汽）

设备的设计和制造应使其产生的危险材料和物质能避免被吸入、摄取、与皮肤、眼睛和粘膜接触或穿透皮肤的风险。当风险不能避免时，应向用户提供适当的警告信息。

A.6.11 无人操作

对于预计在不同使用情况下进行无人操作的设备，应设计和制造为能安全可靠地选择和调整这些使用情况。

A.6.12 连接和断开电源

电源切断后，断开和/或再连接设备不应导致危险情况。尤其是设备不应意外启动，且任何运动部件不应以危险的方式跌落或弹出。

A.6.13 设备组合

如果设备拟与其他设备组合使用，应对每个部件进行设计并提供说明，以便在不产生危险的情况下组装设备。

A.6.14 爆裂

设备应能抵御因负压而引起的爆裂源，且不应以危险的方式排放出气体或其他物质。

A.6.15 卫生条件

设备应以不会引起传染风险的方式进行清洁。

A.6.16 人类工效

设备的设计和制造应符合包括安全移动和操作能力的人类工效原则。

A.7 功能安全和可靠性

A.7.1 概述

对于 IEC 61508 范围内的应用，应符合 IEC Guide 104:2010 中 5.2.5 的要求。

注：功能安全的更多介绍性信息，请查阅 IEC 网站的功能安全板块 http://www.iec.ch/zone/fsafety。文件“功能安全和 IEC 61508”(http://www.iec.ch/about/brochures/pdf/technology/functional_safety.pdf)提供了功能安全的基本介绍。

A.7.2 设备设计

设备的设计和制造应安全可靠，防止危险产生，尤其是：

a) 不会在可预期环境条件下的危险状态下失效，包括与产品电磁兼容标准或通用电磁兼容标准有关的电场、磁场及电磁场干扰环境条件；

b) 能承受可合理预见的误使用；

c) 逻辑性错误(一次只出现一个)不会导致危险；

d) 电源中断或正常波动不会导致危险。

A.7.3 与设备类型相关的危险

一些设备类型可考虑的潜在的危险包括：

a) 意外启动或停止；

b) 与无法停止有关的危险。

A.7.4 系统故障

适用时，安全出版物应规定设备的设计和制造以防止危险的要求，即使在系统失效、或在电源中断和波动期间及之后。

A.8 安全相关的安全风险

以下与安全相关的要求见 IEC 62443。出版物中考虑网络安全的指南见 IEC Guide 120。

——安全风险通常与设备接口有关，例如：HMI、USB、LAN、WLAN 或远程控制操作设备和后续通信层(例如：TCP 端口)。根据第 7 章和图 4 给出的安全风险指数，安全相关的安全风险分析应针对以下类型的安全威胁识别设备的所有潜在安全漏洞：

1) 偶然或巧合的安全违规行为；

2) 使用资源低、一般技能和动机低的简单手段故意进行安全违规行为；

3) 使用适度资源的复杂方法、与所考虑设备相关的特定技能和适度动机的故意进行安全违规行为；

4) 使用拓展资源的复杂方法、与所考虑设备相关的特定技能和高动机的故意进行安全违规行为；

5) 对安全运行有不利影响的安全措施，反之亦然。

技术委员会应将安全相关的安全风险分析结果应用于：

a) 在设计和安装阶段通过配置提供针对给定类型安全威胁的防护措施；

b) 通过风险评估确定保护特定区域免受相关类型安全威胁[上述 1)至 5)]的必要性；

c) 规定系统集成商应如何规定配置区域、系统或组件的要求。

许多安全措施需要系统级管理而不是产品级管理，它们是针对特定安全威胁利用特定安全漏洞的事件的对策。

技术委员会在规定上述 a)至 c)时,宜考虑以下基本安全要求:

——身份验证控制;

——使用控制;

——系统完整性;

——事件的及时响应;

——资源可用性。

注:可能采取的措施包括:

——身份认证和访问控制,以保护系统和数据免受未经授权的访问(可包括技术和组织手段);

——对本地传输或存储的数据进行完整性保护,以检测未经授权的操作。

A.9 信息要求

信息要求包括:

a) 制造商或供应商的名称、品牌名称或商标应清楚地印在电气设备上;或在不可行的情况下印在其包装上。适当情况下还应标明制造的日期和地点;

b) 随设备提供的信息还应包括安全安装(组装)、维护、清洁、操作和贮存的说明;

c) 对于采取所有措施后仍存在的风险,或存在的不明显的潜在风险,应提供适当的警告;

d) 设备上应清楚并不可擦除地标记用于设备安全使用的基本特性、识别信息和需要遵守的规定,以及预期的使用和可合理预见的使用。如果不能做到,记录在随设备提供的说明书中;

e) 通过标记或使用说明书中提供的对设备安全使用的信息至关重要,应便于预期用户的理解。

附 录 B
（资料性）
支撑标准

B.1 基础安全标准

能在以下网址找到制定基础安全标准的技术委员会。
http://www.iec.ch/tctools/horiz_groupsafety.htm

B.2 多专业共用安全出版物

能在以下网址找到制定多专业共用安全标准的技术委员会。
http://www.iec.ch/tctools/horiz_groupsafety.htm

附 录 C
（资料性）
危险、危险情况和危险事件的示例

表 C.1 给出了危险、危险情况和危险事件的示例。

表 C.1 危险、危险情况和危险事件的示例

危险类别	潜在危险源	示例	危险情况	危险事件	可能的伤害或损害
电击及其他电气危险	漏电	连接电线	电线老化部分漏电	接触电线老化部分	电流通过人体
	累积电荷	操作电动机	静电放电火花	火花溅到可燃物上	设备(例如:电机或电子设备)烧坏/人员烧伤
	电弧	通断主电路	提供未经检查的改装装置	绝缘失效导致内部电弧	烧伤、人身伤害、烧伤/其他设备损坏
着火危险	外部火源	火焰蔓延至设备	与其他设备连接的设备着火	火焰蔓延到其他设备	其他设备烧坏/人员烧伤
	内部火源	火焰在设备内部蔓延	设备内部件发热	部件开始起火	其他设备烧坏/人员烧伤
机械危险	不稳定性	配电柜的安装	安装的配电柜不稳	配电柜倒下	人员受伤/财产损坏
	锋利边角	清洁设备	设备存在锋利边角	清洁设备时接触锋利边角	划破手
	振动	使用钻机	人员手持的钻机有强烈振动	由于强烈振动钻机摔落	人员受伤
其他危险	噪声	使用吸尘器	吸尘器发出噪声	儿童长期处于噪声环境下	儿童耳鸣/耳聋
	使用有害物质	气体绝缘开关设备的操作	使用六氟化硫(SF_6)作为气体绝缘开关设备的绝缘介质	SF_6 泄漏	人员中毒
	连接电源	使用插座	使用错误行为将插头插入插座	接触插头的金属触点	电流通过人体
功能错误导致的危险	软件逻辑错误	操作控制设备	控制设备软件逻辑错误	访问有逻辑错误的功能模块	设备控制故障
电场、磁场、和电磁场,其他电离和非电离辐射危险	闪电	操作设备	设备周围出现闪电电磁脉冲	造成设备过电压	设备故障
人类工效	人机界面	读取数据	界面上字样模糊	读错数据	获得错误数据

附 录 D
（资料性）
应用本文件的工具

识别出低压电气设备相关危险，并对相关风险进行预估和评价后，风险评估结果可记录在表 D.1 中。左边一列列出了附录 A 中给出的危险描述。第二栏是技术委员会识别危险的结果，第三栏记录了降低与相关危险相关的风险的解决方案。技术委员会对第三栏的简单验证方法是，例如：参照基础安全标准或多专业共用安全标准或其他标准制定组织（例如：ISO）的相关标准，也可描述标准以外的技术解决方案。

表 D.1 风险评估记录表

要求	是否相关	通过以下方法实现
A.2 初步观察	是	应用附录 A
A.3 安全整合	是	应用标准，尤其是标准中规定的“三步骤方法”： ——固有安全设计措施； ——降低风险措施； ——使用信息
A.4 电气危险防护		
·漏电		
·供电		
·累积电荷		
·开关电弧和电弧故障		
·电击		
·起火		
A.5 机械危险防护		
·不稳定性		
·运行时断电		
·跌落或弹出的物体		
·不合适的表面、边缘或棱角		
·运动部件，尤其是在部件转速可发送变化的情况下		
·振动		
·零件装配不当		
A.6 其他危险防护		
A.6.2 爆炸		
A.6.3 电场、磁场和电磁场，其他电离和非电离辐射危险		
A.6.4 电场、磁场或电磁场干扰		
A.6.5 光辐射		

表 D.1　风险评估记录表（续）

要求	是否相关	通过以下方法实现
A.6.6　着火		
A.6.7　温度		
A.6.8　噪声		
A.6.9　生物和化学影响		
A.6.10　排放、生产和/或使用有害物质(例如:气体、液体、尘埃、雾气、蒸汽)		
A.6.11　无人操作		
A.6.12　连接和断开电源		
A.6.13　设备组合		
A.6.14　爆裂		
A.6.15　卫生条件		
A.6.16　人类工效		
A.7　功能安全和可靠性		
A.7.2　设备设计		
A.7.3　与设备类型相关的危险		
A.7.4　系统故障		
A.8　安全相关的安全风险,规定 a)至 c)时基于 1)至 5)的结果,并考虑基本安全要求		
偶然或巧合的安全违规行为		
使用资源低、一般技能和动机低的简单手段故意进行安全违规行为		
使用适度资源的复杂手段、与所考虑设备相关的特定技能和适度动机的故意进行安全违规行为		
使用拓展资源的复杂手段、与所考虑设备相关的特定技能和高动机的故意进行安全违规行为		
对安全运行有不利影响的安全措施,反之亦然		
A.9　信息要求		

参 考 文 献

[1] ISO 9241-210 Ergonomics of human-system interaction—Part 210:Human-centred design for interactive systems

[2] ISO 10377 Consumer product safety—Guidelines for suppliers

[3] ISO 12100:2010 Safety of machinery—General principles for design—Risk assessment and risk reduction

[4] ISO 17666:2016 Space systems—Risk management

[5] ISO/IEC 82079-1 Preparation of instructions for use—Structuring,content and presentation—Part 1:General principles and detailed requirements

[6] ISO/IEC Guide 50:2014 Safety aspects—Guidelines for child safety in standards and other specifications

[7] ISO/IEC Guide 71 Guide for addressing accessibility in standards

[8] IEC 60050-351:2013 International electrotechnical vocabulary—Part 351:Control technology

[9] IEC 60695-1-10 Fire hazard testing—Part 1-10:Guidance for assessing the fire hazard of electrotechnical products—General guidelines

[10] IEC 61140 Protection against electric shock—Common aspects for installation and equipment

[11] IEC 61508 Series functional safety of electrical/electronic/programmable electronic safety-related systems

[12] IEC 62443 series Security for industrial automation and control IEsystems

[13] IEC Guide 120 Security aspects—Guidelines for their inclusion in publications

[14] IEC TR 61508-0 Functional safety of electrical/electronic/programmable electronic safety-related systems—Part 0:Functional safety and IEC 61508

[15] IEC TR 61641:2014 Enclosed low-voltage switchgear and controlgear assemblies—Guide for testing under conditions of arcing due to internal fault

[16] IEC TS 62443-1-1:2009 Industrial communication networks—Network and system security—Part 1-1:Terminology,concepts and models