

ICS 11.040.01

CCS G 30

YY

中华人民共和国医药行业标准

YY/T 1437—20XX/ISO/TR 24971:2020

代替YY/T 1437—2016

医疗器械 风险管理对医疗器械的应用指南

Medical devices—Guidance on the application of risk management to medical devices

(ISO/TR 24971:2020, Medical devices—Guidance on the application of ISO 14971, IDT)

(征求意见稿)

(本草案完成时间: 2021-08-02)

在提交反馈意见时, 请将您知道的相关专利连同支持性文件一并附上

XXXX - XX - XX 发布

XXXX - XX - XX 实施

国家药品监督管理局 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 风险管理体系通用要求	1
4.1 风险管理过程	1
4.2 管理职责	1
4.3 人员能力	2
4.4 风险管理计划	3
4.5 风险管理文档	4
5 风险分析	5
5.1 风险分析过程	5
5.2 预期用途和可合理预见的误使用	5
5.3 与安全相关的特性的识别	6
5.4 危险和危险情况的识别	6
5.5 风险估计	9
6 风险评价	12
7 风险控制	13
7.1 风险控制方案分析	13
7.2 风险控制措施的实施	15
7.3 剩余风险评价	15
7.4 受益-风险分析	15
7.5 由风险控制措施产生的风险	17
7.6 风险控制的完整性	17
8 综合剩余风险评价	17
8.1 总则	17
8.2 输入和其他考量	18
8.3 可能的方法	18
9 风险管理评审	19
10 生产和生产后活动	19
10.1 总则	19
10.2 信息收集	20
10.3 信息评审	21
10.4 措施	22
附录 A (资料性) 识别危险和与安全相关的特性	23
附录 B (资料性) 支持风险分析的技术	29

附录 C (资料性)	方针、风险可接受性准则、风险控制和风险评价之间的关系.....	33
附录 D (资料性)	安全信息和剩余风险信息	37
附录 E (资料性)	标准在风险管理中的作用	39
附录 F (资料性)	相关信息安全风险指南	43
附录 G (资料性)	未采用 GB/T XXXXX/ISO 14971 设计的组件和器械.....	47
附录 H (资料性)	体外诊断医疗器械指南	49
参考文献.....		67

征求意见稿

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YY/T 1437—2016《医疗器械 YY/T 0316 的应用指南》。与YY/T 1437—2016相比，除结构调整和编辑性改动外，主要技术变化如下：

- 增加了“规范性引用文件”（见第2章）；
- 增加了“术语和定义”（见第3章）；
- 增加了“风险管理体系通用要求”（见第4章）；
- 增加了“风险分析”（见第5章）；
- 增加了“风险评价”（见第6章）；
- 增加了“风险控制”（见第7章）；
- 将“综述”更改为“总则”，并更改了相应的技术内容（见8.1）；将“综合剩余风险评价的输入和其他考虑”更改为“输入和其他考量”，并更改了相应的技术内容（见8.2）；增加了“可能的方法”相关的技术内容（见8.3）；
- 增加了“风险管理评审”（见第9章）；
- 更改了“生产和生产后反馈的回路”，增加了“生产和生产后活动”（见第10章，2016年版的第4章）；
- 增加了“资料性附录A”（见附录A）；
- 增加了“资料性附录B”（见附录B）；
- 更改了“制定用于确定可接受性准则的方针”，并将2016年版的有关内容更改后纳入（见附录C，2016年版的第3章）；
- 更改了“安全信息和剩余风险公示的区别”，并将2016年版的有关内容更改后纳入（见附录D，见2016年版的第5章）；
- 更改了“产品安全标准和过程标准在风险管理中的作用”，并将2016年版的有关内容更改后纳入（见附录E，见2016年版的第2章）；
- 增加了“资料性附录F”（见附录F）；
- 增加了“资料性附录G”（见附录G）；
- 增加了“资料性附录H”（见附录H）。

本文件等同采用ISO/TR 24971:2020《医疗器械 ISO 14971应用指南》。

本文件做了最小限度的编辑性改动：

- 为与现有标准协调，将标准名称改为《医疗器械 风险管理对医疗器械的应用指南》。

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。

本文件由国家药品监督管理局提出。

本文件由全国医疗器械质量管理和通用要求标准化技术委员会（SAC/TC 221）归口。

本文件起草单位：

本文件主要起草人：

本文件及其所代替的文件的历次版本发布情况为：

- YY/T 1437—2016。

引 言

本文件为制造商在开发、实施和保持医疗器械的风险管理过程提供指南，以期满足GB/T XXXXX—20XX/ISO 14971:2019《医疗器械 风险管理对医疗器械的应用》的要求。本文件为GB/T XXXXX—20XX/ISO 14971:2019在各种医疗器械上的应用提供指南。这些医疗器械包括有源的、无源的、植入性的和非植入性的，以及作为医疗器械的软件和体外诊断医疗器械。

本文件中的章和条采用与GB/T XXXXX—20XX/ISO 14971:2019标准相同的结构和条款号，以方便对照标准中适用的要求使用本指南，并在需要处进一步细分子条款。资料性附录包括风险管理具体方面的附加文件。本文件由YY/T 1437—2016的条款和YY/T 0316—2016的资料性附录组成，对以上条款和资料性附录进行融合、结构调整、技术性修订并补充附加指南。

附录H是与国际标准化组织临床实验室检验和体外诊断系统技术委员会(ISO/TC 212)共同合作编写。

本文件描述了制造商能够用于开发、实施和保持符合 GB/T XXXXX—20XX/ISO 14971:2019标准的风险管理过程的方法。如果有能够满足GB/T XXXXX—20XX/ISO 14971:2019的要求的其他方法，亦可采用。

在判定本文件中指南的适用性时，宜考虑医疗器械的性质，即适用范围、如何使用和由谁使用这些医疗器械以及适用的法规要求。

征求意见稿

医疗器械 医疗器械风险管理应用指南

1 范围

本文件依据GB/T XXXXX—20XX/ISO 14971:2019标准，为医疗器械风险管理体系的开发、实施和保持提供指南。

风险管理过程可以是质量管理体系的组成部分，例如某个基于GB/T XXXXX—20XX/ISO 13485:2016^[24]标准的体系，但在GB/T XXXXX—20XX/ISO 14971:2019中并无此要求。GB/T XXXXX—20XX/ISO 13485:2016中一些与风险管理相关的要求（第7章 产品实现和8.2.1监测和测量中的反馈），能通过应用GB/T XXXXX—20XX/ISO 14971:2019来实现。见ISO手册《GB/T XXXXX—20XX/ISO 13485:2016 医疗器械 应用指南》^[25]。

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 XXXXX—20XX 《医疗器械 风险管理对医疗器械的应用》（GB/T XXXXX—20XX/ISO 14971:2019, IDT）

3 术语和定义

GB/T XXXXX—20XX/ISO 14971:2019界定的术语和定义适用于本文件。

注：GB/T XXXXX—20XX/ISO 14971:2019中定义的术语尽可能从ISO/IEC指南63:2019^[20]中获得，该指南专为医疗器械行业开发。

4 风险管理体系通用要求

4.1 风险管理过程

GB/T XXXXX—20XX/ISO 14971:2019 要求制造商在医疗器械的整个生命周期建立、实施、形成文件和保持一个持续的风险管理过程。GB/T XXXXX—20XX/ISO 14971:2019给出了这一过程所要求要素和最高管理者的职责，在本文件中进一步做出了详细解释。

4.2 管理职责

4.2.1 最高管理者承诺

最高管理者有责任建立并保持有效的风险管理过程。重要的是GB/T XXXXX—20XX/ISO 14971:2019强调最高管理者在组织内有权分配职责权限，设定优先事项和提供资源。组织最高管理层的承诺对于风险管理过程的有效是至关重要的。

如果制造商的组织由多个单独的实体组成，如业务单位或部门，最高管理者是指能够指挥和控制这个实体实施风险管理过程的那些人。每个实体可以有自己的风险管理过程（和自己的质量管理体系）。

4.2.2 建立风险可接受性准则的方针

GB/T XXXXX—20XX/ISO 14971:2019要求最高管理者规定用于建立风险可接受性准则的方针并形成文件。附录C提供了关于如何规定此类方针以及宜包括哪些因素的详细指南，例如适用法规、相关标准、公认的最新技术水平和利益相关方的关注。附录C也阐释了此类方针与风险可接受性准则之间的关系，以及在风险控制和风险评价中如何使用这些准则。

方针允许每类医疗器械（或者医疗器械族）采用特定的准则。这取决于医疗器械的特性和预期用途（包括预期患者群体）。GB/T XXXXX—20XX/ISO 14971:2019要求方针为如何建立综合剩余风险的可接受性准则提供指导原则。

4.2.3 风险管理过程的适宜性

GB/T XXXXX—20XX/ISO 14971:2019要求最高管理者按策划的时间间隔评审风险管理过程的适宜性。适宜性的评审是风险管理过程的高层评审并且能够包括下列方面的评审，例如：

- 风险管理程序实施的有效性；
- 风险可接受性准则的充分性，意味着可能需要对特定医疗器械风险可接受性准则进行调整；
- 生产和生产后信息反馈闭环的有效性（见 10.4）。

4.3 人员能力

确保分配有能力的人员是最高管理者的职责。表1中列出了能够参与特定风险管理任务的人员以及支持有效完成有关任务的相关知识和经验的示例。

某些风险管理活动可以由外聘顾问或者专家来执行。宜将所需的能力及满足这些能力的客观证据形成文件。

表1 人员能力及相关知识和经验示例

人员或职能	知识和经验
风险管理负责人	医疗器械风险管理过程
工程师或者科学家	医疗器械技术、设计和工作原理
实施	制造过程
供应链管理	材料和服务的来源，包括外包过程
医疗或者临床专家	临床评价方法学和要求 医疗实践中的应用，包括受益、危险情况和可能的伤害
法规事务	医疗器械拟上市国家/地区的安全和风险管理相关法规要求
质量保证	质量管理体系和质量实践
包装、贮存、处置和流通	包装、贮存、处置和流通相关的危险和风险控制措施
服务工程师、生物医学工程师、或医学物理学家	安装、维护、维修、校准、服务和支持过程相关的危险和风险控制措施和实践
生产后	顾客投诉和不良事件报告，上市后监督
信息服务	数据挖掘过程、文献检索方法
参与评审和批准记录的所有人员	评审和批准相关的职能领域的专门知识或技能

考虑是否需要在风险管理专家的教育中包括下列主题：

- 医疗器械风险管理项目的管理；
- 伦理、安全、信息安全和法律责任；
- 风险、风险可接受性和受益-风险分析的概念；
- 风险管理和可靠性的概率和统计；
- 设计和开发中的风险管理和可靠性；
- 相关标准和法规；
- 风险估计包括确定伤害严重度和发生概率的方法；
- 风险评估的方法学；
- 风险控制的方法；
- 验证风险控制措施有效性的方法；
- 分析生产和生产后信息的方法。

4.4 风险管理计划

4.4.1 总则

风险管理计划描述医疗器械的风险管理活动的范围、参与人员的职责与权限、风险可接受性准则、医疗器械生产和生产后应收集和评审的信息、以及整个产品生命周期内需要实施的风险管理活动。风险管理计划可以是一个独立的文件也可以与其他文件整合在一起，例如，质量管理体系文件。它可以自成一体或者引用其他文件，例如临床策划、生物学评价或可用性评价或者是生产后活动的策划。

风险管理计划是一个“动态文件”，在医疗器械生命周期内当获得新信息时对其进行评审和更新。即使在最后一件医疗器械上市销售后，这些信息宜持续收集。GB/T XXXXX—20XX/ISO 14971:2019要求在风险管理文档中记录风险管理计划的变更。

计划活动的范围和风险管理计划的详细程度宜与医疗器械有关风险水平相适应。GB/T XXXXX—20XX/ISO 14971:2019中的要求是对风险管理计划的最低要求。在计划中制造商可以包括其他事项，如时间表、风险分析工具、或者选择特定风险可接受性准则的理由。

4.4.2 风险管理计划的范围

风险管理计划的范围是识别和描述医疗器械以及计划中的每个要素所适用的生命周期阶段。

风险管理计划的一些要素能够用于产品实现过程（医疗器械的设计、开发和生产），其他要素能够用于生产和生产后阶段（例如医疗器械的安装、使用、维护、最终停用和处置）。

4.4.3 职责和权限分配

风险管理计划识别负责执行与风险管理相关的具体活动的人员或职能（见表1）。此外，风险管理计划识别具有评审和批准风险管理决定和措施的适当权限的人员。这可能需要分配熟悉医疗器械（或医疗器械族）独特的特性及这些特性与安全可能的相关性的人员。这种分配可以包括在计划范围覆盖的特定生命周期阶段和活动所规定的资源分配矩阵中。

4.4.4 风险管理活动评审的要求

风险管理计划详细说明如何完成以及何时完成对特定医疗器械（或者医疗器械族）风险管理活动的评审，包括评审方法、责任人或者职能部门、需要参与评审的人员以及如何管理评审结果。对策划的风险管理活动的评审结果将列入风险管理报告（见第9章）。对风险管理活动的评审要求可能是其他质量体系评审要求的一部分，例如设计和开发评审（见GB/T XXXXX—20XX/ISO 13485:2016^[24]）。

4.4.5 风险可接受性准则

依据制造商确定可接受风险的方针，建立风险可接受性准则。这包括伤害发生概率无法估计时，风险可接受性准则可以只基于伤害严重度。对类似医疗器械（或医疗器械族），其准则可能是通用的。

在启动风险评估之前建立风险可接受性准则是十分重要的。否则，风险评估的结果可能会对建立准则的决定产生影响。

附录C提供了根据方针制定的并在风险评价中应用的准则的进一步指南和示例。

4.4.6 评价综合剩余风险的方法和可接受性准则

评价综合剩余风险的方法及其可接受性准则来自于制造商用于建立风险可接受性准则的方针。GB/T XXXXX—20XX/ISO 14971:2019要求在正在开发的特定医疗器械的风险管理计划中阐述这些方法和准则。第8章列出了针对评价综合剩余风险的一些输入和考虑事项。

4.4.7 验证活动

风险管理计划规定了如何执行GB/T XXXXX—20XX/ISO 14971:2019的7.2要求的两个验证活动。风险管理计划可以明确地详细说明验证活动或者引用其他的计划。

风险控制措施的实施的验证可以是质量管理体系中的设计评审、规范批准、设计和开发验证、或是质量管理体系中的其他验证活动的一部分。

风险控制措施的有效性验证可以是质量管理体系中设计和开发验证的一部分。它可以要求收集临床数据、可用性研究等等，作为质量管理体系中的设计和开发确认的一部分。

4.4.8 与收集和评审生产和生产后信息相关的活动

GB/T XXXXX—20XX/ISO 14971:2019要求制造商建立一个系统用来主动收集和评审关于医疗器械在生产和生产后阶段的信息并且评审这些信息与安全的相关性。因此，重要的是风险管理计划包括建立这一系统所必需的活动。制造商宜理解收集的信息可能是大量的且来自许多不同的来源。所以，宜采用稳健的过程来分析这些信息和识别那些可能未被发现的趋势，以便能够得出适当的结论和采取措施。宜考虑使用统计技术协助处理所收集的数据。

主动收集和评审信息的系统包括监视和接收反馈，例如投诉和不良事件报告。此外，这一系统宜包括主动征求用户的反馈和收集其他相关信息。制造商宜考虑这些活动的范围和程度，并确定哪些活动适合特定的医疗器械。

例如，对于具有长时间使用史、风险很明确的医疗器械，有限的监视可能就足够。对于涉及新的治疗（例如新的预期用途）或者创新技术且可能不太了解其风险的医疗器械，更详细的监视包括上市后临床随访（PMCF）研究，以理解医疗器械实际使用中可能出现的问题。第10章提供了进一步的指南。

收集生产和生产后信息的方法可以是已经建立的质量管理体系过程（例如GB/T XXXXX—20XX/ISO 13485:2016^[24]，8.2）的一部分。在某些情况下，对现有程序的引用是足够的，而对所考虑的医疗器械的任何特定要求都宜在风险管理计划中形成文件。任何监视活动的细节和PMCF研究的细节也宜在风险管理计划中得到规定。

对收集的信息进行评审的频次宜与其风险相适宜，并且可能取决于市场上的该医疗器械的数量、报告的事件数量和报告的伤害严重度。这种收集和评审宜在预期的医疗器械寿命期内持续进行。

4.5 风险管理文档

GB/T XXXXX—20XX/ISO 14971:2019要求制造商建立并保持风险管理文档，包括医疗器械从初始概念到最终停用和处置的整个生命周期内的风险管理活动中创建的记录和其他文件。GB/T XXXXX—

20XX/ISO 14971:2019中的某些条款明确了哪些记录和相关文件作为风险管理文档的一部分进行保持。风险管理文档宜提供医疗器械生命周期内任何阶段风险管理过程评审所需的必要信息。

风险管理文档可以针对每个医疗器械类型或医疗器械族进行构建和组织。在医疗器械整个生命周期内能够及时汇集风险管理记录十分重要, 这些信息可能用来支持整个生命周期内的其他活动和决策, 例如在评审生产和生产后信息时、评价医疗器械更改的影响时或审核时。

风险管理文档是一个逻辑架构, 不必物理地包含所要求的所有记录和相关文件。这些记录和相关文件可以是其他体系(例如制造商的质量管理体系)要求的文档中的一部分。这些记录和相关文件可以以任何形式和媒介存在(硬拷贝、电子记录等)。

GB/T XXXXX—20XX/ISO 14971:2019要求对每种已识别的危险的风险分析、风险评价、风险控制措施的实施和验证, 以及剩余风险评价具有可追溯性。可追溯性是要求证明所有已识别的危险都已在风险管理过程中完全解决。可追溯性工具能为风险管理文档中的每个文件提供索引, 该风险管理文档提供了已识别危险的信息。这种索引有助于对已识别的危险相关的风险知识的管理, 该索引也能用于后续活动如综合剩余风险评价以及生产和生产后信息的评审。可追溯性宜随着新信息的获得和医疗器械更改而更新。

关于未使用 GB/T XXXXX—20XX/ISO 14971:2019设计的医疗器械建立风险管理文档的指南见附录G。

5 风险分析

5.1 风险分析过程

风险分析过程包括以下步骤, 在后面的条款中有更详细的解释:

- 描述医疗器械预期用途和可合理预见的误使用;
- 识别与安全相关的医疗器械的特性;
- 识别与医疗器械有关的危险和危险情况;
- 估计每种危险情况的风险。

5.2 预期用途和可合理预见的误使用

预期用途宜考虑的信息, 例如:

- 预期的医学适应证, 例如治疗或诊断II型糖尿病、心血管疾病、骨折、不孕不育;
- 患者群体, 例如年龄组(成人、儿童、青少年、老人)、性别(男、女)、或疾病状态;
- 与器械交互的身体部位或组织类型, 例如腿或臂;
- 用户特征, 例如患者、非专业人士、医疗保健提供者;
- 使用环境, 例如家庭、医院、重症监护病房;
- 工作原理, 例如机械活塞驱动式注射、X射线成像、MR成像、皮下给药。

可合理预见的误使用是容易预测的人的行为所引起的, 未按制造商预期的方式对产品或系统的使用。它可能与使用错误(例如疏忽、失误、差错)、故意的误用和故意将医疗器械用于制造商非预期的其他(医疗)应用相关。可合理预见的误使用情况可能在设计和开发过程中通过对模拟使用(例如通过应用可用性工程过程)的分析, 或在生产后阶段通过对实际使用的分析进行识别。可合理预见的误使用可能在医疗器械全生命周期内(包括设计活动的迭代)得到识别, 在此期间, 制造商预测潜在误使用的能力逐渐增强。

可用性工程过程能帮助确定某个特定的误使用是否可以合理预见, 例如通过可用性测试期间的观察。可用性测试可能会发现用户未按照制造商说明的方式例行使用医疗器械。发生这种误使用可能是由于不良的工作文化、风险感知不足、对后果的了解有限或由于操作程序不明确。

下面的示例说明了一个应用可用性工程过程识别和分析可合理预见的误使用的实例。更多的关于可用性工程的信息能在IEC 62366-1^[16]和IEC/TR 62366-2^[17]中获得。

示例：一次性使用医疗器械被设计为仅使用一次，但是一些用户可能试图再次使用该医疗器械，这是可合理预见的。因此，在随附文件中包含了请勿重复使用的警告和重复使用造成的可能的伤害的指示。按照 IEC 62366—1^[16]可用性工程的应用证实该安全信息是有效的，即用户将知道正确的使用，并理解医疗器械重复使用的风险。然而，可用性评价还表明一些用户可能忽视该信息而故意重复使用医疗器械。故意重复使用被视为非正常使用，超出了可用性工程过程的范围，因为有关的风险不能在用户接口（见 IEC 62366-2015^[16]，3.1 和 3.26）进行控制。由于该行为可以视为可合理预见的误使用，因此需要按照 GB/T XXXX—20XX/ISO 14971:2019 在风险管理过程中对此类重复使用引起的风险进行分析，并对照风险可接受性准则进行评价。在用户接口之外实施风险控制措施可能是必要的。

5.3 与安全相关的特性的识别

识别可能影响医疗器械安全的特性十分重要。这些特性可以是定性或者定量的并且可能需要设定其界限。附录A中的问题涉及医疗器械的许多方面，能够帮助识别与安全相关的特性。指出关于每一个问题有哪些因素宜进一步详细考虑，从而最终确定与医疗器械有关的所有危险和危险情况。附录A中的问题清单不宜作为核对清单。评审类似医疗器械的可获得的信息和文献，包括不良事件报告，也会有所帮助。

制造商能够确定实现医疗器械的预期用途所必需的性能或功能或可能对安全的影响，并考虑如果任何一个功能不能正常实现时，是否可能会出现任何危险情况。

5.4 危险和危险情况的识别

5.4.1 危险

危险是伤害的潜在来源。根据具体情况，危险可能具有不同的来源和性质。危险的示例是电、运动组件、传染性细菌、化学品、气体、锐边、强电流、温度、电离辐射。

与医疗器械有关的危险能够从5.2确定的预期用途和可合理预见的误使用以及5.3所确定的与安全相关的特性推断出来。GB/T XXXX—20XX/ISO 14971:2019附录C提供了能帮助识别危险和导致危险情况的事件序列的指南。附录H为IVD医疗器械提供了类似的指南，这些器械不正确的诊断信息能够给患者带来间接风险。

5.4.2 危险情况总则

只有在一系列事件发生，形成了危险情况并随后引发或造成伤害时，医疗器械才能导致伤害。事件序列可以包括一系列按时间顺序的原因和结果以及同时发生的事件的组合。当人员、财产或环境暴露在一个或多个危险下时，就会发生危险情况。

危险情况甚至能够来自无故障的情况，即医疗器械在正常条件下按预期使用时。危险情况可能是某些治疗的内在因素，例如，作为正常操作的一部分，体外自动除颤器（AED）向患者施加电击。类似地，伤口灼烧术涉及到在伤口部位施加高能量，以及手术刀有锋利的刀刃用来切割伤口。

附录A以问题的形式提供一个可能影响医疗器械安全特性的指南，这些特性的指南能够帮助识别危险和危险情况。附录B提供了几个能够支持风险分析的技术指南。附录H为体外诊断医疗器械提供了识别危险和危险情况的具体指南。

5.4.3 故障引发的危险情况

在危险情况仅由于故障引起时，发生故障的概率与伤害发生概率是不同的。故障能够引发一系列事件但不一定导致危险情况。危险情况也并不总是引起伤害。

重要的是要理解通常有两种类型的故障能够引起危险情况：随机故障和系统性故障。

5.4.4 随机故障产生的危险情况

随机故障通常是由于物理的或化学的原因引发的，例如腐蚀、污染、热应力和磨损。对于很多随机故障，能够给出故障发生的概率值。以下是随机故障的一些示例：

- 组件失效，如电子组件中集成电路的故障；
- IVD 试剂受到污染引起的不正确结果；
- 医疗器械内或医疗器械上出现传染性或毒性物质；

注：只有在充分了解危险和影响危险情况发生概率的情况下才能够对生物学风险定量估计，例如，无菌保障水平的应用。

5.4.5 系统性故障产生的危险情况

任何活动中的一个错误均能够引起系统性故障。当输入或环境条件的某些特定组合出现时，将系统地引发失效，否则将保持潜伏状态。

导致系统性故障的错误可能发生在医疗器械的任何部分，例如机电医疗器械的硬件和软件中。对任何医疗器械，标记中的系统性故障可能导致使用错误。这些系统性故障可能在医疗器械的开发、生产或维护中的任何时间被引入。以下是系统性故障的一些示例：

- 额定值不正确的熔断器未能阻止危险情况的发生：熔断器额定值可能是设计时规定的不正确；
- 软件数据库未规定满数据库时的状态：如果数据库已满，则软件要做什么不清楚，可能的结果就是系统简单地用新数据替换现有的数据；
- 在医疗器械生产时使用的液体沸点低于体温：在某种情况下，液体的残留物会进入血液，可能导致栓塞；
- 用于肝炎化验的抗体未检测到病毒的一些变体；
- 环境控制设计不当导致毒性物质或传染性介质的污染；
- 编写的用户手册导致如果按照说明执行例行维护，用户可能会受到损伤（例如被尖锐的探针损伤）。

准确估计系统性故障频次是困难的，这主要由于以下原因：

- 系统性故障频次很难测量的。没有大量的相关系统性故障数据或与风险控制相关的参数，要达到合理的置信水平的结果是不可能的。
- 定量估计系统性故障发生概率的方法尚无共识。

由于在这些情形下风险估计是困难的，所以制造商的重点不宜是估计系统性故障的风险，而是实施稳健的系统以防止可能导致危险情况或伤害的系统性故障。

5.4.6 信息安全漏洞引发的危险情况

本文件中的信息安全包括网络安全以及数据和系统信息安全。信息安全漏洞可能导致数据丢失、个人健康信息的泄露、未经授权访问患者记录等。此类情况能够引发最终可能导致伤害（患者损伤或财产损失）的事件序列，示例如下：

- 保密性缺失可能导致个人健康信息泄露；
- 完整性缺失可能导致错误的实验室结果或医疗器械故障；
- 可得性缺失可能妨碍医疗器械关键功能的使用或医疗器械的完全停用。

关于信息安全的进一步指南见附录F。

5.4.7 事件序列或组合

危险情况可能是独立事件序列或组合的结果。图1阐述了危险情况发生的概率 P_1 为各独立事件发生概率的乘积。一个事件序列可以有导致不同危险情况的分支，并且不同事件可能导致相同的危险情况，这些复杂性并未在图1中表示出来。

图1是关于一个电气危险且与医用电气设备内的绝缘导线相关的示例。绝缘材料老化并因裂纹而损坏且裂纹会导致导线裸露的概率很低。下一个可能的事件是用户连接和启动医疗器械，从而（取决于用户界面中的选择）裸露的电线上带有线电压。当用户随后打开外壳时，出现危险情况，即用户暴露在220V的线电压下。此事件序列的组合概率是 P_1 。

用户接触裸露电线的概率被估计为0.10。由于用户总会受到线电压的电击，因此不适的概率是 $P_2=0.10$ 。灼伤的概率较低（0.01），死亡的概率更低（0.001）。

危险情况（HS1）能够导致不同类型的伤害（H1到H3），范围从不适到灼伤甚至死亡。依据伤害的种类，危险情况导致伤害的概率可能是不同的值，这些值在图1中，表述为从 $P_2(HS1)_{H1}$ 到 $P_2(HS1)_{H3}$ 。伤害严重程度会受到暴露环境的影响。例如，根据电压、电流、暴露持续时间和人体位置，电击的后果可能从肌肉收缩到灼伤、心脏颤动或心脏骤停等。

需要强调的是几个场景可能是相互关联的，而不仅仅是伤害最严重或者是伤害发生概率最高的情况需要考虑，其他场景也可能相关。制造商宜考虑记录危险情况的最佳方式，并描述能够导致这种危险情况的一个或多个事件序列以及可能发生的各种不同伤害。

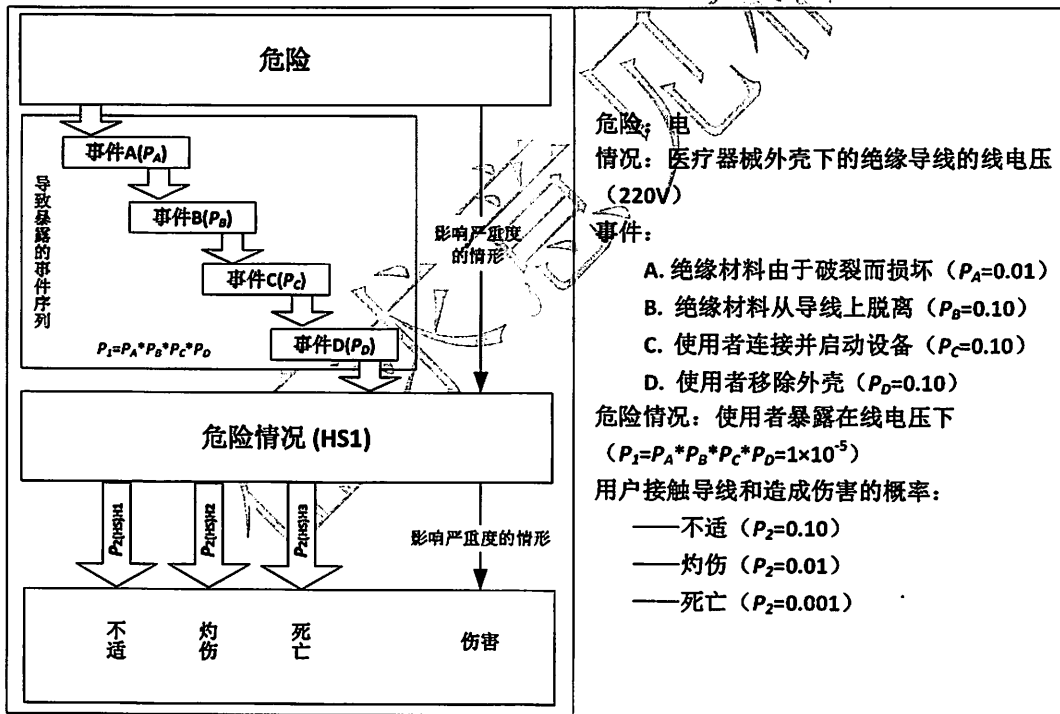


图1 危险、事件序列、危险情况和伤害之间的关系的图示示例

上市的医疗器械的信息能够有助于估计风险。通常采用以下几种方法估计概率：

- 使用历史设计和开发数据；
- 使用分析或模拟技术预测概率；
- 使用实验数据；
- 可靠性估计；
- 生产和生产后信息；

——采用专家判断（专家可以是在适当教育、培训、技能和经验基础上胜任的人，参见 GB/T XXXXX—20XX/ISO 13485^[24]）。

这些方法各有优缺点。为了增加结果的置信度，宜使用互补的方法。专家的判断宜尽可能地作为一个或多个其他方法的补充。当其他方法不能够使用或不充分时，可能有必要仅依赖专家的判断。

5.5 风险估计

5.5.1 总则

GB/T XXXXX—20XX/ISO 14971:2019要求制造商实施风险估计。风险估计可以使用多种方法。这些方法宜检查如下方面，例如：

- 存在危险的情形；
- 导致危险情况的事件序列；
- 危险情况发生的概率；
- 危险情况导致伤害的概率；
- 可能造成的伤害的性质。

风险宜用于决策风险可接受性和风险控制需求的方式表述，例如，使用严重度和概率的分级。为了分析风险，宜对其组成部分即概率和严重度分别进行分析。

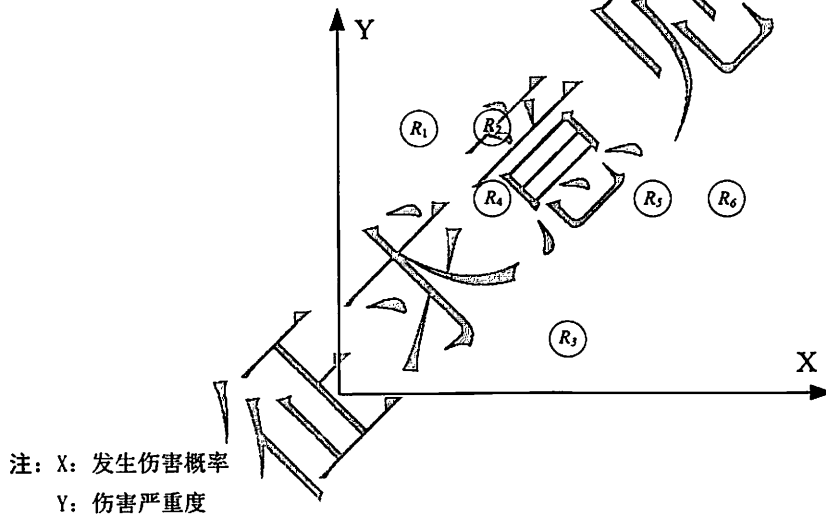


图2 风险图示例说明估计的风险分布

图2中显示的风险图展示了已估计风险的分布情况，这可能对以后的决策非常有用。进行估计时将风险（ $R_1, R_2, R_3 \dots$ ）绘制在图表上。根据此图发展而来的风险矩阵将用于本条款中的所有示例，这并不意味着该方法对医疗器械具有普遍适用性，但在很多情况下该方法可能是有用的。如果一个风险图表或风险矩阵用于风险评级，则宜证明特定的风险图或风险矩阵以及使用的解释适用于该应用程序。

5.5.2 概率

当有充足的数据可用以足够的置信度估计伤害发生的概率时，宜采用定量方法。否则，与具有高度不确定性的定量估计相比，基于专家判断的定性的方法更好。这种情况的一个示例是一个新的医疗器械在设计确认或生产后的数据得到之前，无法获得合适的定量数据。对于定性方法，制造商能采用适合于医疗器械的描述方法来描述一系列概率水平。

虽然概率是一个连续的变量，但是在实践中可以使用若干离散的层级以简化分析。制造商根据估计值的预期置信度决定多少概率层级是合适的。当以更大的置信度估计时，可以使用更多的概率层级。为了便于决策，宜至少确定三个层级。这些层级是描述性的和定性的（如预期的医疗器械寿命期内不发生、可能偶尔发生、可能经常发生等），层级也可以是定量的。制造商宜明确地定义层级，以便每个层级内的内容不会混淆。一个特别地有效的方法是给离散的层级分配非重叠的数字值范围。表3给出了三级定性概率的示例，表5给出了五级半定量概率层级的示例。

对于不同产品族，概率范围的定义可能相同或者不同。例如，制造商能够对X—射线设备选择使用一组概率范围，但对一次性无菌敷料使用另一组概率范围。概率划分尺度能够包括每次使用、每个器械、每小时使用，或者在一定人群中造成伤害的概率等。

对特定的医疗器械，要求将选择的概率水平或范围及其描述方法在风险管理文档中形成文件（见GB/T XXXXX—20XX/ISO 14971:2019, 5.5）。

估计伤害发生的概率有几个重要的因素，包括但不限于下列因素：

- 特定医疗器械使用批次如何？
- 医疗器械的寿命期是多少？
- 用户和患者群体的组成？
- 用户/患者的数量是多少？
- 用户/患者暴露时间和暴露在什么环境条件下？

概率估计涉及从初始事件的发生到伤害发生的情形和事件序列。伤害发生的概率 P 能分解为危险情况发生（即，人暴露于危险中）的概率 P_1 和危险情况导致伤害的概率 P_2 。见GB/T XXXXX—20XX/ISO 14971:2019中图C.1。将其分解为 P_1 和 P_2 能够有助于估计伤害发生的概率 P ，但是这种分解并非强制。

当伤害发生概率被分解为 P_1 和 P_2 时，可能会出现其中一个能够被估计，而另一个不能够估计的情况。这种情况下，可以采取保守方法，将未知的概率设置等于1。当估计的概率非常低以致所产生的风险变得不显著或者可以忽略不计，或者估计的概率非常高以至于引发的风险显然宜被降低时，这种方法可能是有用的。

5.5.3 不能估计概率的风险

当对伤害发生概率的定量估计是基于准确且可靠的数据，或者合理的定性估计是基于有资质的专家的一致意见时，则可以提升风险估计的置信度。然而，这并不总是可以实现的。例如，系统性故障的概率，如在5.4.5中所讨论的那些，是很难进行估计的。当对概率估计的准确性存在疑问时，通常有必要建立一个较宽的概率范围，或确定一个不比某些特定值更差的估值。

概率难以估计的示例包括：

- 软件失效；
- 特殊的误使用情况，如对医疗器械蓄意破坏或篡改；
- 知之甚少的新风险，如对牛海绵状脑病（BSE）病原体的传染性认识不准确，妨碍了对其传播风险的量化；
- 某些毒理学危险，如遗传毒性致癌物和致敏剂，可能无法确定不发生毒性影响的接触阈值的情况。

当伤害发生的概率不能够估计时，有必要仅根据伤害严重度来评价风险。风险控制措施宜侧重于全面防止所有危险情况或防止危险情况导致的伤害发生。如果这是不可能的，风险控制措施宜侧重于降低伤害严重度。

可以推定在设计、开发、生产和维护中所采用的过程的严格程度与某些系统性故障被引入的或未被发现的概率之间存在反向相关。这些过程所需的严格程度能通过考虑系统性故障的后果的严重度和医疗器械外部风险控制措施的有效性来确定。后果越严重并外部风险控制措施有效性越低，过程宜越严格。

5.5.4 严重度

为了进行潜在伤害严重度的分类，制造商宜使用适用于医疗器械的描述方法。严重度实际上是连续的，然而在实践中使用非连续的严重度分级以简化分析。在这种情况下，制造商要决定分成几级是适当的和如何定义。这些层级宜是描述式的且不宜包括任何概率的要素。见表2和表4中的示例。

对特定的医疗器械，制造商需要基于其可能造成的伤害来选择并说明严重度层级。宜采用充分的特异性来定义严重度，以便为风险分析中确定的每个危险分配正确的严重度级别。

对特定的医疗器械，要求将选择的严重度水平或范围及其描述方法在风险管理文档中形成文件（见GB/T XXXXX—20XX/ISO 14971:2019, 5.5）。

注：监管机构使用的术语可用于描述伤害严重度。

5.5.5 示例

可以使用多种方法进行定性分析。一个典型的方法是使用 $N \times M$ 矩阵来描述与每一危险情况有关的伤害严重度和发生概率。审慎地将概率定义为 N 级，严重度为 M 级。矩阵的每个单元代表可能风险全集的一个子集。

一个简单的示例是：使用表2三个严重度层级作为列，表3的三个定性概率层级作为行，构建一个 3×3 风险矩阵。将估计的风险（ R_1, R_2, R_3, \dots ）填入到适当的单元内，结果如图3所示。制造商宜根据需要使这些定义适合于特定的医疗器械并明确化，以确保其可重复地使用。

表2 三级定性严重度示例

通用术语	可能的描述
严重的	死亡或功能或结构丧失
中等的	可逆的损伤或轻伤
可忽略的	无损伤或轻微受伤

表3 三级定性概率示例

通用术语	可能的描述
高	很可能发生，经常，频繁，总是 医疗器械寿命期内很可能多次发生
中	可能发生，但不频繁 医疗器械寿命期内很可能发生几次
低	不太可能发生，罕见，极少 医疗器械寿命期内不太可能发生

		定性严重度层级		
		可忽略的	中度的	严重的
定性概率层级	高	R_1	R_2	
	中		R_4	R_5, R_6
	低		R_3	

注：图3中估计的风险与图2中描述的不相同。

图3 定性 3×3 风险矩阵示例

一个复杂的示例是：使用表4中五个严重度层级作为列，表5的五个半定性概率层级作为行，构建一个5×5风险矩阵。将估计的风险 (R_1, R_2, R_3, \dots) 填入到适当的单元内，结果如图4所示。

表4 五级定性严重度层级示例

通用术语	可能的描述
灾难性的/致命的	导致死亡
危重的	导致永久缺陷或不可逆损伤
严重的/重大的	导致需要医疗或外科手术干预的损伤或缺陷
轻度的	导致不需要医疗或外科手术干预的暂时的损伤或缺陷
可忽略的	导致不便或暂时性不适

表5 半定量概率层级示例

通用术语	概率范围示例
经常	$\geq 10^{-3}$
有时	$< 10^{-3}$ 和 $\geq 10^{-4}$
偶然	$< 10^{-4}$ 和 $\geq 10^{-5}$
很少	$< 10^{-5}$ 和 $\geq 10^{-6}$
非常少	$< 10^{-6}$

		定性严重度层级				
		可忽略的	轻度的	严重的/重大的	危重的	灾难性的/致命的
半 定 量 概 率 层 级	经常					
	有时	R_1	R_2			
	偶然		R_4		R_5	R_6
	很少					
	非常少			R_3		

图4 半定量 5×5 风险矩阵示例

除了3×3或5×5以外，也能采用其他矩阵；然而，多于五个层级的矩阵可能需要更多的数据，以便能够区分各个层级和避免层级交叉。选择矩阵的理由及其结果得分宜形成文件。需要指出，对于作出适当的决策，三个层级的矩阵可能并不总是足够准确。虽然上面的示例是3×3和5×5，但不要求矩阵是均衡的。例如，4×5矩阵可能适用于一个给定的应用。

6 风险评价

GB/T XXXXX—20XX/ISO 14971:2019描述了风险评价的过程。但该文件未规定可接受的风险水平。风险可接受性准则是基于制造商用于确定可接受风险的方针，并且在风险管理计划中形成文件。

在风险评价中，制造商将估计的风险与可接受性准则进行比较并确定这些准则是否得到满足。关于风险评价中应用风险可接受性准则的进一步的指南和示例见附录C。

7 风险控制

7.1 风险控制方案分析

7.1.1 医疗器械设计中的风险控制

降低与医疗器械有关的风险有多种方案。这些方案能单独使用或组合使用。制造商能够探究不同的选择，以合理可行的方式将风险降低到可接受水平。正如GB/T XXXXX—20XX/ISO 14971:2019中所强调的，方案的优先顺序很重要。下面将对此进行解释，并通过一些示例加以说明。

a) 使医疗器械设计和制造过程是固有安全的，通过：

——消除特定的危险；

示例1：设计圆滑边缘的表面以消除可能造成损伤的锋利边缘这一危险。使用手动操作泵替代电动泵以消除电击危险。

——降低伤害发生概率；

示例2：通过没有可触及的带电组件以降低电击造成心颤伤害的概率。通过身份管理以降低未经授权访问数据的概率。通过采用洁净室技术或灭菌以降低微生物污染引起生物学反应的概率。

——降低伤害严重度；

示例3：通过使用小功率电机和低速以降低运动组件挤压造成的伤害严重度。通过使用低电压（低于 42 V）以降低电击伤害严重度。

b) 通过采取防护措施：

——防止危险情况发生；

示例4：采用自动切断或过压阀，电线和电源装置（带盖插头、插座和连接器）的防护罩。运动组件的防护装置或防止患者从台上或床上跌落的保护装置。生活中通过检测以检出不合格品。

——防止危险情况导致伤害；

示例5：采用视觉或听觉报警向用户警示危险情况。

c) 提供安全信息，通过：

——在医疗器械上给出警告；

示例6：警告：失效日期后禁止使用。

——在随附文件中包括禁忌症；

示例7：新生儿禁用。

——提供说明以支持正确使用和避免使用错误；

示例8：在大腿外侧的中部（大腿）使用肾上腺素注射器，必要时穿透衣服。禁止向静脉、臀部、手指、脚趾、手或脚注射。在注射前及注射过程中，将幼童的腿完全固定在适当位置，以免受伤。

——提供使用个人防护设备的说明；

示例9：在处理有毒或者有害物质时使用手套和护目镜。

——提供降低伤害严重度的措施说明；

示例10：沾染有毒物质后请立即用清水冲洗。

——对用户如何正确使用医疗器械的培训；

示例11：用于放射治疗设备或家用透析机的操作者的培训方案。

——提供医疗器械寿命期内安装和维护的说明。

示例12：维护的时间间隔、最长预期寿命期、妥善处置医疗器械的方式。

方案 a) 到 c) 按其降低风险普遍公认的有效性优先级别降序列出。制造商宜在决定最适当的风险控制措施（组合）之前考虑这个顺序。

表6给出了不同种类医疗器械的特定风险控制措施示例，附录D给出了更多关于提供安全信息的指南。

表6 风险控制措施示例

医疗器械	危险	危险情况	固有安全设计	防护措施	安全信息
注射器（一次性使用）	生物污染	在首次使用后再用于其他患者	使用后自毁	首次使用的明显指示	对于再次使用的警告
植入性起搏器	功能丧失	由于电池的过早耗尽而使起搏器停止工作	可靠的长寿命电池	电池耗尽前报警	典型的电池寿命信息
机械式患者呼吸机	气压	软件失效引起的患者气道过压	风机不能输送高压气	呼吸机或呼吸软管上的超压阀	只使用制造商提供的呼吸软管的说明
IVD血液分析仪	系统性误差或偏差	向临床医生报告的不正确结果	自校	提供计量上可溯源的校准品	用正确度质控品验证校准的说明
X射线设备	电离辐射	员工暴露于杂散辐射	不可行（杂散辐射始终存在）	铅屏蔽和铅围裙	所占/辐射区域的辐射水平的信息

在这一步骤中能够研究固有安全设计和防护措施的可能方案的优缺点。方案的选择宜基于这些研究。在此过程中能够创造出许多可能的方案和相关风险的知识。制造商宜考虑如何保留这些知识，以备将来使用。

7.1.2 制造过程的风险控制

制造过程中的偏离或错误能够损害医疗器械的安全，例如：

- 引入有害残留物或微粒；
- 影响关键物理或化学性能，如表面涂层、拉伸强度、抗老化性能、均匀性等；
- 超出临界公差；
- 过程控制不充分，导致呼吸器组装过程中气体管路混淆；
- 削弱组件焊接、粘合和连接的完整性。

固有安全的制造消除由制造过程带来的特定危险从而确保医疗器械中不存在此危险。制造过程中的防护措施，例如检查和/或测试能发现不符合并能防止受影响的医疗器械的流通。

某些技术如失效模式和效应分析(FMEA, 见附录B. 5)以及危险分析和关键控制点(HACCP, 见附录B. 7)能有助于分析制造过程和流通过程中的关键步骤。重要的是还需要考虑对下列方面的风险控制：

- 外包过程，例如采购的产品、组件和服务；
- 医疗器械生命周期的其他阶段，例如医疗器械的贮存、流通、安装、服务、最终停用和处置。

7.1.3 标准和风险控制

通常，标准可以被认为代表了普遍公认的最新技术水平。通过应用标准，制造商能够简化剩余风险的分析工作，但需要强调的是标准可能未阐述与医疗器械有关的全部风险。

许多标准提出了医疗器械的固有安全、防护措施和安全信息。当有相关标准时，标准可能阐述关于特定医疗器械的部分或全部的风险。在没有相反的客观的证据情况下，制造商可以假定符合相关标准的要求即特定的风险降低到了可接受水平。关于使用标准的进一步指南见附录E。

7.2 风险控制措施的实施

GB/T XXXXX—20XX/ISO 14971:2019要求实施风险控制措施，验证风险控制措施的实施及验证其有效性。风险管理计划规定这两种不同的验证活动如何进行。

风险控制措施的实施验证能够从设计文档中获得。风险控制措施的有效性验证可能需要对单个风险控制措施进行测试或者测试医疗器械。验证的要求适用于所有风险控制措施，包括安全信息。用户测试能够提供支持有效性验证的有用信息，例如可用性测试（见IEC 62366-1^[16]）、临床试验调查（见ISO 14155^[26]）或者体外诊断医疗器械的临床性能研究（见ISO 20916^[37]）。附录E提供了关于在风险管理中使用标准的更多的指南。

制造过程中的风险控制措施的实施验证可以通过检查过程规范完成。制造过程中的风险控制措施有效性的验证可以通过制造过程的鉴定来完成，例如过程确认、检查方法的鉴定或者其他适当的方法。

风险管理计划能够通过明确描述或引用其他的验证活动的计划详细说明验证活动。

7.3 剩余风险评价

剩余风险采用与初始风险相同的方法和相同的风险可接受性准则进行评价。剩余风险是可接受的或不可接受的。当不可接受时，宜研究进一步的风险控制方案。当进一步的风险控制不可行时，可进行受益-风险分析。当生产和生产后信息表明风险或其可接受性可能发生变化时，在医疗器械的生命周期内可能重复进行剩余风险评价。

7.4 受益-风险分析

7.4.1 总则

对使用风险管理计划中建立的准则判定为不可接受且进一步风险控制不可行的那些风险，GB/T XXXXX—20XX/ISO 14971:2019允许制造商进行受益-风险分析。受益-风险分析用于确定剩余风险是否超过医疗器械预期用途的预期受益。

受益-风险分析不能用于权衡剩余风险与商业利益或经济利益（即商业决策）。（见GB/T XXXXX—20XX/ISO 14971:2019, A.2.7.4）。

在考虑受益之前宜考虑进一步降低风险的可行性（见附录C）。关于受益是否超过风险的决定，原则上由有经验的和有知识的人作出。这些人通常是由医学、临床或应用专家组成的多学科团队。一个重要考虑因素是，是否可以通过使用无该风险或风险较小的替代解决方案来达到预期受益。这包括将制造商设计的医疗器械的剩余风险与类似医疗器械的剩余风险进行比较。

7.4.2 受益估计

医疗器械产生的受益与使用医疗器械预期改善健康的可能性和程度相关。受益可以描述为对临床结果、患者的生活质量、与诊断相关的结果的正面影响、诊断器械对临床结果的正面影响、或对公共健康的正面影响。受益的性质和程度可能取决于患者群体。

受益有时可能用产生正面影响的程度来描述，例如体验受益的患者的比例以及受益的持续时间。

可以通过了解以下几个因素来估计受益，例如：

- 临床使用期间的预期性能；
- 上述性能带来的预期临床结果；

- 使用类似医疗器械产生的受益；
- 与其他诊断或治疗方案的风险和受益相关的因素。

受益估计的置信度很大程度上取决于阐述这些因素的信息的可靠性，这包括认识到很可能有一系列可能的结果，还可能要考虑的其他因素，如下：

- 比较不同的结果可能是困难的，例如：疼痛与丧失活动能力哪一个更糟糕？不同结果可能由与初始问题完全不同的副作用导致。
- 考虑不稳定的结果是困难的。这些结果可能是由恢复时间和长期效应引起的。

由于应用严谨的方法是困难的，通常有必要做出简单化的假设。因此将重点放在每一方案最可能的结果以及最有利或最不利的结果，通常证明是得当的。

宜考虑以下方面：

- 对患者或其他人预期受益的类型（例如，医疗器械是挽救生命的或在给定的医疗场景下是必要的）；
- 预期受益的程度（例如，患者经历的治疗或诊断的受益的程度）；
- 患者经历的预期受益的概率（即，在治疗或诊断患者疾病或症状方面，医疗器械有效的可能性）；
- 预期效果的持续时间（即对患者的预期受益持续多久）。

在设计过程的不同阶段，受益的估计可能发生显著变化。如果可以获得可靠的临床数据证明医疗器械稳定的性能和有效性，就能够有信心地进行受益估计。在临床数据数量或质量有限的情况下，从获得的任何相关信息中估计的受益都具有较大的不确定性。例如，有时有必要在过程的早期，从预期健康改善的程度和达到预期性能的可能性去估计受益。

当存在重大风险并且受益估计具有高度不确定性时，有必要通过模拟研究或临床调查来验证预期的性能或有效性。这对于确认受益-风险是否符合预期，以及防止患者不必要地暴露于巨大的剩余风险之中是至关重要的。ISO 14155^[26]规定了医疗器械临床研究程序，ISO 20916^[37]规定了体外诊断医疗器械的临床性能研究程序。

7.4.3 受益-风险分析准则

受益-风险判定所涉及的人员有责任理解和考虑风险管理决定的背景，包括技术的、法规的、经济的和背景。这包括对适用的法规或标准中的基本要求的解释，因为它们适用于在预期的使用条件下所考虑的医疗器械。由于这类分析具备高度的产品特异性，不可能有进一步的通用的指南。但是，可以假定阐述特定产品或风险的标准所规定的安全要求与可接受的风险水平是一致的，特别是在使用那些被现行的法规体系认可的标准时。需要指出，可能需要临床调查以验证受益和剩余风险的平衡是可接受的。

7.4.4 受益-风险比较

直接比较受益和风险是复杂的，宜考虑以下内容：

- 疾病的特性或预期患者的状况；
- 数据的不确定性。起初，对危险和所考虑的医疗器械进行文献检索能深入了解受益和风险之间的平衡；
- 市场上可获得的类似医疗器械的生产和生产后信息；
- 普遍公认的最新技术水平；
- 开发中的医疗器械的受益与市场上可获得的类似医疗器械的受益的比较；
- 开发中的医疗器械的剩余风险与市场上可获得的类似医疗器械的剩余风险的比较。

GB/T XXXX—20XX/ISO 14971:2019要求制造商在风险管理文档中记录受益-风险分析的结果。建议包括如何得出结论的理由说明。

7.4.5 受益-风险分析示例

以下为受益-风险分析的示例:

示例1: 当高频外科手术器械的回流电极不适当地接触患者时可能发生灼伤。虽然符合相关的产品标准将此种灼伤的概率最小化, 但仍可能发生。然而, 使用高频外科手术器械的受益超过灼伤的剩余风险。

示例2: 虽然已知 X 射线对患者有潜在伤害, 传统诊断成像的临床有效性几乎总是证明其使用是合理的。然而, 辐射对患者造成的不良的影响是不可忽视的。有标准用于尽量减少对患者的辐射照射。当开发了电离辐射新应用且现有标准不适用时, 制造商验证受益-风险分析的结果至少与替代医疗器械和治疗的结果同样有利。

示例3: 一些耳蜗植入性组件, 例如带有电极阵列的植入性接收模拟器, 一旦植入, 就不容易更换。其预期终生植入, 并要求可靠运行数年甚至数十年(这对于年轻人或儿童来说是尤其重要的考虑因素)。对于这些组件的特定的失效机理可进行可靠性加速试验。然而, 确认那些要延续几十年的组件的可靠性是不可行的。因此, 将器械失效的剩余风险与潜在听力改善带来的受益进行权衡。对于那些可靠性不能确认的组件, 剩余风险依赖于所估计的组件可靠性和可靠性估计的置信度。有时剩余风险超过受益, 有时受益超过风险。

7.5 由风险控制措施产生的风险

为降低某一风险而实施的风险控制措施可能会引入新的风险或增大其他风险, 包括那些之前评价为可接受的风险。例如, 消除用户接口中与某一使用相关的风险能够限制用户使用医疗器械的灵活性, 并限制其干预危险情况的能力。又一个示例是为控制某一特定风险的软件变更, 其无意中破坏了嵌入在软件架构中的另一风险控制措施。制造商宜评审这些影响, 以确保这些风险仍可接受。

实施此评审的一种方式更新医疗器械的风险分析, 包括所有的风险控制措施, 并识别是否引入新的风险或增大现有的风险。对于制造过程的风险控制措施, 制造商可以将对其的评审作为过程风险分析或过程确认的一部分。

7.6 风险控制的完整性

GB/T XXXXX—20XX/ISO 14971:2019要求所有所识别的危险情况产生的风险已经得到考虑, 并所有的风险控制活动已经完成。这能通过保持所有危险和危险情况以及有关风险的清单来实现。可检查该清单确保所有所识别的危险情况已经得到考虑且没有忽略任何风险。这一活动的结果在风险管理文档中形成文件。

8 综合剩余风险评价

8.1 总则

GB/T XXXXX—20XX/ISO 14971:2019要求与医疗器械预期用途的受益相比较, 评价综合剩余风险, 并要求在风险管理计划中包括综合剩余风险的可接受性准则和综合剩余风险的评价方法。

对综合剩余风险的评价是从宽泛的视角评审剩余风险。所有已识别的危险情况已被评价, 并且所有风险均已降至可接受水平或基于受益-风险分析已被接受。此时, 制造商考虑与医疗器械有关的综合剩余风险作为整体是否满足综合剩余风险可接受性准则, 此考虑将所有剩余风险的贡献一并考虑并与医疗器械预期用途的受益相比较。这一步对于复杂的医疗器械和存在大量单个风险的医疗器械特别重要。这种评价能得出医疗器械安全的结论。

综合剩余风险的评价是一项具有挑战性的工作, 它不能够通过将所有的单个风险进行数字相加来实现。困难产生的原因如下:

——每种伤害发生概率与不同严重度的不同伤害相关, 并且可能与不同的危险情况相关。

- 通常认为概率具有不同程度的不确定性。一些来自历史数据或者测试得到的概率可能很精确。另一些概率可能不精确，例如通过专家的判断的估计的；或者不能估计，例如软件失效的概率。
- 不可能对风险分析中通常采用的宽泛的各种类别的单个伤害严重度进行组合。

此外，综合剩余风险可接受性准则可能与单个风险的可接受准则不同。用于评价单个风险的准则通常包括对具有特定严重度的伤害发生概率的限制。用于评价综合剩余风险的准则经常基于一些附加要素，例如医疗器械预期用途的受益。

尚无评价综合剩余风险的最佳方法。制造商负责选择适宜的方法。在下列子条款中介绍了一些适当的方法示例能够用来定义评价方法。本文件旨在帮助制造商建立方法和准则。

GB/T XXXXX—20XX/ISO 14971:2019要求综合剩余风险的评价宜由具备知识、经验和权限的人员来进行。建议具备医疗器械使用知识和经验的应用专家参与。最终，这些评价宜基于对应用知识和临床专业知识具有重要作用的专家的判断。

综合剩余风险评价的结果构成风险管理文档的一部分。建议对接受综合剩余风险的理由说明形成文件。

GB/T XXXXX—20XX/ISO 14971:2019要求制造商告知用户重大剩余风险，并在随附文件中提供必要信息以公开这些剩余风险。公开剩余风险的指南请见附录D。

8.2 输入和其他考量

综合剩余风险的评价能够考虑若干输入和考量。下面是一些输入及其使用的示例。

- a) 不同的事件序列能够导致不同的危险情况和风险，每一危险情况和风险都对综合剩余风险有贡献。例如，一次性使用医疗器械的重复使用可能关系到感染、有毒物质的析出、老化引起的机械故障和生物不相容的消毒剂残留。事件树分析（ETA，见附录 B.4）可以是分析这些风险的适宜方法，以区别具有很大的和可忽略的伤害发生概率或严重度的事件序列。在综合剩余风险的评价中考虑这些风险组合的贡献。
- b) 一个特定的伤害可能来自于不同的危险情况。在这种情况下，基于单个概率的组合，该伤害发生概率能用于确定综合剩余风险。故障树分析（FTA，见附录 B.3）可以是估计这一特定伤害发生的综合概率适宜方法。
- c) 适用于独立单个风险的风险控制措施可能引起矛盾的要求，从而增加综合剩余风险。例如，阐述无意识患者从患者检查床上跌落的说明可能是“不要留下无意识患者无人看护”，这可能与“拍摄 X-射线图像时请站在保护屏之后”的预期保护医护人员免受 X-射线照射的说明相冲突。
- d) 单独考虑某个警告可能使单个风险适当地降低。然而，过多的警告可能使医疗器械用户困惑，从而可能降低单个警告的效果。可能需要分析以确定是否过度地依赖警告和是否这种过度的依赖可能影响风险的降低和综合剩余风险。
- e) 对医疗器械的所有操作说明的全面评审可能会发现说明不一致或难以遵守，这也可能影响综合剩余风险。
- f) 设计确认、可用性研究、临床评价和临床研究的结果能提供关于综合剩余风险的有用信息，来自利益相关方的适当的输入也能提供有用的信息。
- g) 宜考虑所有的单个风险的受益-风险分析。
- h) 在某些情况下，允许稍微增大一个风险以降低另一个风险。例如，允许增大一个人（用户）的风险从而降低另一个人（患者）的风险。这种评价可以采用检查相关重大风险的形式，说明这种权衡取舍的理由和取舍决定中组合的风险水平可接受的理由。

8.3 可能的方法

评价综合剩余风险的方法可以包括下列方法或制造商认为适当的其他方法：

- a) 权衡与医疗器械预期用途相关的受益和综合剩余风险。受益可以用受益大小或程度、预期患者群体中体验受益的概率以及受益的持续时间和频次来描述。评价宜考虑预期医疗适应证的知识、在技术和医学方面普遍公认的最新技术水平、以及可替代医疗器械或治疗方法的可获得性。
- b) 剩余风险的可视化表示可能是有用的。可以将每个单个剩余风险显示在风险图或风险矩阵中（例如图 3 和图 4），给出风险分布的视图。如果多个风险在风险矩阵的较高严重度区域或较高概率区域，或风险聚集在临界线附近，则风险的分布能表明综合剩余风险可能是不可接受的，即使每个单个风险已判定为可接受。
- c) 制造商可以将所考虑的医疗器械与市场上可获得的类似医疗器械相比较。在与类似医疗器械比较时，关键问题是，与所考虑的医疗器械的医疗受益相比，其是否具有可接受的综合剩余风险。医疗器械的剩余风险可以单独地与类似医疗器械的相应风险进行比较，要考虑预期用途的差异。宜仔细评审类似医疗器械在预期用途和不良事件方面的最新信息以及来自科学文献的信息，包括关于临床经验的信息。
- d) 制造商可以利用专家支持对使用所考虑的医疗器械的预期受益相关的综合剩余风险进行评价。这些专家可以来自不同的领域，宜包括那些具备临床和应用经验的和有类似医疗器械知识的人。专家宜具备适当的独立性，不受医疗器械的设计和开发人员的影响。他们能够帮助制造商考虑利益相关方的关注点。请注意 GB/T XXXXX—20XX/ISO 14971:2019 中对培训和经验的要求。
- e) 即使此时所有的单个风险已识别、控制并判定为可接受，对某些风险做进一步调查并将其结果作为综合剩余风险评价的一部分，可能是适当的。例如，可能有许多风险接近不可接受，综合剩余风险不能认为是可接受的，因此进一步的调查将是适当的。
- f) 当某些风险在其原因或所采取的风险控制措施方面相互影响有关时，开展进一步的调查可能是适当的。风险控制措施的有效性的验证不仅宜单独进行，还宜与其他风险控制措施结合进行。这也能适用于旨在同时控制多重风险的风险控制措施。故障树分析 (FTA) 或者事件树分析 (ETA) 可以是发现风险和其风险控制措施之间关系的有用工具。

9 风险管理评审

GB/T XXXXX—20XX/ISO 14971:2019 要求评审风险管理过程的最终结果，以确保风险管理计划已得到适当地执行，综合剩余风险可接受，并已建立适宜的方法收集和评审生产及生产后相关信息。风险管理评审是在所有风险控制措施已经实施和验证后，但在医疗器械商业销售放行之前实施的。风险管理报告提供了该评审的汇总，并包含在风险管理文档中。

如果获得新的信息，例如在生产和生产后阶段，可能需要修改或更新风险管理报告。制造商确定何时对风险管理计划执行情况进行后续的评审并更新风险管理报告，例如，在医疗器械的设计发生重大变更后。

风险管理计划实施情况的评审不应与由最高管理者按照策划的时间间隔对风险管理过程适宜性的评审（见 4.2.3）相混淆。风险管理计划与某类医疗器械（或医疗器械族）的生命周期相关。风险管理过程适宜性的评审与过程的有效性以及如何实施该过程相关。

10 生产和生产后活动

10.1 总则

生产和生产后信息的监视是确保医疗器械制造商闭合反馈回路并使风险管理成为一个持续的生命周期过程的关键步骤。在该阶段，从许多不同来源收集信息，评审其与安全的相关性。适当时，反馈到风险管理过程的早期阶段，以保持医疗器械的安全。

GB/T XXXXX—20XX/ISO 14971:2019要求制造商建立一个系统，以主动收集和评审关于医疗器械可能与安全相关的信息。在风险管理计划中（见4.4.8）记录建立该系统所必需的活动。

生产和生产后的活动可以作为上市后监督系统的一部分。有关上市后监督的更多指南见ISO/TR 20416^[35]。

注：本阶段与GB/T XXXXX—20XX/ISO 13485:2016^[24]的第7章和第8章的相关部分是一致的。更多指南见ISO手册GB/T XXXXX—20XX/ISO 13485:2016 医疗器械-应用指南^[25]。

10.2 信息收集

与医疗器械安全相关的信息可以来自各种来源。制造商在开发和销售类似医疗器械方面越有经验，就越有可能对医疗器械的性能、患者群体和可能发生的可合理预见的误使用和与医疗器械有关的风险有很好的了解。

生产和生产后的活动可以包括接收关于医疗器械安全和性能的信息。信息来源通常包括来自用户、销售人员、服务人员和培训人员的一般反馈。这些信息可能与已发生的伤害相关，或者与未发生伤害的危险情况相关。这些活动包括从利益相关方以获取具体信息和见解，方法包括采用顾客调查、专家用户组（焦点小组）以及制造商主导的医疗器械跟踪/植入登记等。它还包括公开可获得的信息如临床文献、事件报告和不良事件数据库。

这些活动还可以进一步包括在上市批准之后进行的PMCF研究，其目的是用来提升上市后的医疗器械的安全和性能的临床证据。PMCF研究通常解决当医疗器械按照其预期用途使用时与安全或者性能相关的特定问题（即剩余风险）。临床研究的要求见ISO 14155^[26]。关于PMCF的进一步指南见GHTF/SG5/N4:2010^[3]。

收集的信息不必一定与制造商的医疗器械直接相关。具有类似预期用途、类似工作原理或类似危险的其他医疗器械能产生关于制造商医疗器械有关风险的有用信息。这也适用于没有医疗目的但具有类似用途或类似工作原理的其他产品。

表7给出了数据来源的清单，其包含了宜考虑加以分析并可能与安全相关的生产和生产后信息。该表格基于GHTF/SG3/N18:2010^[27]。

如果收集和评审信息是由不同的部门实施的，这些部门之间有效的沟通和协调是至关重要的。

表7 与生产和生产后信息相关的数据来源

数据来源	信息
生产	<ul style="list-style-type: none"> ——对供应商绩效/控制的监视数据 ——过程监视 ——过程检验/试验 ——内部/外部审核
投诉处置	<ul style="list-style-type: none"> ——数量 ——按照医疗器械族 ——按照顾客（医生、医疗机构、患者等） ——投诉原因 ——投诉编码 ——任何伤害严重度 ——涉及的组件

表7 与生产和生产后信息相关的数据来源（续）

数据来源	信息
服务报告	<ul style="list-style-type: none"> ——安装 ——医疗器械的首次使用 ——维护访问的频次 ——维修类型 ——维修频次 ——使用频次 ——更换的部件 ——服务人员
风险管理	<ul style="list-style-type: none"> ——发布的类似医疗器械的不良事件报告 ——利益相关方的关注和普遍公认的最新技术水平
临床活动	<ul style="list-style-type: none"> ——上市后临床随访（PMCF）研究
市场/患者调查	<ul style="list-style-type: none"> ——服务响应时间 ——征集的有关新的或改进的医疗器械的信息
科学文献	<ul style="list-style-type: none"> ——研究出版物
媒体来源	<ul style="list-style-type: none"> ——在线时事新闻 ——医疗信息网站 ——商业期刊、科学期刊和其他文献的文章
信息安全数据来源	<ul style="list-style-type: none"> ——独立的信息安全研究者 ——内部测试 ——软件或硬件技术供应商 ——医疗保健机构 ——与医疗器械共享类似技术的其他器械的公开事件 ——信息共享和分析中心（ISAC）

10.3 信息评审

收集的信息应得到评审以确定这些信息是否与安全相关。在评审中下列问题可以有所帮助：

- 预期用途是否仍然有效？
- 是否取得预期受益？
- 是否有先前未识别的危险或危险情况的证据？例如，是否发生了任何未预见的伤害？
- 是否出现了以前没有预见的误使用？
- 是否有预期用途以外的其他使用的增长趋势？
- 特定危险情况或伤害发生的频次是否意味着伤害发生的概率被低估了？
- 报告的伤害是否表明伤害严重度被低估了？
- 是否有证据表明风险控制措施无效？
- 综合剩余风险评价是否准确地代表了实际的市场经验？
- 普遍公认的最新技术水平是否发生变化？
- 是否有迹象表明风险可接受性准则需要调整？

这些信息的评审能够导致几种可能的结果，例如：

- 正确识别了危险和危险情况。对风险进行了充分的评定并且保持可接受；

- 正确识别了危险和危险情况,但风险已增大并且不再可接受。需要采取进一步措施;
- 未识别出危险或危险情况,需要采取进一步的措施;
- 普遍公认的最新技术水平或医疗器械的受益发生变化,需要采取进一步的措施。

关于普遍公认的最新技术水平的变化,还宜考虑治疗或诊断预期患者医疗状况的替代品的可获得性,包括这些替代品的安全和有效性以及有关的风险。也宜考虑无法获得诊断和治疗的情况下患者的风险和受益。

制造商也宜评价预期用途的预期受益是否已实现或者变化。如果受益发生变化而风险保持不变,则受益与综合剩余风险之间的平衡也会发生变化。受益估计的讨论见7.4.2。

宜考虑采用统计技术辅助数据的处理,例如趋势分析、预测性的可靠性工程技术(例如Weibull分析)和可靠性评价(例如试验医疗器械或组件直到失效、试验返回制造商的失效组件,或者试验同一批次或之前/之后批次的医疗器械)。关于统计技术的选择和使用的进一步指南见ISO/DIS 10017^{[21]1)}。

10.4 措施

如果收集的信息经过评审并确定与安全相关,则GB/T XXXXX—20XX/ISO 14971:2019要求采取若干措施。其中一些措施与特定的医疗器械相关,而其他的措施与风险管理过程相关。

如果存在之前未识别的危险或危险情况,适当时,则按照GB/T XXXXX—20XX/ISO 14971:2019的第5至7章的步骤评估和控制有关的风险。风险评估的结果和实施的风险控制措施记录在风险管理文档中。

如果某个风险已不再可接受,则有必要更新该特定风险的评估。评价收集的信息对先前实施的风险控制措施的影响,以确定这些措施是否仍然有效和充分地降低风险。评价结果宜作为医疗器械改进的输入。适当时,重复GB/T XXXXX—20XX/ISO 14971:2019第5至7章的步骤,并实施新的/附加的风险控制措施。更新的风险评估和实施的风险控制措施记录在风险管理文档中。

可能有必要再次评价与医疗器械预期用途的受益相关的综合剩余风险。也可能有必要重复风险管理评审和编写新的风险管理报告。详见GB/T XXXXX—20XX/ISO 14971:2019的第8章和第9章。

制造商还宜考虑是否需要采取措施处理下列医疗器械:

- 已销售的(即不在制造商的控制范围),因为可能有必要纠正或从市场上撤回这些医疗器械;
- 已制造但未销售的(即仍在制造商的控制下),因为可能有必要隔离和纠正这些医疗器械;
- 未来要制造的,因为可能有必要改进医疗器械的设计和制造或维修过程。

对于市场上的医疗器械,在制定进一步的风险控制措施之前,制造商宜考虑是否将任何紧急信息告知用户、患者和其他利益相关方作为临时措施(例如,GB/T XXXXX—20XX/ISO 13485:2016)^[24]中8.3所述的忠告性通知)。这种沟通的紧迫程度宜与风险程度相适应,因为这些措施的速度影响它们的有效性。时间期限可能会受到法规要求的限制。所采取的决定和措施记录在风险管理文档中。

信息评审的结果可能表明风险管理过程的不充分和不适宜。因此GB/T XXXXX—20XX/ISO 14971:2019要求制造商评价收集的信息对先前实施的风险管理活动的影响,以确定哪些活动宜加以改进。与最高管理者沟通这一评价的结果,最高管理者宜将评价的结果作为所策划的风险管理过程适宜性评审(见4.2.3)的输入。然后,最高管理者决定风险管理过程的哪些部分或者哪些方面需要改进以确保其持续有效。

1) 准备中, ISO/DIS 10017:2020在印刷阶段。

附录 A

(资料性)

识别危险和安全相关的特性

A.1 总则

GB/T XXXXX—20XX/ISO 14971:2019要求制造商识别那些可能影响安全的医疗器械的特性。考虑这些特性是识别医疗器械危险的必要步骤，其中一种方法是提出一系列关于医疗器械的制造、预期用户、预期用途、可合理预见的误使用和最终处置的问题。如果从所有涉及人员（例如使用者、维修人员、患者等）的角度询问这些问题，则使可能存在的危险能够呈现一个更完整的概貌。

在A.2中的问题能够帮助读者识别所有可能影响医疗器械安全的特性。附录H包含了估计体外诊断医疗器械风险所需考虑的附加要点。该清单并不详尽，也不代表所有的医疗器械，因此建议制造商增加适用于特定医疗器械的问题而忽略那些不相关的问题。也建议制造商不要仅从问题的本身，还需要关联其他问题来考虑每一问题。

制造商可进一步查阅相关的临床文献、适用的法规、ISO 16142-1^[29]中的医疗器械安全和性能基本原则或者是ISO 16142-2^[30]中关于体外诊断医疗器械安全和性能基本原则。若医疗器械需涉及信息安全，还有一个来源是AAMI TIR57^[1]。

A.2 问题

A.2.1 医疗器械的预期用途是什么和如何使用？

宜考虑的因素包括：

- 医疗器械的作用与下列哪一项相关：
 - 疾病的诊断、预防、监护、治疗或缓解；
 - 损伤的诊断、监护、治疗、缓解或补偿；
 - 生理结构或生理过程的查验、替代、调节或支持；
 - 妊娠控制？
- 使用适应证是什么？（如患者群体、用户特征、使用环境）
- 禁忌证是什么？
- 医疗器械用于生命维持或生命支持？
- 医疗器械失效时是否需要特殊干预？
- 如果出现信息安全漏洞，医疗器械的性能是否会受到影响（性能下降或可得性丧失）？
- 非授权访问、非授权活动或数据丢失是否会影响医疗器械的安全？

A.2.2 医疗器械是否预期植入？

宜考虑的因素包括植入的位置、患者群体、年龄、体重、身体活动情况等特性，老化对植入物性能的影响，植入物预期的寿命和植入的可逆性，植入物在植入时是否会被修改或配置以及执行修改或配置的访问接口（如与植入性医疗器械的物理接入点或无线连接）。

A.2.3 医疗器械是否预期和患者或其他人员接触？

宜考虑的因素包括预期接触的性质，即表面接触、侵入式接触或植入以及每种接触的时间长短和频次。

A.2.4 在医疗器械中采用了什么材料或组分，或者什么材料或组分与医疗器械共同使用或者接触？

宜考虑的因素包括：

- 与相关物质的相容性；
- 与组织或体液的相容性；
- 与安全相关的特性是否已知；
- 制造医疗器械是否采用了动物源材料？

注：见ISO 10993-1:2018^[22]的附录B，以及ISO 22442系列标准^[39]。

A. 2.5 是否有能量向患者传递或从患者身上获取？

宜考虑的因素包括：

- 传递的能量类型；
- 能量的控制、质量、数量、强度和持续时间；
- 能量水平是否高于类似医疗器械当前应用的能量水平。

A. 2.6 是否有物质提供给患者或从患者身上获取？

宜考虑的因素包括：

- 是供给还是获取物质；
- 是单一物质还是多种物质；
- 最大和最小传输速率及其相应的控制。

A. 2.7 医疗器械是否处理生物材料以用于随后的再使用、输液/血或移植？

宜考虑的因素包括过程的类型和处理的物质（如自动输液/血、透析、血液成分或细胞疗法处理）。

A. 2.8 医疗器械是否以无菌形式提供或预期由用户灭菌，或其他适用的微生物控制方法？

宜考虑的因素包括：

- 医疗器械是预期一次性使用包装，还是重复使用包装；
- 货架寿命问题；
- 重复使用周期次数的限制；
- 产品灭菌方法；
- 非制造商预期的其他灭菌方法的影响。

A. 2.9 医疗器械是否预期由用户进行常规清洁和消毒？

宜考虑的因素包括使用的清洁剂或消毒剂的类型和清洁周期次数的限制。医疗器械的设计可能影响日常清洁和消毒的有效性。另外，宜考虑清洁剂或消毒剂对器械安全或性能的影响。

A. 2.10 医疗器械是否改善患者的环境？

宜考虑的因素包括：

- 温度；
- 湿度；
- 大气成分；
- 压力；
- 光线。

A. 2.11 是否进行测量？

宜考虑的因素包括测量变量、测量结果的准确度和精密度，以及测量仪器或数据是否可能受到损坏。此外，宜考虑校准和维护的需要（见A.2.18）。

A.2.12 医疗器械是否进行分析处理？

宜考虑的因素包括，识别医疗器械是否通过输入或获得的数据得出结论、使用的算法和置信度。宜特别注意数据和算法的非预期应用，以及对算法和数据未经授权的操纵或更改。

A.2.13 医疗器械是否预期和其他医疗器械、药品或其他医疗技术联合使用？

宜考虑的因素包括：

- 识别可能涉及的任何其他医疗器械、药品或其他医疗技术；
- 与交互有关的潜在问题（例如，该医疗器械影响其他医疗器械的性能）；
- 患者是否遵从治疗说明。

A.2.14 是否存在不希望的能量或物质输出？

宜考虑的与能量相关的因素包括噪音、振动、热、辐射（包括电离、非电离辐射和紫外/可见光/红外辐射）、接触温度、漏电流、电场或磁场。

宜考虑的与物质相关的因素包括在制造、清洁或试验中使用的物质，如果其残留在医疗器械中将具有不希望的生理效应。

宜考虑的与物质相关的其他因素包括化学物质、废物和体液的排放。

A.2.15 医疗器械是否易受环境影响？

宜考虑的因素包括操作、运输和储存环境。这些因素包括光、温度、湿度、振动、溢出、对能源和冷却供应变化的敏感性和电磁干扰。

A.2.16 医疗器械是否影响环境？

宜考虑的因素包括：

- 对电力和冷却供应的影响；
- 有毒物质的排放；
- 电磁干扰的产生。

A.2.17 医疗器械是否有需要耗材或附件？

宜考虑的因素包括耗材或附件的规范以及用户在选择时的任何限制。

A.2.18 是否需要维护和校准？

宜考虑的因素包括：

- 是否由用户或专家来进行维护或校准？
- 是否需要专门的物质或设备来进行适宜的维护或校准？
- 校准品的数值溯源到更高级别的参考品；
- 如何确定何时需要维护和再校准；
- 如何验证校准（仍）是可接受的。

A.2.19 医疗器械是否包含软件？

宜考虑的因素包括预期是由用户还是专家进行安装、验证、修改或更换，和软件更新的真实性。

A. 2. 20 医疗器械是否允许获取信息？

宜考虑的因素包括可访问的以太网端口、USB端口、串行端口和可移动硬盘。

A. 2. 21 医疗器械是否存储患者护理的关键数据？

宜考虑的因素包括信息被修改和损坏、非授权访问数据的可能性，和对患者的影响。

A. 2. 22 医疗器械是否有货架寿命的限制？

宜考虑的因素包括医疗器械是否会随着时间劣变、贮存条件和初包装的影响，失效日期的告知（通过标记或指示物）、失效日期后使用的可能性及失效医疗器械的处置。

A. 2. 23 是否有延迟或长期使用效应？

宜考虑的因素包括人机工程学和累积的效应。实例包括盐水泵随着时间推移的腐蚀、机械疲劳、皮带和附件松动、振动效应、标签磨损或脱落、长期的材料降解。

A. 2. 24 医疗器械承受何种机械力？

宜考虑的因素包括医疗器械承受的力是否在用户控制之下，或者通过和其他人员的相互作用来控制。

A. 2. 25 什么决定医疗器械的寿命期？

宜考虑的因素包括电池耗尽、材料老化和由于老化、磨损、疲劳和重复使用引起的组件失效。也宜考虑到备件的可得性。

A. 2. 26 医疗器械是否预期一次性使用？

宜考虑的因素包括：

- 医疗器械使用后是否自毁？
- 用户是否可以明显看出医疗器械已使用过？

A. 2. 27 医疗器械是否需要安全地最终停用或处置？

宜考虑的因素包括医疗器械本身处置过程中产生的废物，或者对医疗器械上所有敏感信息的适当的清除。例如医疗器械是否含有有害的物质（例如有毒的化学或生物试剂），或物质是否可再循环使用？如果医疗器械存储数据，则宜考虑存储数据的适当处置和信息安全，包括数据的移除和保留。

A. 2. 28 医疗器械的安装或使用是否要求专门的培训或专门的技能？

宜考虑的因素包括医疗器械的复杂性与新颖性，以及安装、维护或使用医疗器械的人员的知识、技能和能力。这可能包括培训、教育、能力评定、证书或资格。

A. 2. 29 如何提供安全信息？

宜考虑的因素包括：

- 信息是否由制造商直接提供给最终用户，还是涉及第三方（如安装人员、护理提供者、医疗保健专业人员、实验室主任或者药剂师）的参与，以及这是否涉及培训；
- 调试和向最终用户的移交，以及是否很可能/有可能由不具备必要技能的人员来安装；
- 基于医疗器械的类型和预期寿命期，说明是否需要操作人员或服务人员进行再培训或再认证。

A. 2. 30 是否建立或引入了新的制造过程？

宜考虑的因素包括新的或创新的技术的应用和生产规模的变化。这可能涉及委托生产、供方和厂商的变化。

A. 2. 31 医疗器械的成功应用，是否取决于用户接口的可用性？

A. 2. 31. 1 用户接口设计特性是否可能促成使用错误？

宜考虑的因素包括：控制器和指示器、使用的符号、人机工程学特性、物理设计和布局、操作层级、软件驱动的医疗器械的菜单、警告的可视性、报警的可听性、颜色编码的标准化。有关可用性的更多信息见 IEC 62366-1^[16]，有关报警的信息见 IEC 60601-1-8^[7]。

A. 2. 31. 2 医疗器械是否在因注意力分散而导致使用错误的环境中使用？

宜考虑的因素包括：

- 使用错误的后果；
- 注意力分散是否常见；
- 用户是否可能受到不常见分散注意力情况的干扰；
- 重复的压力是否会降低用户的意识或注意力。

A. 2. 31. 3 医疗器械是否具有连接部件或附件？

宜考虑的因素包括错误连接的可能性、与其他产品连接方式的相似性、连接力、对连接完整性的反馈以及过紧和过松的连接。

A. 2. 31. 4 医疗器械是否有控制接口？

宜考虑的因素包括间距、编码、分组、图形显示、反馈模式、出错、疏忽、控制差别、可视性、启动或变换的方向、控制是连续的还是断续的以及设置或动作的可逆性。

A. 2. 31. 5 医疗器械是否显示信息？

宜考虑的因素包括在各种环境下的可见性、方向性、用户的视力/视野、人群和视角、显示信息的清晰度、单位、颜色编码以及关键信息的可访问性。

A. 2. 31. 6 医疗器械是否由菜单控制？

宜考虑的因素包括层次的复杂性和层次数量、状态认知、设置的位置、导航方法、每一动作的步骤数、顺序的明确性和记忆问题，控制功能相对于其可访问性的重要性，以及偏离规定操作程序的影响。

A. 2. 31. 7 医疗器械的成功使用是否取决于用户的知识、技能和能力？

宜考虑因素包括：

- （预期的）用户、其智力和体力、技能和培训；
- 使用环境、人机工程学方面、安装要求；
- 预期用户控制或影响医疗器械使用的能力；
- 能影响与医疗器械成功交互能力的预期用户的个人特性，见 IEC TR 62366-2^[17]。

A. 2. 31. 8 医疗器械是否由具有特定需求的人使用？

宜考虑的因素包括：

- 具有特殊特性的用户，例如残障人士、老人和儿童，可能需要他人协助才能使用医疗器械；

——具有不同技能水平和不同文化背景和期望的用户，可能在医疗器械的适当应用的认识上存在差异。

A. 2. 31. 9 用户接口是否能用于启动未经授权的动作？

宜考虑的因素包括：用户接口是否允许用户进入限制访问的操作模式（例如，用于维护或特殊的使用），这会增加使用错误的可能性因而增加有关风险；以及用户是否意识到已经进入这种操作模式。

A. 2. 32 医疗器械是否包括报警系统？

宜考虑的因素有错误报警、漏报警、报警系统断开、不可靠的远程报警系统的风险，以及用户理解报警系统如何工作的能力。IEC 60601-1-8^[7]给出了报警系统的指南。

A. 2. 33 医疗器械可能以什么方式被误使用（故意与否）？

宜考虑的因素是连接器不正确使用、关闭安全功能或报警、忽视制造商建议的维护，未经授权使用医疗器械或医疗器械功能。

A. 2. 34 医疗器械是否预期为移动式或便携式？

宜考虑的因素包括对把手、手柄、轮子或制动器的需要、以及对机械稳定性和耐久性的需要。

A. 2. 35 医疗器械的使用是否依赖于基本性能？

宜考虑的因素例如生命支持医疗器械的输出特性或报警的运行。有关医用电气设备和医用电气系统的基本性能的讨论见IEC 60601-1^[5]。

A. 2. 36 医疗器械的使用是否具有一定的自动化程度？

宜考虑的因素包括：

- 当具有一定自动化程度的医疗器械发生错误、警报或故障时用户的意识；
- 当需要干预自动执行动作时用户的意识；
- 用户干预或中止自动执行的动作的能力；
- 用户选择和执行适当的纠正措施的能力。

更多的关于具有一定自动化程度的医疗器械的指南见IEC TR 60601-4-1^[9]。

A. 2. 37 医疗器械是否产生一个输出，作为确定临床行为的输入？

宜考虑的因素包括不正确的或延迟的输出是否可能对患者造成直接或间接的风险，例如不正确的诊断导致患者延误治疗或不治疗。对体外诊断医疗器械的指南见附录H。

附录 B (资料性) 支持风险分析的技术

B.1 总则

本附录提供了若干能用于支持风险分析的技术的指南。其中的一些技术从可能的伤害开始并分析可能导致伤害的各种事件。其他技术从初始事件开始并分析可能导致伤害的后续事件或事件组合。其基本原则是对事件序列进行分析。

需要强调风险分析只是GB/T XXXXX—20XX/ISO 14971:2019中描述的风险管理过程中的一个步骤。而且，本附录所述的技术并未涉及风险分析的所有要素，仅仅提供了支持信息。例如，并不是所有这些技术中都包括危险情况的识别。这些技术是互补的，可能需要使用其中的多项技术来支持一个全面和完整的风险分析。

以下分析技术将更详细地讨论：

- 初始危险分析（PHA）在开发过程早期对于医疗器械设计细节所知甚少时，能用作识别危险、危险情况和可能导致伤害的事件的技术；
- 故障树（FTA）和事件树分析（ETA）在开发过程早期的安全工程中特别有用，用于识别和排序危险和危险情况、可能的风险控制措施以及分析不良事件后果；
- 失效模式和效应分析（FMEA）是用于系统性地识别单个组件的效应或后果的技术，并且随着对设计的成熟和对失效模式的更深入理解，这种技术更加适用；
- 危险和可操作性分析（HAZOP）通常用于开发过程的早期阶段，研究对预期性能的偏离；
- 危险分析与关键控制点（HACCP）通常用于开发过程的后期阶段以验证和优化设计概念或更改。

B.2 初始危险分析（PHA）

PHA是一种归纳方法，其目的是对给定的活动、设施或系统识别可能造成伤害的危险、危险情况和事件。它通常在项目开发的早期进行，此时关于设计细节或操作程序的信息很少，常常可以作为进一步研究的前奏。当分析现有系统或对危险优先处理顺序时，不允许使用更广泛的技术的情形下，这种方法可能是有用的。

在PHA中，通过考虑下列特性形成危险和危险情况的清单：

- 使用或生产的材料及其反应性；
- 使用的设备；
- 使用环境；
- 布局；
- 系统组件之间的接口。

此方法通过下列事项来完成：

- a) 识别危险情况发生的概率和危险情况导致伤害的概率；
- b) 定性评价可能的伤害的程度；
- c) 识别可能的风险控制措施。

获得的结果可以以不同的方式表示，如表格和树状图。

B.3 故障树分析（FTA）

FTA是一种主要对已由其他技术所识别的危险进行分析的方法。它从一个假定的不希望的结果，即一个可能的伤害或危险情况，亦称“顶事件”开始。以演绎的方式，从顶事件开始并询问“为什么”，所识别产生不希望结果的下一个较低功能系统级别的可能原因或故障模式。随后逐步识别不希望的系

操作并依次降低系统级别，直到所需要的系统级别，该级别通常是组件故障模式或者是可以采用风险控制措施的最低级别。这将揭示最有可能导致假定结果的组合，其结果以故障模式树型图的形式形象地表示出来。在树的每一个层级，用逻辑运算符（与门、或门等）描述故障模式的组合。树中所识别的故障模式可以是与硬件故障、人为错误或任何其他有关事件有关的导致不希望事件发生的事件。它们不局限于单一故障状态。

FTA提供了一个系统性方法，该方法足够灵活，可以分析各种因素，包括人的相互作用。故障树分析（FTA）是风险分析中的一种工具，用于估计故障概率，识别导致危险情况的单一故障和共因故障。此种图形化的表示可使系统行为和所包含要素易于理解，但当树变得很大时，可能要求使用计算机系统处理故障树。

有关FTA程序的更多信息见IEC 61025^[12]。

B.4 事件树分析（ETA）

ETA是一种因果分析技术，其基于对可能导致负面结果的系列动作和事件的分析。ETA中使用的逻辑和数学技术与FTA相同。然而，故障树是分析不希望的项事件如何发生的，而事件树是考虑系统中的特定组件或项目失效的影响，并得出该失效对整个系统以及用户和患者的影响。ETA采用归纳法，而FTA是演绎法。

事件树中的初始事件通常属于以下四个类型之一：

- a) 医疗器械中的失效或不安全状态；
- b) 使用错误；
- c) 公共设施失效（例如断电或互联网连接中断）；
- d) 环境条件（例如温度、湿度、海拔高度、天气）。

事件树分析的目标是确定由所选择的初始事件造成并可能最终导致的伤害的可能的负面结果的概率。有必要使用关于系统的详细信息来理解事件序列以构建事件树图。事件树以初始事件开始，然后事件的后果以二元的（成功/失败）方式呈现。每个事件都会创建一个路径，在该路径中会发生一系列成功或失败，在这种情况下能够对该路径发生的总概率进行估计。

有关事件树程序的更多信息见IEC 62502^[18]。

B.5 失效模式和效应分析（FMEA）

FMEA是一种系统性地识别和评价单一故障模式后果的技术，是一种使用问题“如果怎样，会发生什么？”的归纳技术。每次只分析一个组件，因而通常着眼于一个单一故障状态。以“自下而上”模式进行，即按照程序进到下一个更高的功能系统级别。

FMEA不仅限于组件设计的失效，也能包括组件在制造和装配过程中的失效（过程FMEA）以及最终用户对产品的使用或误使用（使用FMEA）。FMEA能够扩展到包括对单个组件故障模式、其发生概率和可探测性（仅到能够检出可启动GB/T XXXXX—20XX/ISO 14971:2019中的预防措施的程度）以及后果的严重度的调查。为实施FMEA，宜详细地了解医疗器械的结构。

这种技术的缺点可能源自于其处理冗余和维修或预防性维护措施的结合带来的困难，及其仅限于单一故障状态。

B.6 危险和可操作性研究（HAZOP）

HAZOP基于一种理论，该理论假定危险情况和伤害是由于设计偏差和操作变化引起的。在开发过程的早期且仅在定义了设计和开发输入时，才能实施HAZOP。它是一种识别危险和可操作性问题的系统性技术。它最初开发是用于化学工业的，关注对设计意图的偏离，但医疗器械的开发人员将其改做它用。

HAZOP能用于医疗器械的操作/功能（例如将用于疾病诊断、治疗或缓解作为“设计意图”的现有方法/过程），或用于对医疗器械的功能可能有重大影响的医疗器械制造或维护/服务过程（例如灭菌）。

HAZOP的两个特点是：

- 使用一个涵盖医疗器械设计及其应用的专业团队；
- 使用引导词帮助识别与正常使用的偏离(全部、无、不/不是、多于/少于、伴随、部分等)。

这种技术的目标是：

- 对医疗器械及其预期如何使用做出完整的描述；
- 系统性地评审预期用途的每个部分，以发现如何才能发生正常操作状态和医疗器械设计的偏离；
- 识别此种偏离的后果，并确定这些后果是否能够导致危险情况或可操作性问题。

当应用于制造医疗器械的过程时，在医疗器械特性取决于制造过程的情况下，最后一个目标特别有用。

有关HAZOP程序的更多信息见IEC 61882^[14]。

B.7 危险分析和关键控制点 (HACCP)

HACCP是一种系统性的方法，用于识别危险和危险情况并通过专注于制造过程中的关键控制点以控制和监视有关的风险。在下面的阐述中，风险管理的术语对常规的HACCP术语适当时进行补充。

HACCP的核心内容包括下列七项原则：

1. 进行危险分析(风险分析)以识别危险和危险情况；
2. 确定关键控制点 (CCP)；
3. 建立适当的界限；
4. 监视每个关键控制点 (CCP)；
5. 建立纠正和预防措施(识别和实施风险控制措施)；
6. 建立验证程序；
7. 建立文件和记录保持程序。

每一医疗器械都有其自身的危险和危险情况，其危险和危险情况可能与预期用途、可合理预见的误使用或与安全相关的特性相关。危险情况可能由生命周期不同阶段例如设计、制造、服务、使用处置等阶段的事件所引发。

有效的HACCP系统的核心聚焦在对所识别危险和危险情况的持续控制和监视。制造商通过建立过程流程图、危险分析工作表和关键控制计划并形成文件，证实所实施的风险控制措施的有效性。

HACCP系统使用下列工具作为文件化的证据：

a) 过程流程图

该图的目的是对过程中所涉及的步骤提供清晰而简单的描述。在后续的工作中流程图对HACCP小组是必要的。流程图将来还能作为其他人为其验证活动而理解过程的指南。过程流程图的范围宜覆盖制造商直接控制的所有加工步骤。

b) 危险分析工作表

此工作表包含危险分析(风险分析)的记录：

- 识别和列出过程中存在重大危险的步骤；
- 列出所有已识别的和每个步骤有关的危险(和危险情况)及其重要性；
- 列出每个危险(和危险情况)的所有风险控制措施；
- 识别出所有关键控制点及其监视和控制。

c) 关键控制计划

该计划基于HACCP七项原则，阐述拟遵循的程序，以确保对特定的设计、产品、过程或程序的控制。

该计划包括：

YY/T 1437—20XX/ISO/TR 24971:2020

- 识别关键控制点和适当的界限；
- 监视和持续控制活动；
- 实施和监视风险控制措施；
- 验证活动和保留记录。

征求意见稿

附录 C

(资料性)

方针、风险可接受性准则、风险控制和风险评价之间的关系

C.1 总则

本附录描述最高管理者定义的制造商用于确定可接受风险的方针和基于方针所建立的风险可接受性准则之间的关系。该描述包括可作为方针的组成部分的各要素，解释了如何将风险可接受性准则用于风险控制和风险评价。针对方针的某些要素，给出了方针、准则和风险评价之间关系的示例。

C.2 建立风险可接受性准则的方针

此方针提供建立风险可接受性准则的框架。这一框架指导准则的建立。这既涉及单个剩余风险可接受性准则，也涉及综合剩余风险的可接受性准则。

GB/T XXXXX—20XX/ISO 14971:2019要求将用于建立风险可接受性准则的方针形成文件，例如作为制造商质量管理体系文件的组成部分，但未必是风险管理文档的组成部分。

建立风险可接受性准则的方针可能通常阐述下列要素：

- 目的；
- 范围；
- 确定可接受风险的因素和考虑事项；
- 风险控制方法；
- 批准和评审的要求。

方针及其组成要素宜量身定制以适合制造商组织的特定需求。每一个要素的详细讨论如下：

——目的描述用于建立风险可接受性准则的方针的目标。

示例1：方针的目标是为建立风险可接受性准则提供指导。这些准则用于评价与制造商[制造商的名称]制造的医疗器械相关的剩余风险。这些准则将确保医疗器械具有与利益相关方期望一致的高安全水平。

——范围规定方针适用的人员、场合和时间。

示例2：本方针适用于所有参与建立、评审、更新和批准由[制造商名称]为商业销售所设计、开发和/或制造的医疗器械风险管理计划中风险可接受性准则的人员。

——在建立风险可接受性准则时宜考虑下列因素和事项：

- 医疗器械拟上市地区的适用的法规要求；
 - 特定类型医疗器械的相关标准，包括对特定性能具有批准/拒绝界限的测试标准（见附录 E）；
 - 普遍公认的最新技术水平，可通过评审类似医疗器械和类似其他产品的标准、最佳技术实践、公认的科学研究成果、权威机构的出版物和其它信息来确定；
 - 来自利益相关方的经过确认的关注，例如通过用户、临床医生、患者或者监管机构的直接沟通，或者通过新闻报道、社交媒体或者患者论坛的间接沟通。重要的是考虑不同的利益相关方群体对风险可接受性的认知和理解可能会有所不同，并受到其背景和利益性质的影响。
- 可以依据 GB/T XXXXX—20XX/ISO 14971:2019, 4.2 的注 1 来定义风险控制的方法。该方法可以包括对可行性的考虑，例如合理可行地将风险降至最低，合理可实现地将风险降至最低，或对受益-风险比无不利影响的情况下尽可能降低风险。另一个可能的风险控制方法可能与风险的大小相关，例如，对低于某一界限的小风险，可以省略风险控制。这在 C.4 中有进一步的详述；

示例3：在对受益-风险比无不良影响的情况下，尽可能地降低风险。考虑技术上可行的措施是否能在不影响医疗器械的预期用途或受益的情况下降低风险。

示例4：将与辐射暴露相关的风险降低到合理可实现的尽可能低的水平（ALARA）时，考虑风险控制措施的技术可行性。

——可在方针中规定批准和审查的要求。这能够包括由谁批准，以及如果需要，多长时间评审一次方针。

示例5：用于建立风险可接受性准则的方针由[最高管理者的职务/职能]批准并且至少每[X]年由[评审机构的名称]评审一次。

C.3 风险可接受性准则

风险可接受性准则是基于制造商用于确定可接受风险的方针建立的。这也适用于不能估计伤害发生概率时接受风险的准则，在这种情况下，准则可以只基于伤害严重程度。在风险管理计划中记录风险可接受性准则。

依据每种类型的医疗器械（或医疗器械族）的特性和预期用途，可以为其建立特定的准则，或者对所有的医疗器械应用相同的准则。风险可接受性准则可以包括对特定性能的定性要求和定量界限的组合，最好是基于标准。

GB/T XXXXX—20XX/ISO 14971:2019也要求建立综合剩余风险可接受性准则。这些准则可以与单个风险的可接受性准则相同或不同。将评价综合剩余风险的方法和其可接受性准则在风险管理计划中形成文件。第8章提供了更详细的关于准则和方法的指南。

C.4 风险控制

风险控制是做出决策和实施措施的过程，这些措施将风险降低到或者保持在规定的水平。这一过程可以用建立风险可接受性准则的方针中包含的方法来指导（见C.2）。下面讨论两种风险控制的方法。

一种可能的方法是考虑风险控制措施的可行性。可行性（是可行的）是指风险控制方案可行或者能够付诸实施。这不应与实用性（是实用的）相混淆，实用性是指有用的和方便的措施。可行性包含技术可行性和经济可行性两部分。

技术可行性是指不考虑成本的情况下降低风险的能力。下面是几个在技术可行性上存在问题的示例：

——采用降低医疗器械有效性或影响预期用途的风险控制措施（例如，降低手术电刀的电压至其有效电压水平以下），对受益与风险之间的平衡产生负面影响。

——过度复杂的医疗器械使用程序导致使用错误的概率增加或者预期用途受到影响，这对受益和风险的之间的平衡具有负面影响（见 GB/T XXXXX—20XX/ISO 14971:2019, 4.2 注 1）；

——造成混淆的多重报警，从而妨碍用户操作；

——包括太多的警告或警示标签以致于妨碍用户操作医疗器械；

——告知太多的剩余风险以致于用户难以理解哪些风险是真正重要的。

经济可行性是指在不使医疗器械成为不合理的经济问题的情况下降低风险的能力。因为如果风险控制措施使医疗器械过于昂贵将使其无法获得。

这些决定必然涉及在接受风险和获得治疗或诊断之间进行权衡。在确定什么可行时应考虑到对人类健康的保护、促进或改善的影响来考虑到成本和可获得性的影响。这些决定中的经济可行性关系到公共健康和整个社会的受益。然而，不宜将经济可行性作为接受不必要的风险的理由。

另外一个可能的风险控制方法是考虑剩余风险的大小。这可以包括根据风险的大小将其归为三类中的一类：

a) 剩余风险的大小超过制造商的风险可接受性准则；

- b) 剩余风险非常小，以至于认为微不足道或可忽略（即消除它不会导致更低的综合剩余风险）；
或
- c) 剩余风险介于 a) 和 b) 规定的两种状态之间；

在进行风险评价之前，该方针可以指导是否宜继续对分类为微不足道或可忽略的剩余风险（b类）进行风险降低工作。

在此方法中，制造商可以使用图C.1中所示的半定量风险图或者风险矩阵以支持风险估计（见5.5）。这一风险矩阵分为三个区域a) 不可接受风险，b) 微不足道的或可忽略的风险，c) 需要调查以确定进一步风险控制是否可行的风险。估计的风险（ R_1, R_2, R_3, \dots ）填入到相应的表格中。风险 R_1 到 R_3 不可接受，风险 R_4 和 R_5 进一步调查；而 R_6 微不足道，依据制造商的方针可以被接受。

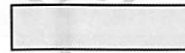
		定量严重度水平				
		可忽略	小	严重/大	重大	灾难性/致命
半定量 概率水平	经常性					
	可能的	R_1	R_2			
	偶尔的		R_4		R_3	
	很少发生的	R_6				
	不大可能的			R_5		

注：

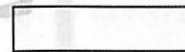
不可接受的风险



调查进一步风险控制



微不足道或忽略的风险



图C.1 三区域风险矩阵示例

C.5 风险评价

在这一步骤中，制造商将估计的风险与在风险管理计划中定义的风险可接受性准则进行比较并确定剩余风险是否可接受。在5.5和图C.1中所示的风险矩阵能支持风险的估计与评价，特别是对那些在标准中没有要求或解决方案的风险。

C.6 示例

制造商用于确定可接受风险的方针能够包括多个要素和方法。表C.1给出了方针、风险可接受性准则和风险评价之间的关系示例，其中包括某些要素和方法。

表C.1 方针各要素、风险可接受性准则和如何在风险评价中应用准则的关系示例

<p>法规要求</p> <p>方针：准则满足医疗器械上市或将上市的每个市场的适用法规的安全要求。例如，法规要求在单一故障状态下医疗器械保持安全，包括软件失效。</p> <p>准则：医疗器械在单一故障状态下保持安全，包括软件失效。</p> <p>评价：对医疗器械进行测试，并应用基于标准或法规中可测试的界限的准则。风险评价能包括检查检测结果、标准符合报告或者证书。</p>
<p>标准</p> <p>方针：准则基于适用的产品和过程标准。</p> <p>准则：1) 采用产品标准中的可测试的界限。 2) 按照 IEC 62366-1^[16]中的过程开发用户接口。</p> <p>评价：1) 检查每个标准的符合性评定报告 2) 检查可用性工程文档。</p>
<p>最新技术水平</p> <p>方针：准则基于普遍公认的最新技术水平，通过对市场上可获得的类似医疗器械的以及对预期用途和任何替代的疗法或医疗器械的文献的评审来确定。</p> <p>准则：1) 医疗器械漏电流是最新技术水平，通过符合 IEC 60601-1^[9]中关于漏电流的界限和试验要求来证实。 2) 传送装置的剂量精度是最新技术水平，通过符合 ISO 11608-1^[9]中关于剂量精度的界限和试验要求来证实。 3) 对冲击引起的机械失效的防护与类似医疗器械处于同水平或更优，通过对比试验如跌落试验来证实。</p> <p>评价：检查证实医疗器械符合或者超过基于最新技术水平的界限的数据和信息，通过基于国际标准或与市场上医疗器械的对比。风险评价可以包括对设计规范和对比测试结果进行检查和比较。</p>
<p>利益相关方的关注点</p> <p>方针：准则解决已知利益相关方的关注点，这些关注点是在关于医疗器械预期用途的医学和科学文献的评审、可用性研究，通过咨询委员会和/或焦点小组的反馈，或在生产后监视期间识别的。</p> <p>准则：1) 牛源性材料相关的风险是公众的一个关注点，通过设计从根本上消除。 2) 用于药物输送的针式医疗器械意外的多患者使用相关的风险对临床组织是一个关注点，因此为使风险被认为可接受，要求给出警告。</p> <p>评价：风险评价可以包括对照利益相关方要求的界限来评审医疗器械的性能，或者是利益相关方（在焦点小组或类似组织中）直接参与风险评价活动。风险评价可以包括将风险估计与利益相关方认为可接受的风险水平相比较。</p>

附录 D (资料性) 安全信息和剩余风险信息

D.1 总则

本附录的目的是阐明“安全信息”和“剩余风险的公开”之间的区别。提供了如何提供安全信息和如何公开剩余风险可以提高风险意识的指南。

D.2 安全信息

安全信息是一种风险控制措施，仅在制造商确定通过其他措施（进一步）降低风险不可行后才宜使用。降低风险的首选方案是实施使医疗器械固有安全的设计特性，如果不可能，则实施防护措施。即使如此，患者、用户或其他人的安全可能仍然依赖于要采取或避免的某些动作，有关这些动作的说明构成了安全信息。

安全信息是指导性的，向用户明确说明采取或避免的动作，以防止发生危险情况或伤害。这些信息可以以警告、注意事项、禁忌证、使用说明（包括安装、维护和处置）或培训的形式提供。GB/T XXXXX—20XX/ISO 14971:2019要求对安全信息的有效性进行验证（例如通过应用可用性工程过程），并可追溯到在风险管理文档中的风险评估。

某些情况下，当地的法规规定了安全信息的文本。

在编制安全信息时，识别该信息向谁提供及如何提供是重要的。这可能包括对风险的解释说明、暴露的后果以及为防止任何伤害宜采取或避免的动作。制造商宜考虑：

- 基于风险水平，对安全信息进行分类的需求；
- 为传达安全信息所需的详细程度；
- 安全信息的位置（例如医疗器械上的警告标签）；
- 为确保清晰易懂拟使用的文字、图片或符号；
- 预期接收者（例如用户、服务人员、安装人员、患者）；
- 提供信息的适当媒介（例如使用说明、标签、用户接口中的警告）；
- 法规要求。

安全信息可以以不同的方式进行告知，这取决于拟在医疗器械生命周期中何时告知信息，例如，通过菜单驱动的医疗器械的用户接口、作为在随附文件中的警告性说明，或在忠告性通知中。

安全信息可以多种形式提供，例如附在医疗器械上的警告标签，使用说明中的警告性声明，图形用户接口上的说明或者培训视频中的说明。下面给出一些示例：

- 警告：勿踩踏表面；
- 警告：勿移除盖子，有电击风险；
- 警告：勿使用已溶血的血清样本，这些样本会干扰测量并影响结果的准确性。

D.3 剩余风险的公开

剩余风险是指在实施所有风险控制措施后残留的风险。剩余风险与医疗器械使用相关的可能产生的副作用或后遗症相关。GB/T XXXXX—20XX/ISO 14971:2019要求制造商向用户告知重大剩余风险。

剩余风险的公开是描述性的，向用户提供必要的信息以使其理解与医疗器械使用有关的剩余风险。其目的是在随附文件中公开信息，以使用户（也可能是患者）能够权衡剩余风险和使用医疗器械的受益，做出明智的决定。制造商检查剩余风险并确定用户需要接收什么信息。制造商关于公开剩余风险的决定记录在风险管理文档中。

公开的信息在临床决策过程中可能意义重大。在预期用途的框架内，使用者能够决定在哪些临床条件中可以使用医疗器械以对患者实现一定的受益。剩余风险的公开也可有助于用户或医疗机构使患者对使用医疗器械期间或之后可能发生的副作用或伤害有所准备。注意，使用者和患者可能是同一个人，例如对于在家庭护理环境中使用的医疗器械。

当编制关于剩余风险公开的信息时，重要的是识别告知的内容以及信息传达的对象。制造商宜考虑：

- 信息的详细程度；
- 用于确保清晰易懂的措辞；
- 预期接收者（例如用户、服务人员、安装人员、患者）；
- 拟使用的方式和媒介。

在确定适当的详细程度时，制造商宜考虑概述信息是否比提供风险管理文档中的详细信息更适当。这些信息的性质和程度宜与剩余风险以及信息的预期接收者的知识和经验相适宜。

下面给出示例说明与使用医疗器械有关的剩余风险和通常公开的副作用：

- 直线加速器能用于治疗肿瘤。肿瘤放射治疗的剩余风险包括红斑或脱发的可能性；
- 在进行磁共振成像（MRI）时，患者会处于封闭的空间。一些患者可能出现幽闭恐惧症；
- 机械通气辅助或替代自主呼吸可能导致并发症，如气道损伤、肺泡损伤或气胸；
- 在接受肾结石碎石术后，大约 10% 的患者尿液中有血或者当小结石碎片通过时感到肾脏疼痛，同时约 2% 的患者会出现尿路感染；
- 使用激光进行眼科手术的潜在并发症包括眼睛肿胀、炎症或疼痛。手术后 6 周 1% 的患者出现轻度光敏感；
- 戴有植入式心律转复除颤器（ICD）的患者可能经历不适当的电击、想象的（幻觉）电击、依赖、抑郁、清醒时对电击的恐惧。

关于体外诊断医疗器械剩余风险公开的附加指南见 H. 5。

附录 E

(资料性)

标准在风险管理中的作用

E.1 总则

标准通过提供产品和/或过程的安全要求，在风险管理中能起到重要作用。ISO/IEC指南63^[20]提供了涉及安全内容的医疗器械标准制定指南。标准是由该领域的专家制定的并且被认为代表了普遍公认的最新技术水平。

当实施风险管理时，制造商首先考虑正在设计的医疗器械、其预期用途、与安全相关的特性以及有关的危险和危险情况。制造商可以选择并应用包含特定要求的产品标准和过程标准，以帮助管理在医疗器械生命周期内的与危险和危险情况有关的风险。

对于满足这些标准的要求和符合性准则的医疗器械，与那些危险或危险情况相关的剩余风险能够被认为是可以接受的，除非有相反的客观证据（例如不良事件报告、产品召回或投诉）。标准的要求（如工程过程或分析性的过程、特定输出界限、警告性说明或设计规范）可以被视为旨在解决特定危险情况的风险的风险控制措施。

在许多情况下，标准编写者已经实施并完成了风险管理的要素，并以设计要求和建立符合性的测试方法等形式为制造商提供了解决方案。开展风险管理活动时，制造商可以利用标准制定者的成果，不必重复分析得出标准要求。因此，标准提供了关于风险可接受性的有价值的信息。这些信息已在全球范围的评价过程中得到确认，包括多轮评审、评论和表决以达成国际共识。

E.2 产品安全标准在风险管理中的使用

产品安全标准可能对特定的危险情况规定了要求（例如设计解决方案、安全界限），该要求一经实施，风险即可接受。当管理风险时，制造商能用如下方式应用这些要求。

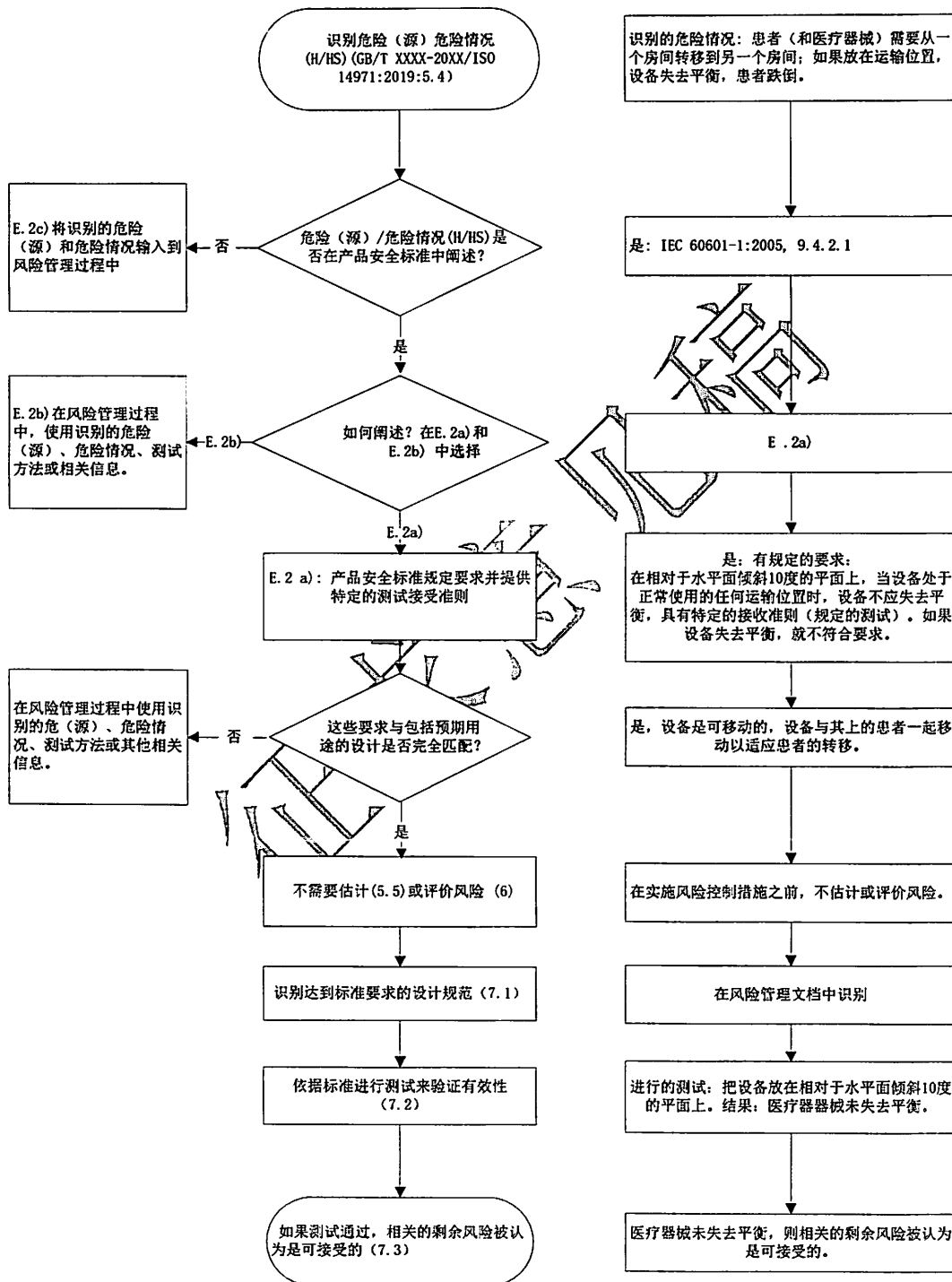
- a) 如果产品安全标准规定了针对特定危险或危险情况的要求，以及特定的接收准则，符合这些要求则推定剩余风险已降至可接受的水平，除非有相反的客观证据。例如：IEC 60601-1^[6]提供了漏电流限值，在规定状态下测量时，该限值即被认为是可接受的风险水平。本示例中，不必开展进一步的风险管理。在这种情况下，实施以下步骤。
 1. 识别与安全相关的特性并识别与医疗器械有关的危险和危险情况。
 2. 识别产品安全标准完全涵盖的危险或危险情况。
 3. 对于所识别的产品安全标准完全涵盖的危险或危险情况，制造商可以依标准中的要求来证实可接受风险。
 4. 制造商宜尽可能确保医疗器械的设计规范符合标准中作为风险控制措施的要求。

注：对于某些产品安全标准，识别全部特定风险控制措施的可能性是有限的。例如：IEC 60601-1-2^[6]中针对复杂医疗器械的电磁兼容性测试。

 5. 通过设计文件的评审，对这些危险情况的风险控制措施的实施进行验证；通过证实医疗器械符合产品安全标准相关要求的测试和测试结果，对风险控制措施的有效性进行验证。
 6. 如果相关要求得到满足，则认为有关的剩余风险是可接受的。对标准的使用宜在风险管理文档中形成文件以支持剩余风险的可接受性。
- b) 如果产品安全标准没有完全规定要求和有关测试和测试接收准则，则情况更加复杂。在某些情况下，标准仅提供了与已知危险或危险情况相关的特定试验，但没有特定的试验接受准则（例：IEC 60601-2-16^[6]）。在另一些情况下，标准仅识别了特定的危险或危险情况而没有进一步的要求（例如 IEC 60601-1^[6]中的某些条款）。由于替代方案的范围太大，无法就如何在

风险管理过程中使用此类标准提供具体指南。但是，鼓励制造商在特定医疗器械的风险管理中使用这些标准内容。

- c) 如果所识别的危险或危险情况未在产品安全标准中特别阐述，制造商宜在风险管理过程中阐述该危险或危险情况。制造商估计和评价风险，必要时，控制这些风险。有关概述使用产品安全标准的流程图和示例，见图 E. 1。



图E. 1 产品安全标准的使用和规定要求和提供特定试验接收准则的标准示例

E.3 过程标准与 GB/T XXXXX/ISO 14971

如下面示例所示，过程标准经常能够与GB/T XXXXX/ISO 14971结合使用。通过以下几种方式实现：

- 过程标准要求将 GB/T XXXXX/ISO 14971 的应用作为过程标准实施的一部分；或
- 过程标准旨在用于风险管理。

以上任一情况，正确使用过程标准都需要注意其与GB/T XXXXX/ISO 14971之间的接口，以使医疗器械达到可接受的风险水平。这些标准宜协同使用，以使输入、输出及其时间安排得到优化。下面举例说明这种理想情况。

a) YY/T 0664 医疗器械软件 软件生存周期过程

YY/T 0664和GB/T XXXXX/ISO 14971之间的关系在YY/T 0664-2020^[15]的引言中有详细描述：“作为主要的基础，这里设定医疗器械软件是在质量管理体系（见YY/T 0664-2020, 4.1^[15]）和风险管理体系（见YY/T 0664-2020, 4.2^[15]）之内开发和维护的。风险管理过程已在GB/T XXXXX/ISO 14971中得到很好地阐述。因此本标准通过直接对GB/T XXXXX/ISO 14971的规范性引用，利用了该有利条件。对软件来说少量附加的风险管理要求是必要的，特别是在识别与危险有关的软件影响因素方面。将这些要求加以汇总并纳入YY/T 0664第七章^[15]作为软件风险管理过程。”

在风险管理过程的危险识别活动中确定软件是否为危险情况的促成因素。在确定软件是否是促成因素时，需要考虑可能由软件间接造成的危险情况（例如：通过提供可能导致给予不适当治疗的误导性信息）。使用软件控制风险的决定是在风险管理过程的风险控制活动中做出的。YY/T0664要求的软件风险管理过程必须包含在按照GB/T XXXXX/ISO 14971建立的医疗器械风险管理过程之中。”

YY/T 0664规范性引用GB/T XXXXX/ISO 14971并特别要求：

- 软件开发策划（见 YY/T 0664-2020, 5.1^[15]），其要求与 GB/T XXXXX/ISO 14971 要求的风险管理计划一致；
- 软件风险管理过程（见 YY/T 0664-2020, 7^[15]），其要求基于 GB/T XXXXX/ISO 14971。

b) IEC 62366-1, 医疗器械 第一部分：医疗器械可用性工程的应用

IEC 62366-1:2015^[16]的图A.4中的流程图说明了风险管理和可用性工程两个并行且互相关联的过程之间的相互关系。IEC 62366-1^[16]识别了几个特定条款，其中可用性工程过程可以补充GB/T XXXXX/ISO 14971描述的风险管理并与之相互作用：

- IEC 62366-1:2015^[16]中 5.1 要求制造商编写使用规范，该规范可以是按照 GB/T XXXXX/ISO 14971 确定预期用途的输入；
- IEC 62366-1:2015^[16]中 5.2 要求制造商识别可能与安全相关的用户接口特性，作为按照 GB/T XXXXX/ISO 14971 实施风险分析的一部分；
- IEC 62366-1:2015^[16]中 5.3 要求制造商识别可能影响患者、用户或其他人员的，与医疗器械使用相关的已知或可预见的危险和危险情况，作为按照 GB/T XXXXX/ISO 14971 实施风险分析的一部分；
- IEC 62366-1:2015^[16]中 5.9 要求制造商对医疗器械的最终用户接口进行总结性评价，作为风险管理的一部分。

c) ISO 10993-1, 医疗器械的生物学评价 第1部分：风险管理过程中的评价与试验

ISO 10993-1^[22]是风险管理过程中医疗器械生物学评价的指南性文件，是每一器械综合评价和开发的一部分。

ISO 10993-1^[22]的附录B提供了按照GB/T XXXXX/ISO 14971的风险管理途径的指南，用于识别与医疗器械有关的生物学危险、估计和评价风险、控制风险、监视风险控制措施的有效性。

该途径将评审和评价来自所有来源的现有数据的与选择和应用额外试验（必要时）的相结合，从而能够对每个医疗器械与其使用中的安全相关的生物学反应进行全面评价。

生物学评价宜以用于其他产品风险相似的方式进行,宜包括:风险分析(危险和有关风险是什么?); 风险评价(风险是否可接受?); 风险控制(如何控制风险?)和综合剩余风险评价。生物学评价宜考虑:

- 选用的不同材料的物理和化学特性;
- 任何临床使用史或人类接触的数据;
- 关于产品和组件材料的任何现有的毒理学和其他生物学安全数据。

所需的数据量和调查的深度可能因预期用途而有差异,并可能取决于患者接触的性质和持续时间。

根据ISO 10993-1^[22],专业的评定员宜确定可获得的信息是否充分,以确定与生物危险有关的综合剩余风险是否可接受。该结论记录在生物评价报告中,成为风险管理文档的一个组成部分。与GB/T XXXXX—20XX/ISO 14971:2019中定义的过程一致,如果综合剩余风险评价得出所识别的风险可接受的结论,则无需进一步的风险控制。否则,宜采取适当措施进一步控制风险。

d) ISO 14155, 人体医疗器械的临床研究-良好临床实践

ISO 14155^[26]阐述了医疗器械上市前和上市后对人类进行的临床调查的设计、实施、记录和报告的良好临床实践,以评定医疗器械的临床性能或有效性和安全性。这与医疗器械的临床风险的估计和受益-风险平衡的评定相关。

征求意见稿

附录 F (资料性) 相关信息安全风险的指南

F.1 总则

GB/T XXXXX—20XX/ISO 14971:2019中描述的风险管理过程能用于与医疗器械信息安全有关的危险和风险。为避免误解认为需要一个单独的过程来管理与医疗器械信息安全相关的风险，在GB/T XXXXX—20XX/ISO 14971:2019的范围中特别提到与数据和系统信息安全相关的风险。这并不排除应用特定标准的可能性，在这些标准中提供了对信息安全风险的评估和控制的特定方法和要求。

数据和系统信息安全的损坏可能导致伤害，例如由于数据丢失、数据访问不受控、诊断信息的损坏或丢失、或者导致医疗器械失效的软件损坏。

本文件中的信息安全包括网络安全以及数据和系统信息安全。

F.2 信息安全风险管理中使用的术语

信息安全风险管理经常采用与GB/T XXXXX—20XX/ISO 14971:2019不同的术语。但是，信息安全风险管理中的术语和GB/T XXXXX—20XX/ISO 14971:2019中的术语之间存在着对应关系。下列术语的定义来源于IEC指南120^[4]。其他定义例如来自AAMI TIR57^[11]的定义也用于信息安全风险管理。

——信息安全：通过防护措施的建立和维护达到的状态，这些措施确保不受恶意行为或影响侵犯的状态。（见 IEC 指南 120:2018^[4], 3.13）。这些恶意行为或影响可能是有意的或无意的；

注：在AAMI TIR57^[11]的2.6和IEC 80001-1:2010^[9]的2.5中，信息安全被定义为医疗器械的一种运行状态。医疗器械的信息资产（数据和系统）被合理地保护，以防保密性、完整性、可得性的降低。由此可见，信息安全侧重于可能引发风险的恶意行为，即能促成风险的事件，并且信息安全被认为是一种不受侵犯的状态，即免于不可接受的风险的状态。（类似于GB/T XXXXX—20XX/ISO 14971:2019的3.26中的安全）。

——威胁：当有违反信息安全而引起伤害的环境、能力、动作或事件时，而存在的危害信息安全的的可能性（见 IEC 指南 120:2018^[4], 3.13）。威胁对应于，能利用脆弱性而导致危险情况的事件或事件序列（见 GB/T XXXXX—20XX/ISO 14971:2019, 3.5）；

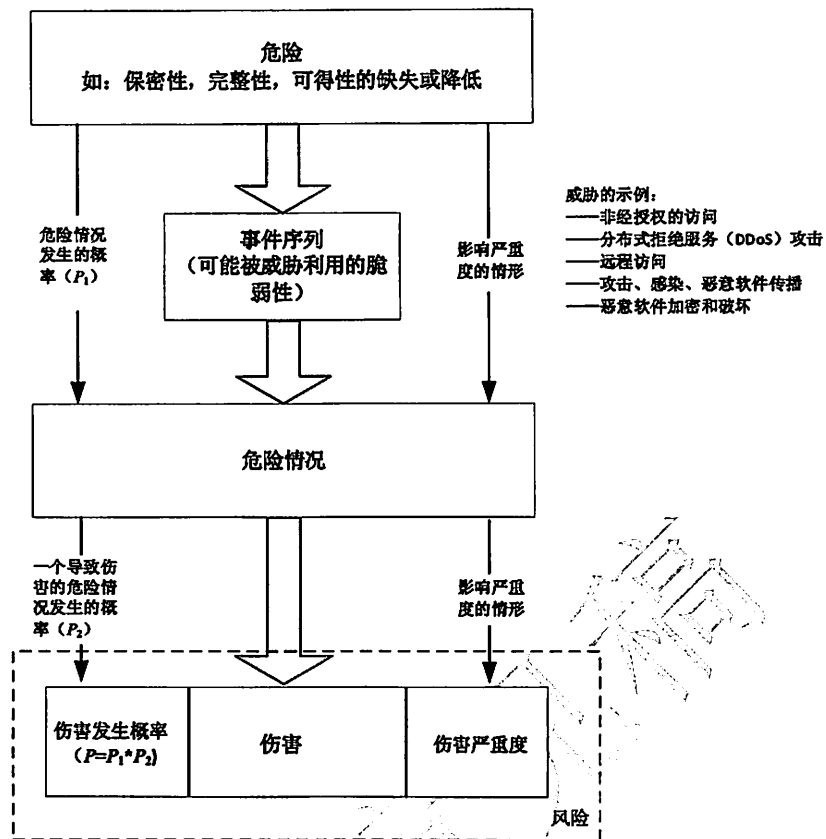
——脆弱性：系统设计、实现或操作和管理中存在的缺陷或弱点，可被用来危害系统的信息安全策略（见 IEC 指南 120^[4], 3.18）。脆弱性可以被视为一种类型的事件或情形（见 GB/T XXXXX—20XX/ISO 14971:2019, 表 C.2）；

——保密性：信息不向未经授权的个人、实体或过程提供或公开的特性（见 IEC 指南 120:2018^[4], 3.6）；

——完整性：准确且完整的特性（见 IEC 指南 120:2018^[4], 3.9）；

——可得性：经授权的客体要求时可获得和可使用的特性（见 IEC 指南 120:2018^[4], 3.5）。

与信息安全相关的危险、事件序列、危险情况和伤害之间的关系可见图F₁所示。



图F.1 危险、事件序列、危险情况和伤害与信息安全术语之间的关系

F.3 GB/T XXXXX/ISO 14971 与信息安全之间的关系

一个常见的误解是GB/T XXXXX—20XX/ISO 14971:2019只适用于人的健康，而忽视伤害的定义包括对财产和环境的损害。这个误解经常出现在对信息安全的讨论中，认为GB/T XXXXX—20XX/ISO 14971:2019仅限于与患者和用户相关的风险，而不覆盖信息安全相关风险。

宜注意的是，IEC指南120^[4]中关于信息安全的定义与安全的定义不是同一层面的。安全与风险管理的最终结果相关，而信息安全则关注恶意行为或事件对系统特性和性能的影响。

GB/T XXXXX—20XX/ISO 14971:2019中伤害的定义适用于人体、财产和环境，可能存在一些重叠。例如对电子健康记录的损坏（对财产的损坏）可能导致错误的诊断，从而可能导致患者受伤（对人体的损害）。需要注意的是，信息安全风险管理的范围往往更广。表F.1中列出了几个可能导致伤害的信息安全危险的示例：

表F.1 在信息安全的危险情况下的危险、事件序列、危险情况和伤害示例

危险	事件序列	危险情况	伤害
丧失数据完整性	1) 无需开放的网络端口的脆弱性被利用 2) 输注泵的剂量设置数据被非授权的访问而修改	不正确的剂量数据导致输液未按预期输送	健康恶化 死亡
丧失数据完整性	1) 无需开放的网络端口的脆弱性被利用 2) 患者数据或诊断结果被非授权的访问而修改	修改的数据导致不正确的临床决策或程序，或缺少治疗	健康恶化 不必要的手术

表F.1 在信息安全的危险情况下的危险、事件序列、危险情况和伤害示例（续）

危险	事件序列	危险情况	伤害
丧失数据可得性	1) 无需开放的网络端口的脆弱性被利用 2) 医疗器械的性能因 DDoS 攻击或勒索软件而降低或终止	延误治疗 无法诊断	医疗器械功能 丧失 健康恶化
丧失数据保密性	1) 无需开放的网络端口的脆弱性被利用 2) 泄露个人健康信息	拒绝保险承保范围导致缺乏治疗	心理压力 健康恶化

此外，在区分这些领域时，有时会使用术语“安全风险”和“信息安全风险”。本文遵循 ISO/IEC 指南 63^[20] 的建议，其中术语“安全”不宜作为形容词使用。在利用 GB/T XXXXX/ISO 14971 的框架管理与信息安全相关的风险时，宜谨记信息安全风险管理的目标也是为了达到安全（即免于不可接受的风险）。

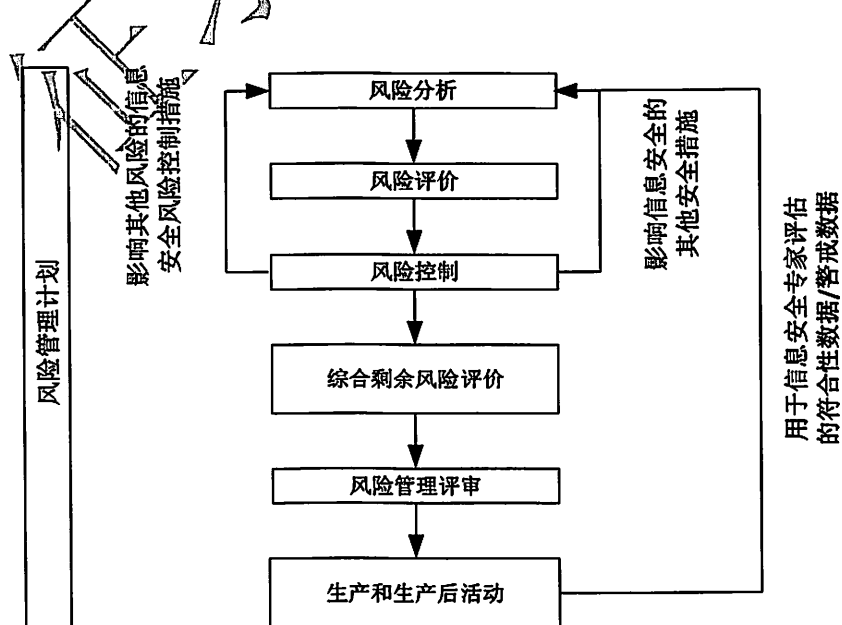
需要注意的是 IEC 指南 120^[4] 中的信息安全的定义包括非故意的行为，例如不是由于恶意攻击导致的个人健康信息的意外泄露；与正常使用相关的信息安全危险也宜进行评价，例如向未经授权的人员展示个人健康信息。

F.4 信息安全风险管理特性

信息安全风险管理遵循与其他风险的管理类似的过程，该过程步骤包括建立风险可接受性准则、实施风险分析、风险评价、风险控制、综合剩余风险评价等。所使用的数据源、分析工具和技术以及确认等特定细节可能是不同的，但是整体过程是相同的。

GB/T XXXXX—20XX/ISO 14971:2019 要求评价风险控制措施引起的风险。信息安全风险控制措施可能会带来新的风险，反之亦然。例如一个信息安全风险控制措施要求用户在使用前输入密码，但在生命挽救医疗器械（如自动体外除颤器）上，由于忘记密码而导致的潜在延迟可能是不可接受的，因此宜考虑不同的选择，图 F.2 阐述了这种关系。

与信息安全相关的危险的管理可能要求不同于其他危险管理的方法和途径，类似于与可用性或可靠性相关风险控制方法的差异。



图F.2 信息安全风险控制措施与其他风险控制措施可能的相互作用

严重度定义为“危险可能后果的度量”（见 GB/T XXXXX—20XX/ISO 14971:2019, 3.27）。严重度通常用人的健康恶化程度表示。低严重度可以定义为暂时的不适或不需要医疗干预的轻度损伤，中等严重度可以定义为需要医疗干预的损伤，高严重度可以定义为需要立即进行医疗干预并可能导致永久性损伤甚至死亡的损伤。在信息安全风险管理中，安全的数据系统保持高度保密性、完整性和可得性。因此，与安全系统损害相关的伤害的严重程度宜考虑很多因素其中包括这三个因素的丧失或降低的结果。

伤害通常是对人体健康的损伤或损害并且与基本安全（例如电击）或者医疗器械的预期用途（例如 X射线成像时的辐射暴露）相关。在信息安全风险管理中，伤害通常是对财产的损害，并与医疗器械中的信息（例如个人健康信息的泄露、软件或数据的修改或损坏）或连接设备中可得的信息相关（例如连接丢失、信用卡信息的访问）。

伤害发生概率通常是设计和制造、材料选择、公差、设计余量等的函数。这些因素通常能以高水平置信度来预测。而在信息安全风险管理中，发生的概率通常是动机、经济受益以及机会的函数，例如开放的漏洞。这些因素都不容易估计。此外，一旦漏洞信息在互联网上公开，漏洞被利用的概率可以迅速从“微小”变为“每次”。

F.5 保密性、完整性、可得性优先顺序

在评价与信息安全相关的风险时，制造商确保信息安全优先级（保密性、完整性和可得性）适当地考虑医疗器械的预期用途。在某些应用中，信息的完整性备受关注，完整性的丧失可能导致患者病历的更改（如医嘱或者医疗数据/图像的更改）。在其他情况下，保密性的丧失可能更为重要，因为泄露个人健康信息能导致潜在勒索。

保密性丧失的另一个示例是设计特性未加密（静态或传输中的数据）的情况。这些特性的反向工程可能会危及医疗器械的操作，从而导致对患者的损伤。医疗器械可得性的丧失可能导致诊断或治疗的延误。特别是对于生命支持或救生医疗器械而言，可得性的丧失或有效性的降低对于人的健康至关重要。这些示例表明，与信息安全相关的风险可能会影响患者的健康，这取决于医疗器械的预期用途。

附录 G

(资料性)

未采用 GB/T XXXXX/ISO 14971 设计的组件和器械

G.1 总则

本指南假定制造商已经建立了符合 GB/T XXXXX—20XX/ISO 14971:2019 的风险管理过程。本指南并未替代或消除 GB/T XXXXX—20XX/ISO 14971:2019 对医疗器械的任何要求，而是向制造商介绍了一个弥补风险管理文档中可能存在的缺陷的方法。

由于各种原因，制造商可能没有对医疗器械的每个组成组件遵循 GB/T XXXXX—20XX/ISO 14971:2019 中所述的所有过程和要求，例如专利组件、软件组件、非医疗来源的子系统，或市场上已有的医疗器械。在这种情况下，证明符合 GB/T XXXXX—20XX/ISO 14971:2019 时，制造商的风险管理文档可能是有限的和不充分的。然而，在大多数情况下，关于医疗器械及其组成组件的大量信息是可以获得的。例如通过评审医疗器械或市场上类似医疗器械的生产后数据可以获得关于实际使用的信息。相关的可靠性和生产数据以及以前编制的与安全相关的文件也可能是可得的。

本附录旨在为制造商提供一个关于如何利用可获得的信息建立一个今后可维护的初始风险管理文档的指南。

注：“医疗器械”包括医疗或非医疗来源的子系统、组件和软件组件。

利用可获得的信息，制造商能建立风险管理文件，该文件将是考虑中的特定医疗器械建立初始风险管理文档的基础。该文件能够作为充分证据来证明特定医疗器械的风险是可以接受的，并且该医疗器械对于其预期用途是安全的。另一方面，制造商能够确定附加的风险控制措施是恰当的。例如与普遍公认的最新技术水平相比可能表明，采取附加的措施是对完全符合 GB/T XXXXX—20XX/ISO 14971:2019 的保障。

G.2 风险管理计划

GB/T XXXXX—20XX/ISO 14971:2019 要求策划所有的风险管理活动，特别是那些创建风险管理文档以证明医疗器械对于其预期用途是安全的活动。GB/T XXXXX—20XX/ISO 14971:2019 中给出了风险管理计划中的强制性要素。

在建立风险管理计划时，宜特别注意：

- a) 医疗器械生命周期剩余阶段的风险管理活动（特别是维护、最终停用和处置，如适用）；
 - b) 职责和权限的分配；
 - c) 今后风险管理活动评审的要求；
 - d) 医疗器械的风险可接受性准则，基于制造商确定可接受风险的方针，包括在伤害发生的概率不能估计时接受风险的准则。
 - e) 评价综合剩余风险的方法和综合剩余风险的可接受性准则；
- 注1：d) 和 e) 中的准则可以由生产和生产后信息支持。
- f) 对现有风险控制措施和必要的新风险控制措施的验证活动。
 - g) 收集和评审生产和生产后信息的活动，以及如何利用这些信息确定与医疗器械有关的风险是否可以接受；

注2：设计文件或其他文件能够包含一些验证证据。

G.3 风险管理文档

由于医疗器械的设计没有应用GB/T XXXXX—20XX/ISO 14971:2019，制造商宜开始为医疗器械建立一个风险管理文档。可能已经实施了一些风险控制措施，但没有将医疗器械有关的危险和危险情况的可追溯性形成。因此，制造商可以首先确定已对医疗器械采取的解决方案，然后确定这些方案所控制的危险和危险情况。这些解决方案现在被认为是风险控制措施，并记录在风险管理文档中。

上述建立风险管理文档的方法可以由下列几个步骤组成：

1. 将医疗器械的预期用途、可合理预见的误使用以及与安全相关的特性形成文件。可合理预见的误使用可从生产后阶段收集的实际使用信息中得到。附录 A 中的问题有助于确定与安全相关的特性。
2. 识别医疗器械已经采用的所有可被视为风险控制措施的解决方案。
3. 识别与医疗器械有关的所有危险和危险情况，以及它们可能造成的伤害。
4. 确定是否存在未实施风险控制措施的危险或危险情况。这些情况下，估计和评价风险并实施 GB/T XXXXX—20XX/ISO 14971:2019。对于已实施风险控制措施的危险和危险情况，验证它们的有效性并估计和评价剩余风险。对于使用风险管理计划中定义的风险可接受性准则判定为不可接受的剩余风险，制造商宜考虑进一步的风险控制并应用 GB/T XXXXX—20XX/ISO 14971:2019。
5. 将每个所识别的危险和危险情况到风险控制措施的可追溯性形成文件。可追溯性能够通过以下要素形成文件：
 - 所识别的危险和危险情况；
 - 可能发生的伤害；
 - 风险控制措施；
 - 风险控制措施的实施验证和有效性验证；
 - 任何剩余风险的可接受性。
6. 按照 GB/T XXXXX—20XX/ISO 14971:2019 的第 8 章评价综合剩余风险。
7. 按照 GB/T XXXXX—20XX/ISO 14971:2019 的第 9 章评审风险管理计划的执行情况。在风险管理报告中将结果形成文件。

这些步骤中生成的记录和其他文件构成初始风险管理文档。

附录 H (资料性) 体外诊断医疗器械指南

H.1 总则

H.1.1 IVD医疗器械的风险管理

本附录的目的是为GB/T XXXXX—20XX/ISO 14971:2019的特定方面在IVD医疗器械中的应用提供指南。本指南重点关注不正确的或延迟的体外诊断结果给患者带来的间接风险，旨在通过本文件中的通用指南进行补充。对器械用户、其他人员和环境的风险在本附录的其他部分进行了阐述。其他诊断医疗器械的制造商也可能发现这些指南很有用。

在本附录中，“临床医生”作为通用术语，指的是看诊患者的医疗保健提供者以及要求检查的、解释检查结果和根据IVD检查结果采取措施的医疗保健提供者。有关IVD行业和检验医学中常用的其他术语定义见ISO 18113-1^[34]。

由于IVD医疗器械及其预期用途的多样化，本附录只能提供通用指南，目的是在制造商的风险管理过程中，促进批判性思维、跨职能分析和知情决策。本附录中的问题和示例，旨在指导具有适当科学、工程和临床专业知识的人员制订和实施有效的IVD医疗器械的风险管理计划。它们并非详尽无遗，也不一定代表所有IVD医疗器械的最佳实践。每个制造商宜确定什么适用于其特定IVD医疗器械。

H.1.2 IVD医疗器械风险管理的背景

对于IVD医疗器械制造商来说，管理对患者的风险可能是一项挑战。这些风险是间接的，通常以涉及“合格中间人”的扩展事件序列为特征。“合格中间人”的示例是：经过培训的使用IVD医疗器械进行体外诊断检查的使用者和依赖检查结果的临床医生。ISO 15189^[27]国际医学实验室质量和能力标准要求医学实验室控制对患者的风险。为支持这一要求，基于与GB/T XXXXX—20XX/ISO 14971:2019描述的原则和概念，开发了ISO 22867^[28]以描述医学实验室的风险管理过程，这将促进IVD医疗器械制造商与医学实验室之间有效的风险沟通。

制造商风险管理过程中的安全信息和公开的剩余风险是医学实验室风险管理过程的重要输入。相反地，IVD医疗器械用户对此类信息的需求以及实验室使用IVD医疗器械的反馈是制造商风险管理过程的重要输入。在开发或更改IVD医疗器械时，制造商有责任将用户对风险管理信息的需求作为设计输入。

当制造商向医学实验室提供IVD医疗器械时，任何无法通过设计或防护措施控制的风险，连同控制这些风险所需的安全信息一起转移给实验室。制造商也在随附文件中公开任何剩余风险，以便实验室负责人评价这些风险并确定其可接受性。

制造商能够提供安全信息来告知IVD医疗器械的用户，但不能影响临床医生要求检查检验、接收结果和根据检查结果采取措施的行为。

某些IVD医疗器械预期由临床医生在医疗点使用，而自测IVD医疗器械实际由患者使用。虽然这些医疗器械也可能存在相似的风险场景，但是这类用户控制风险的能力可能会更加有限。因此，重要的是护理点器械和自测器械设计为具有适合于实验室以外的（预期的）用户和（预期的）使用环境的风险控制措施。

H.2 风险分析

H.2.1 预期用途和可合理预见的误使用

H.2.1.1 分析用途和临床用途

绝大多数IVD医疗器械有两种用户。重要的是考虑：

- 完成全部检查或部分检查的用户（“分析用途”）；
 - 接收、解释检查结果并根据结果采取措施的临床医生（“临床用途”）。
- 预期用于自测的IVD医疗器械，患者可能是唯一的用户。

H.2.1.2 器械描述

每一项风险分析都从识别和记录IVD医疗器械及其在产生检查结果中的特定作用的清晰描述开始。描述IVD医疗器械时需要考虑的问题包括：

- 该器械是单独使用得出检查结果，还是与其他器械联合使用？
 - 如果器械是一个独立的分析系统，它是否是自动化的？（软件、机器人）
 - 如与其他 IVD 医疗器械联合使用以形成一个系统，它在产生检验结果中的作用是什么（例如样本收集系统、样本容器、测量仪器、软件、数据库、试剂、校准品、质控品或附件）？
 - 如果是系统的一部分，IVD 医疗器械如何与系统的其他组件交互作用？
- 是否有其他必要但未提供的试剂或附件？
- 器械是否采用新的或创新的技术（例如用于测量、通信）？
- 器械是否采用数字信息技术记录和/或传送检查结果给临床医生或与移动通信应用程序进行通讯？
- 软件应用程序是否提供诊断或治疗建议？
- IVD 医疗器械是否与基于体外诊断结果而立即实施治疗的医疗器械进行通信（例如测量血糖水平并与植入的胰岛素管理系统进行通讯的 IVD 医疗器械）？

H.2.1.3 分析用途

IVD医疗器械的预期用途包括预期被检测或测量的分析物、可接受的样本类型、校准、质量控制和预防性维护活动、以及使用的环境。重要的是还宜考虑可合理预见的误使用（见H.2.3.5）。

在确定IVD医疗器械的分析用途时考虑的问题包括：

- 器械拟测量或检查什么分析物？
- 检查结果是定性的、半定量的还是定量的？
- 器械是用于检查前、检查或检查后阶段？
- 能够分析哪些样本？（例如血清、血浆、全血、尿液、其他体液、组织）
- 这些样品中潜在的其他物质是否会干扰分析过程？
- 在核酸测序程序中，扩增产物的污染是否对来自环境的 DNA/RNA 的污染敏感？
- 在特定的使用环境（例如医学实验室、急诊室、手术室、救护车、重症监护室、新生儿监护室、疗养院、医生办公室、筛查诊所或患者家中）中使用是否有任何额外限制？
- IVD 医疗器械是否与其他器械或网络进行接口、连接或通讯？
- 谁将使用该 IVD 医疗器械进行检查，何种培训和资格是适宜的？

H.2.1.4 临床用途

IVD医疗器械的预期临床用途（在某些管辖区称为适应证）包括医疗条件和使用检查结果的患者群体。制造商可以依靠内部或外部的临床专家了解以下内容：

- 如何将体外诊断检查结果用于临床决策；
- 医学决策点和需要的准确程度；
- 临床医生能否识别不正确的结果（例如基于错误的程度或与其他临床信息的一致性）；
- 出现异常或非预期结果时，临床医生会采取什么行动；
- 延迟结果的临床重要性（如有）；

——不必要的医疗干预的潜在不良后果。

确定临床用途时需要考虑的其他问题包括：

——检查结果是否用于：

——为了治愈、治疗或预防疾病或其他健康状况而进行的诊断？

——测量体液成分以确定患者的健康状况？

——监测治疗药物水平以确保有效剂量？

——确定捐献血液或器官的安全性？

——筛查人群是否存在某种特定标记物？

——预测替代方案（“伴随诊断”）的治疗效果？

——预测患病的风险？

——其预期用途之外的其他应用？

——结果用于检测、诊断、预测或监测哪些损伤、疾病或状况？

——谁将使用体外诊断检查结果：医学专家、普通临床医生还是患者？

——检查结果在医疗决策中所起的作用：

——作为立即做出医疗决策的依据？

——结合其他相关信息以指导医疗决策？

——哪些患者群体将主要受益于体外诊断检查？

——哪些患者群体宜被明确禁忌？

H.2.2 与患者的安全相关的特性

H.2.2.1 总则

除了与其他医疗器械相同的生物、化学、电气、机械和信息安全的特性外（见附录A），IVD医疗器械还具有决定其预期临床用途适用性的分析性能和可靠性特性。一些IVD医疗器械可以同时进行多项检查，其临床性能依赖于对结果模式的解释（如多重检测）。采用数字信息技术的IVD医疗器械还可能具有与存储和传输检查结果或辅助信息到医疗决策所需位置的能力相关的特性。不满足性能、可靠性或通讯要求可能引发一系列对患者可能造成危害的事件序列。

H.2.2.2 与患者安全相关的性能特性

a) 定量检查测量取自患者的代表性样本中的含量。结果通常用浓度或百分比表示。所需的分析性能取决于医学应用，但假性升高、假性正常和假性降低的结果可能会影响诊断，导致不当或延误的治疗，并导致患者伤害。伤害的类型和严重程度取决于医学决策点的误差程度。

定量 IVD 医疗器械的相关性能特性可能包括：

——测量值的正确度（偏差、对参考标准的溯源性）；

——测量精密度（重复性、中间精密度、再现性）；

——分析特异性（干扰或交叉反应物质的影响）；

——分析灵敏度（区分数量限制或范围的能力）；

——检出限（能够可靠检测的最低量值）；

——定量限（能够准确测量的最低量值）；

——测量区间（确认的分析性能的数值范围）。

b) 半定量检查提供具有临床意义的近似测量值。其值通常根据顺序量表给定或报告为数量界限，可以用数字表示（例如在指定的数值范围内，或者大于或小于特定的量，效价或梯度稀释）或相对量表示（例如+3、+2、+1 或微量）。半定量检查的常见示例如尿液“试纸”、检测酮类物质的片剂和血清学凝集程序。

如果检查结果报告为在低倍场视野或高倍场视野中观察到的细胞数量，则显微镜检查也能够被认为是半定量的。例如尿液显微镜检查在高倍场中可能报告 0 到 5 个红细胞。

半定量 IVD 医疗器械的性能特性能够包括：

- 分析灵敏度（区分数量限制或范围的能力）；
- 分析特异性（干扰或交叉反应物质的影响）；
- 检出限（能够可靠检测的最低量值）；
- 被测量信号值的精密度（重复性、再现性）。

- c) 定性检查确定分析物是否存在，并且报告阳性、阴性或不确定的结果。阈值和相关数据库可以定义阳性或阴性结果。假阳性结果或假阴性结果，可能影响诊断或治疗。

定性 IVD 医疗器械的性能特性可能包括：

- 分析灵敏度（含有分析物的样品中真阳性结果的比例）；
- 分析特异性（含有分析物的样品中真阴性结果的比例）；
- 诊断灵敏度（真实阳性结果在患有疾病患者中的比例）；
- 诊断特异性（真实阴性结果在无疾病患者中的比例）。

H.2.2.3 与患者安全相关的可靠性特性

当临床医生依据体外诊断检查结果做出紧急医疗决策时，如急诊或重症监护时，及时的结果与准确的结果同样重要。当需要时却不能得出结果可能延误必要的医疗干预。

IVD 医疗器械的可靠性特性可能包括：

- 系统可靠性（故障平均间隔时间、平均故障时间）；
- 组件兼容性（包括版本和关键公差）；
- 软件可靠性（无错误运行）；
- 试剂或控制品稳定性；
- 系统可用性（避免使用错误）。

H.2.2.4 与患者安全相关的数字信息技术特性

对患者和样本的正确识别显然是必须的。有些检查还需要关于患者、样本或检查的辅助信息，以便正确解释结果。如果 IVD 医疗器械被设计为收集、存储和报告这些和检查结果在一起的信息，则导致数据损坏或更改的器械特性可能导致误诊或不适当的治疗。

临床医生需要的辅助患者信息可能包括：

- 正确的患者姓名和样本识别信息；
- 患者详细信息（年龄、性别、群体、遗传因素、药物、营养状况）；
- 样本详细信息（样本类型、描述、采集时间）；
- 测量详细信息（测量程序、测量单位、测量不确定度）；
- 使用详细信息（阈值、参考区间）。

可能影响患者安全的数字信息技术特性包括：

- 设备和/或网络（无线或有线）之间的连接；
- 互联网数据传输；
- 与数字应用程序的接口（互联网或移动网）；
- 模拟 IVD 医疗器械结果的应用程序；
- 嵌入式软件应用程序（例如解释或治疗建议）；
- 无屏蔽的数据传输（例如静电放电（ESD）敏感性）；
- 数字化信息的存储（例如易受损坏、操控或删除）；

——其他的连接设备的中断（产生额外的危险）。

H.2.3 对患者已知的和可预见的危险

H.2.3.1 危险识别

从患者角度看，如果IVD检查结果可能导致：（1）可能造成伤害的不适当的医疗干预；（2）缺乏必要的医疗干预以预防伤害，则IVD检查结果将被视为危险。以下概括性的危险可能引起或促成潜在的有害医疗决策。具体的危险宜根据错误的程度和导向、延误的程度，或者不正确的或缺失的辅助信息来确定。

除了对于IVD医疗器械自身的危险识别，还宜评价与连通性相关的危险识别。越来越多的IVD医疗器械直接或通过计算机网络，无线技术或互联网连接到其他器械和系统，对其安全运行带来新的挑战。随着连接器械的使用日益增多，以及IVD医疗器械产生的健康信息的频繁电子交换，确保有效的IVD医疗器械功能和安全的需求变得越来越重要。识别由于连通性而可能导致下述危险的失效，宜作为IVD医疗器械风险管理过程的一部分。

a) 不正确的检查结果

对于定量和半定量检查，如果与正确值的差值超出临床应用所需的误差限度，则可认为结果是不正确的，分析性能要求通常在设计输入过程中建立。

一些医学决策可能会受到检查结果大小的影响，因此不正确结果的临床意义可能取决于测量值与真实值之间差异的大小。

对于仅提供阳性或阴性结果的定性检查程序（例如HIV和妊娠检查），检查结果为正确、不正确或不确定。

b) 延迟的检查结果

如果医疗决策需要检查结果或其辅助信息，并且临床医生没有及时收到这些信息以支持关键的治疗或干预决策，则认为检查结果和其辅助信息是延迟的。可以建立标准定义什么是医学应用（例如紧急护理情况）的临床显著延迟。

c) 不正确的随附结果信息

与体外诊断检查结果一起提供的辅助信息错误的后果取决于该信息在临床决策中如何使用，以及该错误是否会导致或促成伤害。

H.2.3.2 故障条件下的危险的识别

IVD医疗器械在使用过程中发生故障可能导致H.2.3.1中定义的一种或多种危险。可能导致危险的故障情况包括：

- 批内或批间不一致性（例如试剂、校准品、质控品）；
- 不可溯源的赋值（例如校准品、标准物质、质控品）；
- 试剂非特异性（例如干扰因子、抗体）；
- 样本或试剂携带污染物（例如移液器）；
- 测量不精密度（例如系统水平）；
- 不稳定的材料（例如运输、贮存或使用期间）；
- 系统故障（例如硬件、软件、组件、附件）；
- 数字技术故障例如：
 - 软件/硬件易被入侵（例如数据更改或被窃）。
 - 数据传输引发的不正确或丢失的结果，不适当的治疗建议，或者由于环境状况引发的失效而造成的延误（例如静电放电，EDS）；
 - 连接引起的被连接医疗器械的功能损坏，对患者造成不安全情况；

- 数字应用程序错误地连接到另一设备或者数字应用程序；
- 数据存储损坏造成的不正确信息或延误的结果；
- 由于失去网络连接引起的结果或患者信息的可利用性延误。

当IVD医疗器械使用数字应用软件时，故障导致的结果延误包括：

- 智能器械操作系统的变化，引起应用不可得从而引发治疗延误，或者是在非预期行为中引起的不正确治疗建议；
- 智能器械数据存储能力或者数据传输速度的局限，引起的治疗延误或者不正确的治疗建议；
- 应用程序与智能器械之间的时间不协调，导致治疗延误或者不正确的结果（特别与显示过期结果有效相关）。

H. 2. 3. 3 来自正常使用的危险的识别

尽管所有的警告、注意事项和使用说明都得到遵守、医疗器械的功能符合预期、分析性能符合制造商的宣称，IVD医疗器械技术的固有局限性有时仍可能导致H. 2. 3. 1中描述的一种或多种对患者的危险。每个检查结果都会受到不可避免的变化来源的影响。即使分析性能已经过优化以最大限度地降低风险，正常使用中的偶然结果仍可能成为个别患者的危险。

正常使用中发生的潜在危险可能包括由于以下原因导致的不准确的结果：

- 由统计所赋的截断值的不确定性引起的定性检查程序的固有假阴性和假阳性率；
- 与定量检查程序有关的测量不确定度（性能宣称通常代表95%的测量结果处于医学定义的目标限值内）；
- 将结果错误分类为“异常”或者超出“正常”参考区间（依据经验确定的“正常”群体研究中的95%的中心结果而）；
- 样本中干扰物质的影响（例如交叉反应抗体、某些药物或生化代谢物或样本制备材料）；
- 分析物本身的生物学变异性（例如天然蛋白质的异质性、正常分析物浓度的种群差异）；
- 分析物自身的化学特性（例如固有的不稳定性、粘着性）；
- 患者样本基质的多变性（即“基质效应”）；
- 仪器组件有限的可靠性。

注：医学上定义的性能要求考虑了在预期患者群体中检查结果的统计分布。正常使用中发生危险情况被认为是剩余风险不可避免的/消除不了的贡献。

H. 2. 3. 4 来自使用错误的危险的识别

使用错误可能导致一个或多个H. 2. 3. 1中描述的危险。非常规的实验室过程可能尤其容易导致使用错误。在IVD医疗器械设计和开发中，可合理预见的使用错误（即由易于预测的人的行为导致）能够通过可用性工程过程予以识别并可能预防。有关信息和指南见IEC 62366-1^[16]。

在医学实验室或护理点潜在导致IVD危险的使用错误包括：

- 忽视特殊要求（例如在常规实验室程序之外）；
- 未按顺序执行操作，包括检查前和检查后的过程（例如不清晰的操作说明，混淆的用户接口）；
- 数据输入错误（例如患者姓名、身份证号码、出生日期或年龄、性别等）；
- 患者进行自我测试时的使用错误可能包括：
 - 样本量不足（例如量太少无法准确测量）；
 - 未正确装载试剂（例如在器械准备就绪用于测量前）。

H. 2. 3. 5 可合理预见的误使用导致的危险的识别

可用性工程过程还能帮助IVD医疗器械制造商预防可合理预见的误使用引发的危险和危险情况。指南见IEC 62366-1^[16]。

可合理预见的误使用的示例如下：

- 在阅读说明书或完成培训前使用 IVD 医疗器械；
- 无视警告、说明或其他安全信息；
- 采集不适当的样本类型（例如应为枸橼酸钠血浆时但使用血清）；
- 报告的检查结果用于禁忌的或未经确认的临床用途；
- 在重症监护场所使用自测 IVD 医疗器械（例如准确度可能不足）；
- 使用未经验证的第三方校准品、试剂、质控品或者附件；
- 在不正确的条件下贮存材料（例如应冷藏但使用室温）；
- 在规定的的环境条件之外操作 IVD 仪器；
- 禁用、不理睬、或未能启用安全特征（例如以减少用户的烦恼）；
- 忽视进行规定的仪器维护；
- 连接至不具备充分的网络连接和信息安全的信息系统；
- 恶意造成不正确结果或延迟治疗，包括：
 - 被第三方应用程序或个人强行控制并冒充器械以改变结果、在连接的数字应用程序上产生不正确结果；
 - 破坏器械软件配置，产生不正确的结果；
 - 在传送过程中拦截数据从而延误结果或者向用户发送不正确的结果。

患者进行自我检测时，可合理预见的误使用可能包括：

- 分割或重复使用试剂条（例如为降低成本）；
- 从替代部位获取样本（例如由于疼痛而从指尖以外的地方）；
- 静脉穿刺部位未进行清洁消毒（例如可能发生污染/感染）；
- 在不适当的环境条件下贮存试纸条（例如过热的车辆）。

H.2.4 潜在伤害的识别

GB/T XXXXX—20XX/ISO 14971:2019要求制造商依据可能发生的伤害的概率和严重度，估计每种所识别的危险情况有关的风险。这就要求制造商以足够的特异性识别出对患者潜在的伤害（例如损伤）以对严重度适当地赋值。

对于某些检查，单一危险情况能导致几种不同的伤害，表现为一系列严重度。制造商宜确定将哪些伤害包括在风险分析中，以确保对健康和安全的保护，且将理由形成文件。所有经过合理判断可能发生的伤害都宜包括在内。如果生产和生产后的信息表明有其他伤害发生，可以将其增加到风险分析中。

注：识别潜在伤害进行风险分析和确定其严重度和发生概率，需要了解IVD检查结果的临床用途。因此，有资格的医学专家参与风险分析是必不可少的。

可能有助于识别和分类潜在伤害的问题包括：

- 预期用途是否是对严重疾病治疗的主要决定因素？如果是，误诊或不适当的治疗可能会造成什么伤害？
- 预期用途是否涉及检测传染病病原体（例如甲肝或艾滋病毒）？如果是，假阴性结果是否会导致感染扩散到群体中的其他人？
- 预期用途是否用于检测和诊断遗传疾病（例如镰状细胞病、血红蛋白病携带者、易患阿尔茨海默症、乳腺癌风险增加等）？如果是，假阴性结果是否会导致可预防的或可治疗的疾病恶化？假阳性结果是否会导致不必要的医疗干预和潜在的伤害？

- 预期用途是否用于预测药物或器械的有效性?如果是,假阴性结果是否会导致治疗受益丧失和随后的伤害?假阳性结果是否会产生有害后果?
- 预期用途是否用于筛选输血或器官移植提供者?如果是,不正确的结果是否会导致疾病传播给受体或导致正常功能器官的排异反应?
- 预期用途是否用于监测关键的人体功能?如果是,不正确的结果或接收结果的严重延迟会带来什么伤害?
- 如发生医疗干预,结果不可逆(例如手术切除、堕胎)还是结果可逆(有无进一步的医疗干预)?
- 医疗器械是否需要连接互联网,是否会发生患者数据的更改或被盗(例如不充分的信息安全)?
- 确定伤害严重度的指南,见 5.5.4。

H.2.5 危险情况的识别

GB/T XXXXX—20XX/ISO 14971:2019要求制造商编制出一套全面的危险情况以用于风险分析,但由制造商确定危险情况的构成因素以进行风险分析(通用指南见GB/T XXXXX—20XX/ISO 14971:2019的附录C.4)。一种方法是评审事件序列。见H.2.6以识别(1)使患者暴露于危险中的事件或状况;(2)超出制造商或器械用户任何合理控制方式的事件或状况,以及(3)使制造商能够开展客观风险分析的事件或状况。

IVD医疗器械危险情况示例可能包括以下事件:

- 临床医生接收到不正确的实验室结果;
- 延误治疗(例如 IVD 医疗器械失效);
- 延误向临床医生报告紧急实验室结果;
- 不适当的治疗(例如基于错误的自测结果);
- 患者样本识别错误(例如由于使用错误);
- 随同患者结果一起报告的不正确的信息(例如由于网络失效)。

以下问题能够有助于分析与不正确结果相关的危险情况:

- 是否考虑到其他诊断指标的可能的情况下,导致 IVD 检查对象的健康情况的假阴性或假阳性结果仍然显得“可信”,因此在决定临床处置/不处置之前不会得到进一步确认?
- 是否很少、有限的或没有可获得的其他诊断工具来确认或否认潜在的假阳性或假阴性 IVD 检测结果?

H.2.6 可预见的事件序列的识别

H.2.6.1 总则

识别和分析可能导致危险情况和潜在发展为伤害的可合理预见的事件序列或者事件组合,对于估计可能发生的伤害概率是必要的。理解这些活动和事件还可以帮助制造商选择危险情况以进行风险分析,并识别降低风险和风险控制的机会。

拟分析的具体的事件序列取决于特定的IVD医疗器械及其预期用途。在概述事件序列时,制造商应考虑预期用户的知识、技能和能力、预期使用环境,以及任何可能增加风险或降低风险的事件和情形。

虽然医学实验室按照设计的用于检测错误的控制程序来运行,但制造商应考虑其在检测特定失效模式方面的有效性。零星的随机失效对于实验室来说尤其难以检测。经验丰富的临床医生知道这一点并质疑任何与其他可用信息或其临床印象不一致的结果。然而,如果错误结果貌似合理,如果它影响诊断或治疗决策,则可能导致不适当的或延误的治疗和对患者的潜在伤害。

IVD医疗器械的功能故障如果导致关键医疗决策所需的IVD结果的可获得性显著延迟,则会产生危险情况。虽然用户负有制定备份和恢复计划的主要责任,但器械失效可能是一个促成因素。与进行常规检查的实验室相比,临床上显著的延迟更可能发生在支持紧急护理的护理点或实验室中。

H.2.6.2 事件序列的描述

IVD医疗器械的风险场景通常涉及比其他医疗器械更长的事件序列。它们包括不受制造商直接控制的活动，例如由器械用户（例如医学实验室或护理点用户）执行的活动，以及由申请检查结果的临床医生做出的医疗决定和活动。

描述宜从初始事件（通常是正在分析的危險的原因）和直接受制造商控制的事件开始，通过器械用户可预见的决定和行动符合逻辑地进行，以导致所识别的每种伤害（作为可预见的结果）的临床决定和行动而结束。

描述宜尽可能详细，以涵盖主要的初始事件和促成事件，但不能过于详细，以免无关紧要的事件妨碍分析。制造商可以将复杂序列划分为较短的片段，以便由具备专业知识的人员进行分析。在H.2.7.2中讨论了这种方法。图表（如流程图、事件树）有助于记录和沟通复杂的事件序列。

a) 制造商控制的事件

导致危险情况的事件序列中的初始事件可能以制造商质量管理体系的失效而发生。故障条件或潜在使用错误可能由制造商直接控制的活动引起，例如：

- 设计和开发；
- 器械标记；
- 制造和供应商管理；
- 产品库存和流通；
- 设备维护；
- 培训和产品支持。

b) IVD 医疗器械用户控制的事件

使用错误和器械失效可能发生在实验室或护理点的器械运行期间。用于预防或探测危险的活动以及用户采取的响应措施由实验室或护理场所直接控制。这些器械用户将制造商提供的防护措施和安全信息纳入其自身的风险管理过程。

IVD医疗器械的用户也可能通过误使用导致或促成对患者的风险（见H.2.3.5），包括未能保持适当的质量保证程序、应急和恢复计划，或信息安全保护。向临床医生报告或不报告检查结果的决定完全在医学实验室或IVD医疗器械的其他用户控制之下。在分析IVD医疗器械用户控制下的事件序列时，宜考虑预期用户的能力和 Use 环境。

通常由用户控制的使用IVD医疗器械制造商提供的信息、材料和支持的活动示例包括：

- 与 IVD 医疗器械配套使用的样品采集器械的选择、使用和贮存；
- 患者样品的采集、处理和贮存；
- 系统的安装和建立（包括用户培训）、组件或耗材鉴定以及性能验证；
- 对附件、耗材和部件的选择、准备、使用和贮存（包括失效日期的管理）；
- 校准活动和计量溯源性；
- 质量保证活动（例如质量控制、能力验证、delta 检查）；
- 评审和报告检查结果；
- 与临床医生沟通（预期用途、禁忌证、召回结果、上市后监督）；
- 局域网络和互联网连通性；
- 生物危险废物处置；
- 设备维护、维修、最终停用和处置；
- 应急和恢复计划（例如备份系统）。

c) 临床医生控制的事件

临床医生控制的事件通常开始于接收和评审检查结果以及决定是否作为有效的结果而接受。较大的错误可能会被质疑和拒绝（例如与其他诊断信息相矛盾的结果、不符合生命的异常结果），但貌似可信的结果可能会被接受为有效的并且可能用于医疗决定。

注：临床决策被明确排除在范围之外，临床决策是指是否使用特定医疗器械或IVD医疗器械的临床决定，而不是指受不正确的或延迟的IVD结果影响的临床决定。

当在护理点使用IVD医疗器械时，如医生办公室、诊所或专科医院，临床医生通常参与患者样本的收集、处理、清点和贮存，并可能完成许多或全部的IVD医疗器械用户活动。在这种情况下，制造商通过随附文件中的安全信息影响临床活动的机会可能更大。为风险分析识别的事件序列宜反映IVD医疗器械在实际使用环境中的使用情况。

风险分析宜考虑任何可合理预见的临床用途。为了风险管理，随附文件中禁忌的或未明确说明的临床用途可被视为可合理预见的误使用。需要注意的是，为医学实验室的IVD医疗器械用户编写的随附文件并不总是能够送达申请检验和根据检查结果采取措施的临床医生。

通常由临床医生控制，可能由医学实验室指导和支持的决定和活动示例包括：

- 将结果与预期值进行比较；
- 要求确认或证实检查；
- 在无检查结果（如果延迟）的情况下推进；
- 建立临床诊断；
- 开始或停止治疗。

H.2.7 伤害发生概率估计

H.2.7.1 总则

风险分析宜考虑H.2.6.2中描述的整个事件序列。患者受到伤害的概率是与特定危险和潜在伤害有关的事件序列中每个事件的组合概率。估计伤害发生概率所使用的方法可能取决于事件序列的复杂性。一个重要的考虑因素是确保分析可以由具备与所分析的IVD医疗器械有关的适当的知识和专业特长（包括IVD医疗器械的分析用途和临床用途以及所涉及的技术）的人员进行。制造商可以将整个事件序列作为一个整体或分成部分进行分析，取决于何种方法更适合于客观的风险分析。H.7给出了将不同风险分析方法应用于常见IVD医疗器械场景的示例。

对于涉及短的事件序列的IVD医疗器械，例如自我检测或护理点的器械，风险分析可相对简单。可组建一个跨职能的专家团队，基于其专业判断，加上可获取的分析信息和临床信息（例如上市前的研究、类似产品的经验、相关的生产后信息），对每种所识别的危险情况下伤害发生概率进行估计。跨职能团队宜包括熟悉该器械的设计、结构、使用和维修、使用环境（如医学实验室、护理点、患者家中）以及检查结果临床用途的专家。对于设计的包含软件的与其他设备和/或互联网连接的医疗器械，团队还宜包括连接性和信息安全方面的专家。

对于复杂事件序列或事件组合，将危险情况的分析进行分段，通过将专家的专业知识和专门技能应用于相关事件序列的分析，可以更有效地利用专家资源。这被称为“ $P_1 \times P_2$ ”方法，在下面章节中有更详细的解释。

H.2.7.2 使用“ $P_1 \times P_2$ ”方法的特别指南

GB/T XXXXX—20XX/ISO 14971:2019图C.1所示的方法能够有助于具有延伸事件序列的复杂风险场景。例如，来自不正确结果的事件能够延伸出医学实验室至临床医生的决策和行动，这大大超出了实验室或制造商任何合理的风险控制方法。危险情况发生概率（ P_1 ）和危险情况导致伤害的概率（ P_2 ）由相应的专家分别估计。概率 P_1 与使用IVD医疗器械并且得出结果的实验室的分析相关，而 P_2 与临床医生对这一结果的使用和基于结果做出的决定和行动相关。综合这些概率从而获得伤害的总概率（ $P = P_1 \times P_2$ ）。

对于预期用于医学实验室的IVD医疗器械，事件序列可分为分析部分和临床部分，危险情况定义为向临床医生报告错误的结果、报告结果在临床上显著的延误或未能报告需要的结果。每个分段的概率可分别评估如下：

- P_1 是危险情况的发生概率；
- P_2 是危险情况导致特定伤害的概率。图 H. 1 说明了将“ $P_1 \times P_2$ ”方法应用于涉及 IVD 医疗器械的风险场景，在这种情况下血液分析仪在医学实验室进行血糖测量，该图描绘了整个事件序列，起始于制造商校准品赋值过程失效，结束于多种患者伤害的可能性。

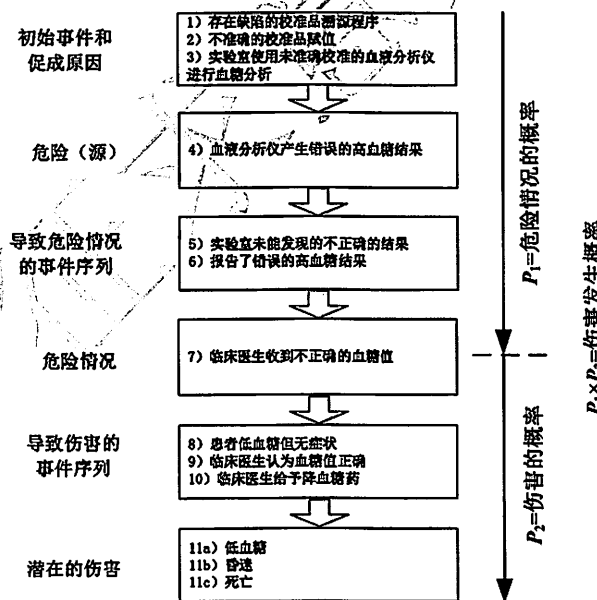
图H.1以医学实验室的血液分析仪进行血糖测试为例说明“ $P_1 \times P_2$ ”方法对IVD医疗器械的应用。图中描述的整个事件序列，起始于制造商赋值分配过程的失误结束于对患者多重伤害的可能。

该示例中的危险是由制造商不准确的校准品赋值导致不正确（假高）的血糖检测结果。本场景中的前两个事件处于制造商的控制之中，随后的导致危险情况的后续事件发生在实验室中，超出了制造商的直接控制，但这些事件可能由制造商在随附文件中提供的安全信息潜在控制。其余的事件超出了实验室的直接控制，因此本场景中的危险情况（即暴露在危险中）可以定义为超出制造商任何风险控制措施的事件。对于涉及不正确IVD结果的此类情况，要进行有效的风险分析，能够将危险情况定义为实验室报告和/或临床医生收到不正确的结果时发生的事件。

在此风险分析中，危险情况发生的概率（ P_1 ）和危险情况下导致伤害的概率（ P_2 ）可以由相应方向的专家分别估计。然后将这两种概率结合起来，给出伤害总概率的估计。

P_1 ：危险情况发生的概率

负责估计 P_1 的人员宜熟悉该IVD医疗器械的设计、结构、使用和维修，充分理解使用环境（如医学实验室、护理点、患者家中）。分析 P_1 事件通常不需要专业医学应用的详细知识。



图H.1 关于 IVD 医疗器械不正确血糖测量的实验室场景事件序列的说明

P_2 ：危险情况下发生伤害的概率

负责估计 P_2 的人员宜熟悉IVD结果的医学使用。可以根据不良事件数据、医学文献和生产后信息，利用专业临床判断和类似IVD检查的经验来对概率 P_2 进行估价。估计 P_2 时通常不需要详细了解IVD医疗器械的性能或结果是如何产生和报告的。

H. 2. 7. 3 估计伤害发生的概率的指南

表H. 1中的问题旨在促进对事件序列的系统性分析和指导开展适宜的概率估计。这些问题宜根据IVD医疗器械的类型、特定预期用途和所使用的风险估计方法进行适当调整。

问题1至问题4是关于的事件序列的分析部分，能够帮助制造商估计 P_1 。问题5至问题8是关于事件序列的临床部分，能够帮助制造商估计 P_2 。

表H. 1 帮助估计伤害发生概率的问题

有多大可能性……	考虑点
1. …发生初始事件（例如器械失效或使用错误）？	<ul style="list-style-type: none"> ——预防/探测措施的有效性如何？ ——能估计概率吗？如果不能，则设定概率=100% ——频次是否取决于使用环境？阐述最坏情况。 ——特定的故障、失效模式和/或使用错误是否会以可合理预见的组合发生，从而导致危险？
2. …IVD 医疗器械失效或使用错误产生不正确的结果？	<ul style="list-style-type: none"> ——旨在确保准确结果的措施的有效性如何？或者能否探测到分析性能不可接受的变化？ ——常规的质控程序是否会拒绝不正确的检查结果？ ——使用环境有何影响？分别分析不同的使用环境。 ——器械是否及时提示使用者纠正问题（例如：“血液不足”），以便在复检时取得有效的检查结果？
3. …不正确的结果或不正确的辅助信息被报告给临床医生？	<ul style="list-style-type: none"> ——是否对照危急值对异常的检查结果进行评审，或是否在向临床医生报告之前进行其他的验证？ ——报告前是否会对罕见的或非预期的结果进行确认（例如新生儿筛查程序）？
4. …报告检查结果（或辅助患者信息）时出现临床上显著的延迟？	<ul style="list-style-type: none"> ——结果对于及时的诊断或治疗决定是否关键？ ——延迟多久会造成危险情况？ ——排除功能故障或失控情况所需的时间是否会导致临床上不可接受的延迟？ ——确保及时获得结果的备份程序是否是标准实验室/标准医疗实践的期望？ ——能否在关键结果要求的时间内进行第二次检查并报告结果？
5. …临床医生相信不正确的结果是有效的？	<ul style="list-style-type: none"> ——临床医生是否会因与患者的临床状况不符、与其他临床数据相矛盾或生理上不合理而识别出结果不正确？ ——有能力的临床医生会质疑、重测或确证不符合临床印象的结果吗？ ——现行的医疗实践标准是否要求确认（例如对II型糖尿病的诊断进行两次独立的糖化血红蛋白（HbA1c）测量）？
6. …由于结果不正确出现不正确的医疗决定和/或干预（或缺乏干预）？	<ul style="list-style-type: none"> ——结果是否用于诊断、治疗或监测？ ——结果是否会成为做出特定医疗决定的主要依据？还是仅在体征、症状、其他检查结果和患者病史中使用？ ——阳性或“异常”结果是否总会导致特定的医疗决定或治疗，或仅会导致进一步的调查？ ——假阴性或假“正常”筛查结果是否会导致临床医生错过可治疗的身体状况？

表H.1 帮助估计伤害发生概率的问题（续）

有多大可能性……	考虑点
7. …因未能及时得到 IVD 结果而导致一个不适当的医疗决定或活动?	——鉴于临床医生可获得的体征、症状、病史和其他检查结果，这些结果在多大程度上用于指导干预或治疗?
8. …因不适当的医疗决定或措施导致对患者的伤害?	——对患者立即做出决定或干预有多紧急? ——在采取必要的措施中，不适当的措施或延迟会产生什么医疗后果? ——患者的状况会多大程度增加伤害发生的概率? ——对患者以外的人员是否有影响，例如： <ul style="list-style-type: none"> • 传染媒介向他人传播的可能? • 胚胎或胎儿暴露于致畸剂或辐射? • 由于不必要的暴露而产生微生物耐药性? • 移植器官的假排异反应? • 因错误诊断而导致需要家庭心理辅导? • 假阳性新生儿筛查结果导致父母焦虑?

H.3 风险控制

H.3.1 总则

由于临床医生的决定和行动大多不在制造商的任何合理的风险控制手段的范围内，因此风险控制活动宜侧重降低制造商控制下的事件的概率。这包括向实验室用户提供安全信息和验证安全信息的有效性。如果制造商使用 $R_1 \times R_2$ 方法，这意味着风险控制措施旨在降低 R_1 的概率。

H.3.2 固有安全的设计和制造

通常通过降低报告错误结果或发生临床严重延误的概率（例如通过确保性能特性满足医疗要求）来减少患者的风险。对于血糖、电解质、酶和治疗药物等分析物的定量测量，限制误差的大小可以降低不恰当的医疗决定的频次。

控制检查结果准确度和可靠性的设计特征的示例包括：

- 校准品值的正确度（例如对公认的参考标准的可追溯性）；
- 测量不确定度（例如测量系统的精密度）；
- IVD 试剂（例如优化组分）的分析特异性；
- 检测限或定量限（例如改进的测量技术）；
- 仪器的可靠性（例如减少硬件或软件失效）；
- 阳性和阴性样本的区分（例如稳定的阈值）；
- 消除容易出错的程序步骤（例如自动化、防错）；
- 组件版本可追溯性和阳性样本标识（例如条形码）；
- 软件的功能（例如最新技术水平的编码标准）；
- 系统易用性（例如可用性工程）；
- 数据网络和互联网连接（例如信息安全）；
- 降低试剂或校准品的可变性变（例如批次规格、供应商要求）；
- 防止虚假结果（例如间歇性的组件失效）；
- 试剂、校准品或质控物质的稳定性（例如微生物学控制）。

H.3.3 IVD 医疗器械或制造过程中的防护措施

IVD医疗器械或试剂盒预期用于预防能导致错误的或延迟的情况的探测特征示例包括：

- 液位感应器，以确保足够样本量（例如探测“吸取量不足”）；
- 故障探测系统（例如分光光度计漂移、不适当的温度控制）；
- 样本质量检查（例如溶血、黄疸、血脂）；
- 探测和去除样本中的人为干扰（例如泡沫或纤维蛋白凝块）的控制措施；
- 验证校准品或试剂批次是否正确的内置控制器（例如条码阅读器）；
- 提醒操作人员故障情况和恢复程序的报警和错误信息；
- 识别有疑问结果的，从而开展反向测试、评审或者让步的软件；
- 对供应组份的进货检验；
- 过程中的可接受性测试和最终产品的可接受性测试。

注：关于用户所实施的探测方法的建议，如质量控制测试、确认性检查或阈值提示，都被视为安全信息，而非防护措施。

H.3.4 安全信息

向IVD医疗器械的用户提供安全信息，目的为防止危险或危险情况发生。如果（1）此类信息指导用户采取或避免某些的行动，（2）预期用户能够遵循这些说明，以及（3）可合理预见用户将遵循这些说明，则安全信息能是一种有效的风险控制措施。宜明确忽视这些安全信息的不良后果。

安全信息能够用于医学实验室或其他预期用户的风险管理过程。使用户能够控制风险的安全信息的示例包括阐明下列内容的警告、说明和其他信息：

- 与 IVD 医疗器械有关的化学的或生物危险；
- 禁忌的医疗病症或临床用途；
- 样品收集、贮存和制备；
- 不恰当的样本类型的识别；
- 用户可探测到的干扰物质（例如可见溶血）；
- 危险原因，包括潜在使用错误；
- 不兼容的系统组件和附件；
- 拟安装 IVD 医疗器械的场地的公用设施（例如使用环境）；
- 试剂贮存不当和超效期使用；
- IVD 医疗器械的安装、服务和处置；
- 质控样品和频次；
- 当测量值高于测量区间上限时，经确认的测量区间和样品稀释说明；
- 生物参考区间和医学决策点；
- 经确认的可重复使用物品的清洁方法；
- 预防性维护程序；
- 接口和连接要求；
- 系统失效时的备份和恢复。

注：关于安全信息可以遵循法规或标准，如ISO 18113系列标准(所有部分)^[34]。

H.3.5 标准和分析性能准则的作用

少数的国际产品标准定义了IVD医疗器械的普遍公认的最新技术水平。例如ISO 15197^[28]（血糖自测器械）和ISO 17593^[32]（口服抗凝治疗的自我监测器械）。然而，一些IVD医疗器械标准涉及固有的某些方面，这能够提供证据，证明特定危险情况的风险已经降低到最新技术水平。

例如，ISO 17511^[31]规定了一个过程，用于建立IVD校准品的值到更高计量水平的参考物质的计量溯源性，这些参考物质定义了患者结果准确性的最新技术水平。检测医学溯源联合委员会（JCTLM）在<http://www.bipm.org/jctlm/>网站上维护IVD参考测量系统数据库。使用JCTLM批准的参考测量系统符合ISO 17511^[31]，能够提供制造商已将与检查结果准确性有关的风险降低到公认的最新技术水平的证据。

其他与风险控制潜在相关的IVD标准的示例包括ISO 17822-1^[33]（体外诊断测试系统 用于检测和识别微生物致病体的基于定性核酸的体外检测程序 第1部分：通用要求、术语和定义）、ISO 20776^[36]（临床实验室测试和体外诊断试验系统 传染者的易感性测试和抗菌剂易感性试验装置的性能评估 第2部分：抗菌剂易感性试验装置的性能评估）、ISO 20916^[37]（体外诊断医疗器械 使用人体样本进行临床性能研究 良好研究实践）、ISO 23640^[40]（体外诊断医疗器械 体外诊断试剂的稳定性评定）、IEC 61010-2-101^[11]（测量、控制和实验室用电气设备的安全要求. 第2-101部分：实验室诊断（IVD）医疗设备的特殊要求）、IEC 61326-2-6^[13]（测量、控制和实验室用电气设备 电磁兼容性要求 第2-6部分：特殊要求. 实验室条件下诊断（IVD）医疗设备），以及IEC/ISO 80001-1^[19]（风险管理在IT网络引入医疗器械时的应用 第一部分：角色、责任与活动）。

某些分析物公认的性能准则能在世界卫生组织（WHO）、国际和国家公共卫生机构、标准化组织、专业医学学会和监管机构的出版物中找到。

制造商有责任证明这些标准和性能准则适用于其特定IVD医疗器械及其预期用途的程度，并按照GB/T XXXXX—20XX/ISO 14971:2019的要求验证所有相关的危险情况均已得到考虑。

H.3.6 用户教育和培训

对于复杂的用户接口、困难的检查程序或关键的临床应用，安全信息可以采用制造商提供培训和教育方案的形式以帮助避免使用错误。也可以提供适用于持续教育方案的培训材料。

例如，口服抗凝治疗监测系统的产品标准（ISO 17593^[32]）要求制造商为临床医生提供确认过的培训方案，并为患者和这些器械的其他用户提供教育方案。制定国际标准的专家认为，这些风险控制措施是必要的，以确保在家庭环境中使用的风险是可接受的。

在确定由安全信息降低风险的程度时，考虑：

- 使用环境、器械用户的资质和能力可能存在很大差异；
- 世界各地的质量控制和质量保证实践不统一；
- 向IVD医疗器械用户提供的医疗使用禁忌和干扰药物的信息可能并不总是能传递到申请检查的临床医生。

H.4 受益-风险分析

7.4为实施受益-风险分析提供了指南。

如果无法直接描述IVD医疗器械的受益，可以建立替代终点。示例包括IVD医疗器械用于识别特定疾病、在疾病的不同阶段提供诊断、预测未来的疾病发作、和/或识别对给定治疗有反应的患者的能力。

H.5 剩余风险公开

H.5.1 总则

附录D解释公开剩余风险的目的是向器械用户、潜在的临床医生和患者提供信息，以便他们能够权衡使用IVD医疗器械的风险及其受益，并就风险可接受性做出明智的决策。制造商宜考虑医学实验室和临床医生所需要的信息，以评价固有的剩余风险，并确定进一步降低风险措施的必要性。

IVD医疗器械剩余风险的公开能够采取不同的形式，包括随附文件中提供的关于性能规格（“声明”）IVD医疗器械或检查程序的局限性、和/或制造商无法消除危险和危险情况的潜在原因。剩余风险的公开是对作为安全信息提供给用户的风险控制措施的补充。

注：随附文件中剩余风险的公开也可能在国家法规或标准有规定，如ISO 18113标准（所有部分）^[34]。

H.5.2 性能规范

对相关的分析性能特性和临床性能研究结果（见ISO 20916^[37]）的描述，允许医学实验室主任和临床医生来评价IVD医疗器械在其预期医疗应用中的效用。

性能特性的描述宜足够详细，以便实验室或其他用户能够：

- 验证 IVD 医疗器械能否按制造商所预期的运行；
- 确定与检查结果有关的测量不确定度；
- 了解检查结果将满足临床医生的医疗需求。

在实际或模拟使用条件下进行性能评价的结果可在随附文件中总结并呈现。

H.2.2.2给出了潜在相关的性能特性的示例。

H.5.3 IVD医疗器械的局限

ISO 18113-1^[34]要求随附文件公开IVD医疗器械的分析方面和临床方面的局限。这些局限描述了IVD医疗器械可能无法按预期执行的情况，因此可以作为公开剩余风险的一种方式。例如：

- 用户无法探测的干扰物质（例如药物、生物代谢物）；
- 性能特性可能不适用的特定患者群体；
- 超出测量区间的值（测量区间外的性能特性未经确认）；
- 参考区间或医学决策点可能不适用的患者群体；
- 对预期用途未经确认的原始样品类型；
- 可能影响检查结果但尚未被研究的情况和因素。

H.5.4 公认的使用局限

一些可能导致危险情况的事件或情形被认为是检验医学的常识。这些风险是通过标准的医疗或实验室实践来应对，通常不会在使用说明中描述以避免用户陷入不必要的细节。制造商宜考虑附加的信息是否适当以确保用户意识到与这些事件或情形有关的风险，谨记传递过多风险的危险，可能会使用户难以理解哪些风险需要重点控制。例如：

- 关于警告、说明和其他安全信息所隐含的理解是，不遵守这些可能导致危险和危险情况。不希望制造商特别将所有此类违规行为视作剩余风险。没有遵循明确的警告或说明被视为误使用（见H.2.3.5）。
- 预计机电设备偶尔会出现失效并需要维修，以及所使用的超过有效期的生物材料可能变得不稳定并失效。
- 预计实验室还将实施应急计划（例如备用系统或备用实验室）以确保在这些情况下提供必要的服务（见ISO 15189^[27]）。

H.6 生产及生产后活动

H.6.1 总则

建立有效的生产后信息（投诉、不良事件和产品不合格）监视系统对制造商来说是个挑战，特别是对预期在医学实验室中使用的器械，因为监视危险情况和伤害的实际频次的可靠数据可能很难获取。监视危险的发生及其原因更加直接，因为这种反馈可以由经历事件的器械用户直接提供。宜收集和分析器械失效、使用错误和医疗事故的报告，并将观察到的频次与预期频次进行比较（考虑繁忙实验室漏报的可能性）。

在建立生产后信息收集系统时，制造商可利用产品风险分析对预期的伤害、危险情况、危险及其原因制定一个分类和编码方案，有助于基于风险优先级的调查。事件可以根据所估计的潜在伤害的严重度以及不正确或延迟的结果将导致伤害的概率进行分类。该工具对投诉处置、上市后监督和不良事件报告以及产品失效调查是有用的。

H. 6.2 监视分析性能

收集IVD医疗器械生产和生产后信息的有效系统要求监视来自内部和外部可获得的分析性能数据。

性能数据的内部来源可以包括在产品放行测试、赋值活动、稳定性监视过程和产品失效调查中例行收集的生产数据。

性能数据的外部来源可以包括来自自愿参加外部质量控制和能力验证方案、用户性能评价以及仪器安装和服务活动所例行获得的数据。

H. 6.3 监视临床性能

医学实验室通常无法知道报告的结果是不正确的和可能已经导致不适当的医疗决定、干预或损伤，除非收到临床医生的投诉。因此，宜作为生产后活动的一部分认真监视任何报告的伤害严重度及其频次。

除了监视关于临床事件的顾客反馈，制造商还宜调查更多的来源，以了解类似产品发生的新的和突发的危险或危险情况。这些来源可包括由监管机构维护的不良事件和召回数据库，以及来自公共安全机构、国家医学实验室协会的报告和医学文献。

H. 7 IVD 医疗器械风险场景示例

H. 7.1 总则

下面的通用示例说明了常见类型IVD医疗器械造成的危险情况的不同风险分析方法。这些示例不预期代表唯一推荐的方法，也可能不适用于所有的此类器械或预期用途。IVD医疗器械制造商有责任决定对其器械使用适当的风险分析方法。风险管理计划宜将整个生命周期中使用的方法及其选择理由形成文件。

H. 7.2 医学实验室自动分析仪检查结果不正确

在此场景中，一个患者正在接受临床医生的诊断，医生从中央医学实验室预约体外诊断检查。如果IVD医疗器械产生的结果不正确并被报告给临床医生，导致伤害可能发生的事件序列如下：

- a) 初始事件发生（如器械故障或使用错误）；
- b) IVD 医疗器械产生临床上不正确的检查结果（即一个危险）；
- c) 器械使用者未能发现结果不正确（或其原因）；
- d) 器械使用者向临床医生报告不正确的结果（即危险情况）；
- e) 临床医生未识别到结果不正确；
- f) 不正确的结果误导临床医生误诊；
- g) 临床医生不适当地干预/不干预；
- h) 患者因临床医生的干预/不干预而受到损伤（即经受伤害）。

在上述的场景中，来自于不正确结果的危险的事件序列由医学实验室延伸到临床医生，临床医生的决定和行动在很大程度上超出制造商风险控制的任何合理手段。出于风险分析的目的，当临床医生收到不正确的结果时，患者可以被认为处于危险情况中，因为该事件后患者暴露于基于不正确结果的任何临床决定和行动带来的可能的伤害。

危险情况的定义允许将风险分析分为分析部分和临床部分，依据危险情况进行区分。每个部分可以由适当专家组成的跨职能团队独立地分析和记录，这些专家可以侧重于与其专业知识相关的事件。这两部分分析的结果可以组合得出伤害的总概率。

这种方法有效地利用了技术专家和医学专家。它还允许为风险管理文档创建临床风险分析报告，其可被用于发生设计更改时支持风险分析的更新，以及确定在生产后监视期间遇到的任何危险情况下的伤害发生的严重度和概率。

H.7.3 个人（自测）器械：不正确的血糖状态分级

在此场景中，被诊断患有2型糖尿病的患者定期监测其血糖浓度，并在结果显示高血糖时自行施用降血糖药物。虽然患者实际上是低血糖，但IVD医疗器械不正确地给出了一个升高的结果，并且降血糖药物导致患者的血糖进一步降低。导致伤害可能发生的事件序列如下：

- a) 初始事件的发生（如器械故障或使用错误）；
- b) 个人 IVD 医疗器械产生临床上错误的血糖结果（即一个危险）；
- c) 患者未识别结果不正确；
- d) 不正确的结果误导患者做出不适当的治疗决定（即一种危险情况）；
- e) 患者进行降血糖治疗；
- f) 患者出现明显的低血糖（即经受伤害）。

在上述的场景中，由于不正确的被升高的血糖测量引起对患者血糖状态分类不正确的事件序列主要局限于制造商控制下的事件以及患者基于制造商提供的安全信息的决策和活动。出于风险分析的目的，当发生可能直接导致伤害的事件时（如自行施用降血糖药物）则可以认为患者处于危险情况中。

在这种情况下，分割事件序列没有实际优势。整个风险分析可以由适当的技术专家和医学专家组成的跨职能团队有效地执行。

H.7.4 用于护理点的便携式IVD医疗器械：关键结果延迟

在此场景中，一名疑似内伤的患者正在紧急护理机构接受治疗，该机构进行IVD检查以评定潜在的器官损害。虽然操作人员遵照使用说明，但当临床医生需要决策是否进行紧急程序时，IVD医疗器械显示错误信息，无法获取结果。导致伤害可能发生的事件序列如下：

- a) 初始事件的发生（例如器械故障或使用错误）；
- b) IVD 医疗器械无法产生临床上必要的检查结果（即一个危险）；
- c) 器械使用者无法在要求的时间内重复检查；
- d) 临床医生未获得支持干预决定的结果（即一个危险情况）；
- e) 临床医生在无检查结果受益的情况下做出关键决定/行动；
- f) 医生的决定/行动不适合于患者的病证；
- g) 患者因临床医生的行动/未行动而受到损伤（即经受伤害）。

在上述的场景中，事件序列导致临床医生在没有评定内部器官损害的情况下执行紧急程序。出于风险分析的目的，当在需要时未收到预期结果，此后患者暴露在无检查结果受益情况下做出的临床决定和行动中，则可以认为患者处于危险情况中。

制造商可以考虑是将整个事件序列作为整体来分析还是将其划分为部分，宜基于哪种方法更适于客观的风险分析。

参 考 文 献

- [1] AAMI TIR57:2016, Principles for medical device security — Risk management
- [2] GHTF/SG3/N18 2010, Quality management system — Medical devices — Guidance on corrective action and preventive action and related QMS processes (available from <http://www.imdrf.org/documents/doc-ghtf-sg3.asp>)
- [3] GHTF/SG5/N4 2010, Post-market clinical follow-up studies (available from <http://www.imdrf.org/documents/doc-ghtf-sg5.asp>)
- [4] IEC Guide 120:2018, Security aspects — Guidelines for their inclusion in publications
- [5] IEC 60601-1, Medical electrical equipment — Part 1: General requirements for basic safety and essential performance
- [6] IEC 60601-1-2, Medical electrical equipment — Part 1-2: General requirements for basic safety and essential performance — Collateral Standard: Electromagnetic disturbances — Requirements and tests
- [7] IEC 60601-1-8, Medical electrical equipment — Part 1-8: General requirements for basic safety and essential performance — Collateral standard: General requirements, tests and guidance for alarm systems in medical electrical equipment and medical electrical systems
- [8] IEC 60601-2-16, Medical electrical equipment — Part 2-16: Particular requirements for basic safety and essential performance of haemodialysis, haemodiafiltration and haemofiltration equipment
- [9] IEC TR 60601-4-1, Medical electrical equipment — Part 4-1: Guidance and interpretation — Medical electrical equipment and medical electrical systems employing a degree of autonomy
- [10] IEC 60812, Failure modes and effects analysis (FMEA and FMECA)
- [11] IEC 61010-2-101:2015, Safety requirements for electrical equipment for measurement, control and laboratory use — Part 2-101: Particular requirements for in vitro diagnostic (IVD) medical equipment
- [12] IEC 61025, Fault tree analysis (FTA)
- [13] IEC 61326-2-6, Electrical equipment for measurement, control and laboratory use — EMC requirements — Part 2-6: Particular requirements — In vitro diagnostic (IVD) medical equipment
- [14] IEC 61882, Hazard and operability studies (HAZOP studies) — Application guide
- [15] YY/T 0664-2020/IEC 62304:2006 and AMD1: 2015, Medical device software — Software life cycle processes—Amendment 1
- [16] IEC 62366-1:2015, Medical devices — Part 1: Application of usability engineering to medical devices
- [17] IEC TR 62366-2, Medical devices — Part 2: Guidance on the application of usability engineering to medical devices
- [18] IEC 62502, Analysis techniques for dependability — Event tree analysis (ETA)
- [19] IEC 80001-1:2010, Application of risk management for IT-networks incorporating medical devices — Part 1: Roles, responsibilities and activities
- [20] ISO/IEC Guide 63:2019, Guide to the development and inclusion of aspects of safety in International Standards for medical devices

[21] ISO/DIS 10017, Quality management—Guidance on statistical techniques for ISO 9001:2015

[22] ISO 10993-1:2018, Biological evaluation of medical devices — Part 1: Evaluation and testing within a risk management process

[23] ISO 11608-1, Needle-based injection systems for medical use — Requirements and test methods — Part 1: Needle-based injection systems

[24] ISO 13485:2016, Medical devices — Quality management systems — Requirements for regulatory purposes

[25] ISO Handbook: ISO 13485:2016, Medical devices – A practical guide

[26] ISO 14155, Clinical investigation of medical devices for human subjects — Good clinical practice

[27] ISO 15189, Medical laboratories — Requirements for quality and competence

[28] ISO 15197, In vitro diagnostic test systems — Requirements for blood-glucose monitoring systems for self-testing in managing diabetes mellitus

[29] ISO 16142-1, Medical devices — Recognized essential principles of safety and performance of medical devices — Part 1: General essential principles and additional specific essential principles for all non-IVD medical devices and guidance on the selection of standards

[30] ISO 16142-2, Medical devices — Recognized essential principles of safety and performance of medical devices — Part 2: General essential principles and additional specific essential principles for all IVD medical devices and guidance on the selection of standards

[31] ISO 17511, In vitro diagnostic medical devices — Measurement of quantities in biological samples — Metrological traceability of values assigned to calibrators and control materials

[32] ISO 17593, Clinical laboratory testing and in vitro medical devices — Requirements for in vitro monitoring systems for self-testing of oral anticoagulant therapy

[33] ISO/TS 17822-1, In vitro diagnostic test systems — Qualitative nucleic acid-based in vitro examination procedures for detection and identification of microbial pathogens — Part 1: General requirements, terms and definitions

[34] ISO 18113 (all parts), In vitro diagnostic medical devices — Information supplied by the manufacturer (labelling)

[35] ISO/TR 20416, Medical devices — Post-market surveillance for manufacturers

[36] ISO 20776 (series), Clinical laboratory testing and in vitro diagnostic test systems — Susceptibility testing of infectious agents and evaluation of performance of antimicrobial susceptibility test devices

[37] ISO 20916, In vitro diagnostic medical devices — Clinical performance studies using specimens from human subjects — Good study practice

[38] ISO 22367, Medical laboratories — Application of risk management to medical laboratories

[39] ISO 22442 (series), Medical devices utilizing animal tissues and their derivatives

[40] ISO 23640, In vitro diagnostic medical devices — Evaluation of stability of in vitro diagnostic reagents