

ISO/TC210 N1089 (2019-04-30)

ISO/DTR24971: 2019 (E) 翻译稿:

医疗器械——ISO14971 应用指南

目 录

前言

引言

1. 范围
2. 规范性引用文件
3. 术语和定义
4. 风险管理体系通用要求
 - 4.1 风险管理过程
 - 4.2 管理职责
 - 4.3 人员资格
 - 4.4 风险管理计划
 - 4.5 风险管理文件
5. 风险分析
 - 5.1 风险分析过程
 - 5.2 预期用途和可合理预见的误用
 - 5.3 识别安全性相关特征
 - 5.4 识别危险和危险情况
 - 5.5 风险评估
6. 风险评价
7. 风险控制
 - 7.1 风险控制方案分析
 - 7.2 风险控制措施实施
 - 7.3 剩余风险评价
 - 7.4 受益-风险分析
 - 7.5 风险控制措施引起的风险

7.6 风险控制的完整性

8. 综合剩余风险评价

8.1 综合剩余风险评价的一般考虑

8.2 综合剩余风险评价的输入以及其他考虑

8.3 综合剩余风险评价的可能方法

9. 风险管理评审

10. 生产和生产后活动

10.1 信息收集

10.2 信息评审

10.3 措施

附录 A (资料性附录) 危险源和安全相关特征识别

A.1 总则

A.2 问题

附录 B (资料性附录) 风险分析技术

B.1 总则

B.2 预先危险分析

B.3 故障树分析

B.4 事件树分析

B.5 失效模式及效应分析

B.6 危险与可操作性研究

B.7 危险分析和关键控制点

附录 C (资料性附录) 风险可接受性考虑

C.1 风险等级

C.2 风险控制选项分析

C.3 可行性考虑

C.4 示例

附录 D (资料性附录) 安全信息与剩余风险信息

D.1 总则

D.2 安全信息

D.3 剩余风险披露

附录 E (资料性附录) 国际标准在风险管理中的作用

E.1 总则

E.2 国际产品安全标准在风险管理中的运用

E.3 国际过程标准与 ISO14971: 20XX

附录 F (资料性附录) 安全相关风险指南

- F.1 安全风险管理中使用的术语
- F.2 ISO14971: 20XX 与安全风险之间的关系
- F.3 健康风险与安全风险之间的关系
- F.4 健康风险与安全风险的区别
- F.5 保密性、完整性、可用性优先顺序

附录 G (资料性附录) 未采用 ISO14971 设计的部件和器械

- G.1 总则
- G.2 风险管理计划
- G.3 风险管理文件

附录 H (资料性附录) 体外诊断医疗器械的指南

- H.1 总则
- H.2 风险分析
- H.3 风险控制
- H.4 受益-风险分析
- H.5 剩余风险披露
- H.6 生产和生产后活动
- H.7 体外诊断医疗器械风险情况举例
- H.8 使用数字技术的个人体外诊断医疗器械特别指南

参考文献

前 言

国际标准化组织 (ISO) 是由各国标准化团体 (ISO 成员团体) 组成的国际性联合会。ISO 的技术委员会通常进行国际标准的制定工作。各成员机构若对某技术委员会已确立的项目感兴趣, 均有权派代表参加该委员会的工作。与 ISO 保持联系的各国际组织 (官方的或非官方组织的) 也可参加有关工作。ISO 与国际电工委员会 (IEC) 在电气技术标准方面保持紧密合作的关系。

ISO/IEC 指令的第 1 部分描述了用于开发本标准以及进一步维护本标准的过程。应特别注意不同类型的 ISO 文件需要的批准准则不同。本标准的起草符合 ISO/IEC 指令, 第 2 部分: 编辑规则 (见 www.iso.org/directives-and-policies)。

本标准的某些元素被注意到可能涉及专利权。ISO 不应负责识别任何或者所有此类专利权。在编制文件过程中识别的任何专利权的细节将列入引言和/或 ISO 已收专利声明的清单中 (见 www.iso.org/patents)。

本标准中出现的任何商品名称是为了方便用户而提供的信息并不代表认可。

关于标准自愿性的解释以及与符合性评价相关的 ISO 特殊术语和表达方式的含义, 以及 ISO 在技术性贸易壁垒 (TBT) 方面遵守世界贸易组织 (WTO) 原则的信息, 请参阅以下网址: www.iso.org/iso/foreword.html。

本标准采用 ISO/TC210 技术委员会、医疗器械质量管理和通用要求技术委员会和 IEC/SC62A 技术委员会、通用电气技术委员会医用电气设备通用安全分会体外诊断系统及医学实验室检验标准化委员会联合编制。附录 H 与 ISO/TC212 技术委员会、体外诊断系统及医学实验室检验标准化委员会联合编制。

本标准的第二版废除并取代第一版标准, 且在技术上做了修订。与第一版相比较, 主要的变化如下:

- ISO/TR24971: 2013 条款和 ISO14971: 2007 的一些资料性附录进行融合、调整、技术性修订并补充附加指南。
- 为了鼓励使用, 本标准中的条款和子条款采用了与 ISO14971: 20XX 相同的结构和编号。资料性附录包括风险管理具体方面的其他指南。

引 言

本标准为制造商在开发、实施和保持医疗器械的风险管理过程中提供指南帮助, 以期满足 *ISO14971: 20XX, 医疗器械 风险管理对医疗器械的应用* 的要求。本标准为 ISO14971: 20XX 在各种医疗器械上应用提供指南。这些医疗器械包括有源的、无源的、植入的和非植入的, 以及作为医疗器械的软件和体外诊断医疗器械。

本标准中的条款和子条款采用与国际标准 ISO14971: 20XX 相同的结构和条款号, 以方便使用本指南来实现标准要求, 并在需要处 (考虑有用的情况下) 进一步细分子条款。资料性附录包括风险管理具体方面的其他指南。本指南由 ISO/TR24971: 2013 的条款和 ISO14971: 2007 的资料性附录组成, 并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。

本标准对制造商提供了能够用于开发、实施和保持符合 ISO14971: 20XX 标准的风险管理过程的方法。如果有能够满足 ISO14971: 20XX 的要求的其他方法, 亦可采用。

在判定本标准中指南的应用性时, 应考虑: 医疗器械的类型、应用的对象、如何使用这些医疗器械, 以及适用的法规要求。

1 范围

本标准依据ISO14971:20XX标准,为医疗器械风险管理过程的开发、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ISO13485:2016^[21]标准的体系,但在ISO14971:20XX中并无此要求。ISO13485:2016中的一些与风险管理相关的要求(第7章产品实现和8.2.1:监测和测量反馈),可以通过应用ISO14971:20XX来实现。请见ISO手册:ISO13485:2016,医疗器械应用指南^[26]。

2 规范性引用文件

本文参考引用了下列文件,这些文件的部分或者全部内容构成了本标准的要求。凡注明日期的引用文件,仅引用的版本适用于本标准。凡未注明日期的引用文件,其最新版本(包括所有修订本)适用于本标准。ISO14971:20XX,医疗器械 风险管理对医疗器械的应用

3 术语和定义

ISO14971:20XX中给出的术语和定义适用于本标准。可用于标准化工作的ISO和IEC术语数据库,网址如下:

—IEC 电子百科: <http://www.electropedia.org>

—ISO在线浏览平台: <http://www.iso.org/obp>

注:ISO14971:20XX中定义的术语主要源自ISO/IEC指南63:20XX^[20]ISO14971:20XX中定义的术语尽可能从ISO/IEC指南63:20XX^[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

ISO14971:20XX要求制造商应在医疗器械的整个生命周期建立、实施、记录和保持一个持续的的风险管理过程。ISO14971:20XX给出了这一过程的要求步骤和最高管理者的职责,在本标准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

最高管理者有责任建立并保持有效的风险管理过程,在ISO14971:20XX对最高管理者的强调是很重要的。最高管理者在组织内有权分配职责,设定优先事项和提供资源。组织最高管理层的承诺对于一个有效的风险管理过程是必需的。

如果一个大企业由多个独立的实体组成,如业务单位或部门,最高管理者可以是领导和控制这个实体实施风险管理过程的那些人。每个实体可以有本部门的风险管理过程(或流程)(以及质量管理体系)。

4.2.2 建立风险可接受性准则的方针

ISO14971:20XX要求最高管理者规定有关建立和评审风险可接受性准则的方针并形成文件。附录C提供了详细的关于如何规定此类方针以及应包括哪些因素的指南。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。

此方针允许每种类型医疗器械(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)。此方针也为如何建立综合剩余风险的可接受性准则提供了指导原则。

4.3 人员资格

保证指派合格人员是最高管理者的职责。表1中列出了可承担特定风险管理任务的人员的示例，以及支撑有效完成列出的任务相关知识和经验。

某些风险管理活动可以由外部咨询人员或者专家来完成。应记录所需的能力以及满足这些能力的客观证据。

考虑是否有必要在风险管理专家的教育中纳入以下专题：

- 医疗器械风险管理项目的管理；
- 伦理、安全、保障和法律责任；
- 风险和风险可接受性的概念；
- 风险管理和可靠性的概率和统计数据；
- 设计开发中的风险管理和可靠性；
- 相关标准和法规的使用；
- 风险估计包括确定伤害发生的严重程度和概率的方法；
- 风险评价的方法；
- 降低/控制风险的方法；
- 验证风险控制措施有效性的方法；
- 生产和生产后风险管理的方法

表1 人员资格及相关知识和经历示例

人员或职能	知识和经验
风险管理者	医疗器械风险管理过程
工程师或者科学家	医疗器械技术和功能
操作	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	临床评估方法和要求， 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
质量保障	质量管理体系和质量实践
包装、储存、搬运和分销	包装、储存、搬运和分销相关的危险和风险控制措施
安装、维护、服务和支持	安装、维护、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	数据采集过程、文献检索方法
参与评审和批准记录的所有人员	与评审和批准相关的职能领域专家

4.4 风险管理计划

4.4.1 总则

风险管理计划阐述：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、以及整个器械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参考其他文件，例如临床规划、生物学评价或可用性评价。

风险管理计划是一个“动态文件”，在医疗器械的生命周期内获得新信息时，需要进行评审和更新。即使最后一件医疗器械上市销售后，仍需要连续收集信息。风险管理计划的变更需要记录在风险管理文档中。

活动策划的程度和风险管理计划的详细水平应与医疗器械相关风险水平相符合。ISO14971:20XX中列出了风险管理计划的最低要求。制造商可以加入其它条款，如时间一日程、风险分析工具、或者是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

此范围识别和阐明医疗器械和其生命周期的各个阶段，计划中的每一个要素在这些阶段中可实施。

风险管理过程的一些要素适用于产品实现过程（医疗器械的设计、开发和生产）。其它要素适用于生产和生产后阶段（医疗器械的安装、使用、维护、停用和处置）。

4.4.3 职责分配

风险管理计划确定负责执行风险管理相关的特殊活动的人员或职能（见表1）。同时，风险管理计划确定有适当的权限评审和批准风险管理的决定和活动的人员。这可能指派熟悉该医疗器械（或医疗器械族）及其安全相关性的人员。这种分配可以纳入为特定的生命周期阶段和计划范围所覆盖的活动而规定的资源分配矩阵。

4.4.4 风险管理活动评审的要求

风险管理计划具体明确了在生命周期内，如何完成、何时完成一个特定医疗器械或者医疗器械族风险管理活动的评审。该评审包括评审方法、评审时机、责任人或者责任职能部门、需要参与评审人员以及对评审结果如何管理。策划风险管理活动评审的结果将列入风险管理报告（见第9条）。风险管理活动的评审要求可以是其它质量管理体系评审要求的一部分，如设计、开发评审（见ISO13485^[2]）。

4.4.5 风险可接受性准则

依据制造商的判定可接受性风险的方针，确定风险可接受性准则。当伤害发生的概率无法估计时，风险可接受性准则可以只依据伤害的严重度。这种准则对同类产品是相同的。风险可接受性准则可能是制造商已经建立的质量管理体系文件的一部分，可以参考风险管理计划（见ISO13485^[2]示例）。

在启动风险评价之前建立风险可接受性准则十分重要。否则，对准则的决定会受到风险评价的结果的影响。

4.4.6 评价综合剩余风险和风险可接受性准则的方法

评价综合剩余风险和风险可接受性准则的方法来自于制造商建立的风险可接受性准则的方针，针对开发的特定医疗器械产品上述方法和准则并且需要在风险管理计划中进行阐述。第8章列出了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

风险管理计划明确了完成ISO14971:20XX的7.2条款要求的两个验证活动。风险管理计划可以明确地或者通过参考其它的计划，详细说明验证活动。

风险控制措施实施的验证可以是设计评审、规范批准、质量管理体系中的设计和开发验证的一部分、或者质量管理体系中的其它方法。

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，需要收集临床信息、可用性研究等等，作为质量管理体系中的设计和开发验证的一部分。

4.4.8 与生产和生产后信息的收集和评审相关的活动

ISO14971:20XX要求制造商建立一个主动收集和评审医疗器械在生产和生产后与安全相关的信息的体系。因此，风险管理计划应包括建立这一体系所必需的活动。制造商需要理解收集到的信息通常庞大并且来自许多分散的来源。所以，需要采用稳健的过程来分析这些信息和识别那些易隐藏的趋势，从而得出适宜的结论和采取的措施。统计技术应在信息收集的过程中起到辅助作用。

这一体系主动收集和评审信息包括监视和接收来自使用者的反馈，例如抱怨和不良事件报告。此外，这一系统应包括主动征求使用者的反馈和收集其它信息。制造商应考虑这些活动的范围。

对于具备较长使用历史和低风险的医疗器械，有限的监测可能已经足够。对于具备新型治疗（例如新的预

期用途)或者创新技术和可能具备高风险的医疗器械,更加缜密的监视包括上市后的临床跟踪(PMCF)研究可能对理解医疗器械实际使用产生的事项有保障作用。进一步的指南请见第10章。

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中的一部分(见ISO13485:2016,第8.2章的示例^[21])。在采用一个已经建立的满足许多案例程序的同时,考量的医疗器械的任何特殊要求应在风险管理计划中形成文件。任何监测活动的细节和PMCF研究的细节也应在风险管理计划中得到规定。

对收集到的信息的评价的频率应与其风险相符合并取决于市场上的该产品数量、已报告的事件数量和报告的危害的严重程度。这种收集和评价应在该医疗器械的预计寿命期内保持。

4.5 风险管理文档

ISO14971:20XX要求制造商建立并保持风险管理文档,包括医疗器械从原始构思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。ISO14971:20XX中的独立条款明确了一部分应作为风险管理文档保存的记录和相关文件。风险管理文档应提供医疗器械生命周期任何阶段风险管理过程评审所需的必要信息。

风险管理文档可以按一个医疗器械或者一个医疗器械族进行构建或者组织。在医疗器械整个生命周期内及时收集风险管理记录十分重要,因为在整个生命周期内可能需要这些信息支持其他活动和决定,例如在生产和生产后信息评审或者审核期间。

风险管理文档是一个逻辑架构,它不需要实际包含所有所需的记录和相关文件。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,也可以以任何形式和媒体存在(硬拷贝,电子记录等等)。

ISO14971:20XX要求每种已识别危险进行的风险分析、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。可追溯性就是要求证明所有已识别的风险都在风险管理过程中完全解决。可以使用可追溯性工具检索风险管理文件中的每个文件,该风险管理文档规定了所识别的危险有关的信息。这种检索对已识别风险知识的管理和后续活动中如综合剩余风险评价以及生产和生产后的信息评审作用很大。获得新信息以及医疗器械发生改变时,应更新可追溯性系统。

注:关于未采用ISO14971:20XX设计的医疗器械构建风险管理文档的指南,请见附录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,在下面的子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用;
- 识别与安全相关的医疗器械特征;
- 识别医疗器械的危险和危险情况;
- 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用

预期用途应考虑的信息,例如:

- 预期的医疗适应症,例如治疗或诊断2型糖尿病、心血管疾病、骨折、不孕不育;
- 患者人群,例如年龄组(成人、儿童、青少年、老人),性别(男、女),或疾病状态;

- 身体部位或相互作用的组织类型，例如腿或臂；
- 使用者身份，例如患者、非业内人士、医护人员；
- 使用环境，例如家庭、医院、重症监护病房；
- 工作原理，例如机械活塞驱动注射器、x射线成像、磁共振成像、皮下给药等。

可合理预见的误用是指未按照制造商预期的方法使用医疗器械，但这种使用可能源于容易预测的人类行为。这包括使用错误（失误过失、疏忽或错误）、故意误用行为以及有意将医疗器械用于其它（医疗）应用，这些均并非制造商预期。可合理预见的误用事件能够在设计和开发期间通过模拟使用分析例如应用可用性工程过程，或在生产后阶段的实际使用分析予以识别。使可合理预见的误用在医疗器械整个生命周期内得以识别，包括设计活动互动，可使得制造商预见潜在误用的能力逐步增强。

可用性工程过程能帮助确定一个特殊误用是否可合理预见，例如通过可用性测试期间的观察。可用性测试可能揭示用户未按照制造商建议的方法使用医疗器械。不良的工作作风、未充分感知风险、对后果的认知有限或操作程序不明确，均可能会导致这种误用。

下面的例子描述了一例通过应用可用性工程过程来识别和分析可合理预见的误用事件。关于可用性工程的更多信息请查阅 IEC62366—1 和 IEC/TR62366—2^[17]。

示例：一次性医疗器械被设计为仅使用一次，但是一些使用者可能试图再次使用这医疗器械，这是可合理预见的。因此，请勿二次使用的警告包含在随附文件中。根据 IEC62366—1^[18]可用性工程的应用证明此安全信息是有效的，即使用者知道正确使用并理解医疗器械再次使用的风险。然而，可用性评价也显示一些用户可能不顾这信息而故意再次使用医疗器械。由于此行为可被视为在可用性工程过程（见 IEC62366—1 第 3.1 章^[18]）中的异常使用，依据 ISO14971: 20XX，这些来自再次使用的风险需要在风险管理过程中依据风险可接受性准则进行分析和评价。

5.3 识别与安全相关的特征

识别可能影响医疗器械安全的特征十分重要。这些特征可以是定性或者定量的并且可能受到一定限制。附录 A 中的问题涵盖了医疗器械的许多方面，可以帮助识别与安全相关的所有特征，最终目的是尽可能地识别与医疗器械相关的所有危险和危险情况。对于相似的医疗器械，评审现有的信息和文献，包括类似医疗器械的不良事件报告，也是很有帮助的。

制造商可以确定医疗器械的性能或功能，这些性能或功能是实现其预期用途所必需的或必要的，或可能影响安全，并考虑如果任何功能不能正常实现是否可能会出现任何危险情况。

5.4 识别危险和危险情况

5.4.1 危险

危险即伤害的潜在源。情况不同，危险的来源和类型有所不同。危险可以是电、移动部件、传染细菌、化学物、气体、尖锐边缘、强电流、温度、离子辐射。

与医疗器械相关的危险可能源于 5.2 条款确定的预期用途和可合理预见的误用以及 5.3 条款中确定的与安全相关的特征。ISO14971: 20XX 附录 C 提供的指南能够帮助识别危险和引发危险情况的事件序列。

5.4.2 危险情况

医疗器械只有在一系列事件发生时才会造成伤害，因为事件的发生导致危险的情况，进而导致或导致伤害。事件序列可能包括按时间顺序的因果序列以及并发事件的组合。当人员、财产或环境暴露在一个或多个危险时，危险情况发生。

即使没有故障，也可能出现危险情况，即医疗器械在按预期执行时处于正常状态。危险情况可能是一些治疗的内在方面，例如，体外自动除颤器（AED）向患者施加电击，这是正常操作的一部分。类似地，伤口灼烧术在伤口部位施加高能量以及手术刀有锋利的刀刃制作切口。

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，这些特征指南能帮助识别危险和危险情况。附录 B 对支持风险分析的几个技术提供了指南。附录 H 对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，故障的概率与伤害发生的概率是不同的。故障能触发事件序列但不一定导致危险情况。危险情况并不总是引起伤害。重要的是要了解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 随机故障引发的危险情况

随机故障是由于物理或化学因素引发的，例如腐蚀、污染、热应力和磨损。很多随机故障可通过给出一个数值来表示故障发生的概率，以下是一些示例：

- 部件故障，如电器部件中集成电路的故障；
- 体外诊断试剂受到污染引起的伴随时间退化；
- 医疗器械内或医疗器械上出现感染性或有毒的物质；

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，例如，无菌保证水平的应用，才能对生物学风险定量估计。

5.4.5 系统性故障引发的危险情况

任意活动中的一个错误均可引起系统性故障。当某些特定输入的组合或环境条件出现，将系统性引发一个故障，否则将保持潜伏。

导致系统性故障的错误可能发生在医疗器械的任何部分，例如在机电医疗器械的硬件和软件中。系统性标签错误可导致所有医疗器械出现使用错误。这些系统性故障可以在医疗器械的开发、生产或维护中的任何时间出现。以下是系统性故障的一些例子：

- 不正确的保险丝将无法阻止危险情况：设计时保险丝额定值错误；
- 软件数据库未提供数据库充满时的条件：如果数据库已充满，将不清楚软件会做什么，可能出现的结果是系统简单地用新记录替换旧记录；

—医疗器械生产过程中使用的液体沸点低于人体温度：在一定的情况下，残留的液体可能进入血液引起栓塞；

—肝炎化验中的抗体未发现病毒（新）变种；

—环境控制设计不当，导致被有毒物质或病原体污染；

—编写使用操作手册表明，如果按照指南执行例行维护，操作者可能会受到尖锐探针的伤害。

准确估计系统性故障发生概率是困难的，这主要有以下原因：

—测量系统性故障的频率是十分费力的。没有系统性故障的大量数据或与风险控制有关的参数，就不可能在结果上获得合理的置信度。

—尚无统一方法定量估计系统性故障发生率。

因为在这些情境下，风险估计是困难的，所以制造商不应将重点放在估计系统性故障的风险上，而应实施稳健系统预防可能导致危险情况或伤害的系统性故障。

5.4.6 安全漏洞引发的危险情况

本标准中的安全，包括网络安全以及数据和系统安全。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。此类情况可能引发一系列事件，最终可能导致伤害（患者受伤或财产损失），示例如下：

—机密性文件丢失可能导致个人健康信息泄露；

—完整性的丧失可能导致错误的实验室结果或医疗器械故障；

—失去可用性妨碍医疗器械关键功能的使用或引起医疗器械完全停用。

关于安全的进一步指南请见附录 F。

5.4.7 事件序列或组合

危险情况可以是多个独立事件的序列结果或者是多个独立事件组合的结果。图 1 阐述了这种情况。危险情况发生的概率 P 由产品的独立事件发生的概率给出。事件序列可能有导致不同危险情况的分支，不同事件可能导致相同危险情况，这些复杂性并未在图 1 中体现。

图 1 中的示例是一个电器危险和相关的医疗电器器械中的绝缘电线。这里有一个很小的概率：绝缘材料老化并且出现裂缝，这些裂缝使电线开放，下一个可能事件是使用者连接和启动这一医疗器械，从而（取决于使用者界面中的选择）开放的电线带有带电电压，也就是使用者暴露于在线电压 220V。这一事件序列的综合概率是 P 。

使用者实际触碰开放电线的概率可以被估计为 0.10。因为使用者将从在线电压中得到惊吓，不适的概率是 $P=0.10$ 。烧伤或者甚至于死亡的概率比较低（0.01 或 0.001）。

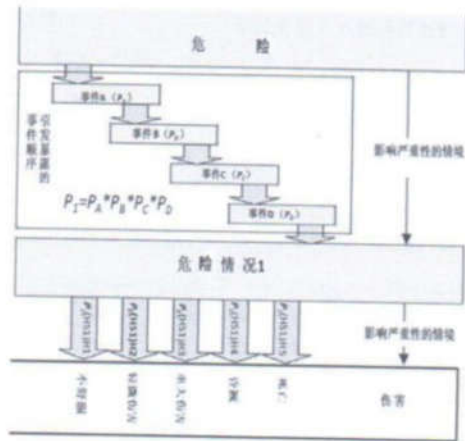


图1: 图示示例说明危险、事件顺序、危险情况和伤害之间的关系

危险情况 (HS1) 能够导致不同种类的伤害 (H1 到 H3), 范围从不舒服到轻微或重大伤害到昏厥或死亡。依据伤害的种类, 危险情况导致伤害的概率可能有不同的概率值, 这些值在图1中, 表述为从 $P_{2(HS1)}$ 到 $P_{5(HS1)}$ 。伤害的严重性受到暴露环境的影响。例如, 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, 取决于电压、电流、暴露持续时间和人体位置。

需要强调的是不仅严重性损伤的情况或者是损伤发生最高概率的情境需要考虑, 其它相关情境也需要。制造商应考虑何种方式记录危险情况是最佳的, 并描述能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不同类型的伤害。

市场上关于医疗器械的信息可用于风险估计。通常采用以下几种方法估计概率:

- 使用相关历史数据;
- 使用分析或模拟技术预测概率;
- 使用实验性数据;
- 可靠性评价;
- 生产和生产后信息;
- 专家判断使用 (这方面的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 ISO13485^[24])。

这些方法各有优缺点。在结果中为了增加可信度, 应使用互补的方法。专家的判断应尽可能地与一个或多个其他方法联合使用。当其他方法无法使用或不充分时, 可能需要完全依赖专家的判断。

5.5 风险估计

5.5.1 总则

风险估计可使用多种方法。虽然 ISO14971: 20XX 并未要求使用某一特定的方法，但确实需要进行风险估计。风险的概念是伤害发生的概率与伤害严重程度的组合，即伤害可能多么严重。风险估计应检查的因素，如：

- 危险发生的情境；
- 导致的危险情况的事件顺序；
- 危险情况出现的概率；
- 危险情况导致伤害的概率；
- 产生伤害的性质。

风险宜以方便风险控制决策的方式表示，例如，使用严重性和概率尺度。为了分析风险，应分别分析其构成部分，即概率和严重度。

图 2 中显示的风险图展示了已估计风险的分布情况，这对以后的决策非常有用。风险将在估计时绘制在图表上。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，但在很多情况中是有用的。如果一个风险图表或风险矩阵用于风险评级，则应证明特定的风险图表或风险矩阵以及使用的解释适用于该应用程序。

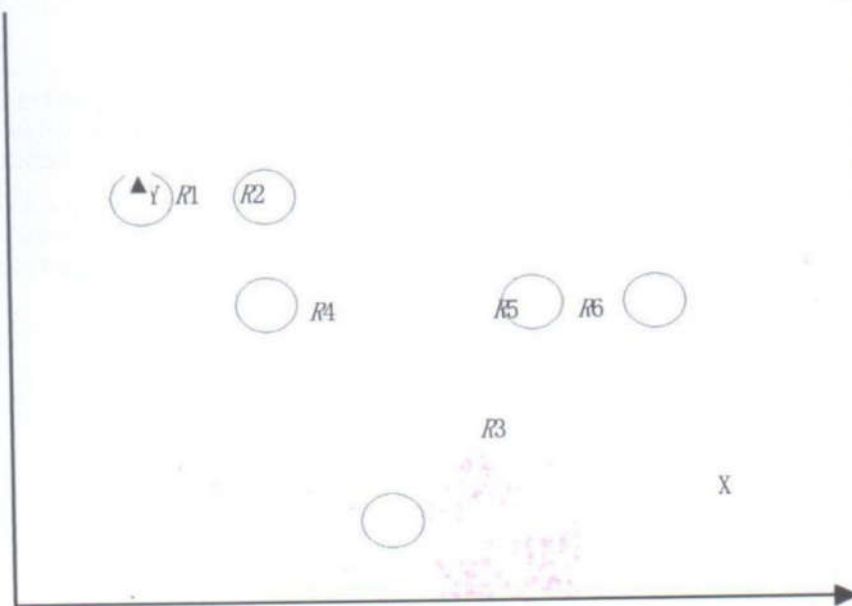


图 2—风险图示例：风险估计分布

5.5.2 概率

当可获得足够数据，确定伤害发生概率时，定量方法是首选。如果这是不可能的，制造商应使用定性方法。与高度不确定性的定量的方法比，这种方法更好。这种情况的一个示例是一个新的医疗器械，直到设计确认或当生产后数据能够得到以后，合适的定量的数据才能获得。对于一种定性方法，制造商能够使用适当的医疗器械的描述符。

虽然概率是一个连续的变量，但是在实践中为了简化分析，可使用一个离散的层级数字。制造商根据估计的预期置信度决定需要的概率层级。当以更大的可信度来估计时，要使用更大数量的概率层级。为了便于做决定，至少应识别出三个层级。层级可以是描述性的和定性的（如，医疗器械的生命周期内预计不发生、可能发生几次、可能频繁发生等），也可以是定量的。制造商应明确地规定层级，以便落在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。三个定性概率等级的示例和五个半定量概率等级的示例分别参见表 3、表 5。

不同的医疗器械族概率的规定范围可能不同。例如，制造商可以对一套 X-射线器使用一种规定，但对一次性无菌敷料也可以选择不同的规定。不同概率范围的适宜性取决于其应用。概率量表包括每次使用、每个器械、每小时使用，或者在一定人群中造成伤害的概率，等等。

分析概率发生时有几个重要的因素，包括但不限于下列因素：

- 特定医疗器械多久使用一次？
- 该医疗器械的使用寿命是多久？
- 使用者和患者人群的组成？
- 使用者/患者的数量？
- 使用者/患者暴露的时长以及在什么情境下暴露？

估计包括从初始事件发生的到损害发生的情境和事件序列。伤害发生的概率 P 可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 。参见 ISO14971: 20XX 中图 C.1。为了估计伤害发生的概率 P ，将其分解为 P_1 和 P_2 是有好处的，但是这样分解并非强制的。当伤害发生的概率被分解为 P_1 和 P_2 时，可能会出现其中一个能够被估计，而另一个不能估计的情况。出现以上情况，可以采取保守方法，即设置未知的概率等于 1。当估计的概率非常低以致由此产生的风险变得可以忽略不计，或者非常高到明显需要降低由此产生的风险时，这种方法可能是有用的。

5.5.3 无法估计概率的风险

在准确的和可靠的数据基础上或当合理的定性的估计是基于有资质的专家的判断，对发生伤害的概率作出定量估计时，风险估计的可信度被加强了。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，估计是极其困难的。当概率估计的准确性受到怀疑时，通常需要为概率建立一个较宽的范围，或确定它不比某个特定的值糟糕。概率很难估计的示例包括：

- 软件故障；
- 特殊的误用情况，如蓄意破坏或篡改医疗器械；

- 对新的危险认识不足，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，如遗传毒性致痛物和致敏剂，这种情况下可能无法确定不发生毒性影响的接触阈值。

当伤害发生的概率无法估计时，有必要仅根据伤害的严重度来估计风险。风险控制措施应侧重于整体防止危险情况或防止危险情况引发伤害。如果无法做到这一点，风险控制措施应侧重于降低伤害的严重度。

可以假设在设计、开发、生产和维护中使用的过程的严格性与被引入的或剩余未检测到的某些故障的概率之间成反比。考虑系统性故障结果的严重度和外加到医疗器械风险控制措施的有效性，可以确定这些过程所需的严密性。结果越严重并且外部风险控制措施越低效，这些过程应越严格。

5.5.4 严重度

为了对潜在伤害的严重度分类，制造商应使用适宜的医疗器械的描述符。现实中，严重度是连续的；然而，在实践中，使用严重度层级的离散数简化了分析。在这种情况下，制造商需要决定需要多少个类别以及它们是如何定义的。这些层级应是可描述性的并且不应包括任何概率的元素。参见表 2、表 4 中的示例。

严重度层级需要由制造商根据特定医疗器械可能造成受伤或其他伤害来选择和判断。严重度层级需要记录并充分定义其特性，以便能够正确分配伤害严重度的层级。

注：监管机构使用的术语可用于描述伤害的严重度。

5.5.5 示例

定性分析可用到几种方法。一个典型的方法是使用 N 乘 M 矩阵来描述关于每个危险情况相关的伤害发生的严重度和概率。认真地定义概率的 N 层级和严重度的 M 层级。矩阵的每个单元代表可能风险全集的一个子集。单元格是通过划分可能的概率范围和可能得后果范围来创建。

一个简单的例子是：基于表 2 三个严重性层级作为列，表 3 的三个定性概率层级作为行，来定义一个 3×3 矩阵。将估计的风险 (R_1, R_2, R_3, \dots) 填入到相应的单元格。结果如图 4 所示。为了确保其可再次使用，制造商应按需将这些特定器械明确定义。

表 2—严重度层级定性示例

通用术语	可能的描述
重大的	死亡或性能或结构丢失
适度的	可逆的伤害或轻伤
微不足道的	不会引起受伤或轻微受伤

表 3—概率层级定性简化示例

通用术语	可能的描述
高	可能发生，经常，频繁 医疗设备生命周期内可能多次发生

中	能发生，但不频繁 医疗器械生命周期内可能发生几次
低	不太可能发生、罕见、极少 医疗器械生命周期内没有可能发生

定性严重度层级

		微不足道的	适度的	重大的
定性 概率 层级	高	R_1	R_2	
	中		R_3	R_4, R_5
	低		R_6	

注：表 4 中估计的风险与表 1 中描述的不同。

表 4—3×3 风险矩阵定性示例

5×5 风险矩阵示例更为详细，其使用表 4 中的五个严重性层级作为列，表 5 中的五个半定性概率层级作为行。估计的风险 ($R_1, R_2, R_3 \dots$) 结果如图 5 所示。

表 4—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
严重的	导致永久损伤或不可逆伤害
重大的	导致需要医学或外科干预的伤害或损伤
轻微的	导致暂时的不需要医学或外科干预的伤害或损伤
微不足道的	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	$< 10^{-6}$

定性严重性层级

	微不足道的	轻微的	主要的	严重的	危急的
经常					
有时	R_1	R_2			
偶然		R_3		R_4	R_5
很少					
非常少			R_6		

图 5—半定量风险矩阵示例

除 3×3 或 5×5 矩阵外，也可使用其他矩阵；然而，多于 5 个层级的矩阵需要显著多的数据才能明显地区分不同层级。应记录选择矩阵及其结果分值的理由。请注意，具有三个层次的矩阵可能并不总是足够精确地进行适当的决策。虽然上面的例子是 3×3 和 5×5 时，但无需对这些矩阵平衡。例如，4×5 矩阵可适用于一个给定的应用。

6 风险评价

ISO14971: 20XX 规定了风险评价的过程。但此标准未规定可接受风险的层级。风险可接受性准则应基于制造商的判定可接受风险的方针和其在风险管理计划中的文件规定。

在风险评价中，制造商将估计的风险与可接受性准则进行对比从而决定这些准则是否得到满足。在风险评价中风险可接受性准则的应用示例与进一步的指南请见附录 C。

7 风险控制

7.1 风险控制方案分析

7.1.1 总则

用于降低医疗器械相关风险的若干方法既可单独使用也可联合使用。制造商须研究不同的方案，以合理可行的方式将风险降低到可接受水平，如 ISO14971: 20XX 中所强调的，优先顺序很重要。对此，下面的示例可以说明和阐述。

a) 达到固有安全的医疗器械设计：

—消除特定的危险；

例1 设计无锋利边缘的表面以消除潜在的割伤风险。使用手动操作泵而非电泵以消除潜在的电击风险。

—降低伤害的发生概率；

例2 不提供可接触的带电部件（带盖插头、插座、及连接器）以降低电击造成的震动伤害的概率。应用身份管理以降低未经授权而接触资料的概率。

—降低伤害的严重度；

例3 使用低功率发动机并低速移动部件以降低被挤压的伤害严重度。使用安全电气低电压（低于42 V）以降低电击伤害的严重度。

b) 通过下列方式采取防护措施：

—防止危险导致危险情况；

例4 采用自动切断或过压阀。对电线和电源单元进行保护性覆盖。用于移动部件或防止患者从桌上或床上跌落的保护装置。

—防止危险情况导致伤害；

例5 采用可视性或听觉性的警报向使用者警示危险情况。

c) 通过下列方式提供安全性信息：

—在医疗器械上给出警告；

—限制医疗器械的使用或限制使用情境；

—通知可发生的不适当使用、危险或其他有助于降低风险的信息；

—推广个人处理毒性或有害物质时使用个人防护设备，例如手套和眼镜；

—包括降低伤害严重度的措施的信息，例如危险物质造成污染后采取的措施；

—对使用者提供如何正确使用医疗器械的培训；

—对使用者在医疗器械生命周期内提供安装和维护的建议，例如维护时间间隔、最大产品预期服务寿命、善处置医疗器械。

方法a) ~c) 以通常公认的降低风险有效性的递减顺序列出了清单，制造商在决定使用哪种措施组合之前应考虑这些顺序和其他因素。

表6列出了不同医疗器械具体风险控制方案示例，更多关于安全信息的指南请见附录D。

在这一步骤中，固有安全设计和保护性措施的可能性解决方案的优势和劣势可以得到调研。设计解决方案的选择应基于这些调研。在此过程中会创造许多可能的设计解决方案和相关风险的知识。制造商应考虑如何保留这些知识，以备在将来应用。

表 6 风险控制措施部分示例

产品 / 过程	危险	危险情况	固有安全设计	防护措施	安全性信息
注射器（一次性使用医疗器械）	生物污染	在首次使用后再用于其他患者	使用后自毁	首次使用后的明显指示	对于再次使用和由于此种再次使用可能引起的不良后果的警示
植入式起搏器（有源植入物）	失效	由于电池的过早失效而使起搏器失效	使用非电驱动和控制	使用差分放大器和附加的滤波器算法	警告通常遇到的危险处境
机械式病患呼吸机	气压	软件失效引起的患者空气通道超压	吹管无法释放高压	呼吸机阀或者呼吸软管超压	建议只使用制造商运输的呼吸软管
IVD分析仪	系统错误或误差造成的错误结果	向临床医生报告的不正确结果	自我校准	提供可溯源的真实质控品	告知用户如何验证校准精度
X射线设备	离子辐射	员工暴露于流散辐射	无离子辐射操作（可行）	铅盾和铅围裙	占用区的辐射水平的信息

7.1.2 制造过程的风险控制

制造过程能够危及医疗器械的安全性，例如：

- 引入危险性残渣或微粒；
- 导致暴露于现存危险的错误，例如影响关键物理和化学材料特性，如表面涂层、抗拉强度、抗老化性、均匀性等；
- 超出临界公差；
- 在呼吸机的安装其间气体线路混淆；
- 部件焊接、粘合和连接完整性削弱。

医疗器械制造固有的安全性能够降低来自制造过程中的特定的危险从而确保此危险不出现在医疗器械中。制造过程中的保护性措施不一定能够降低危险但是可以预防危险对医疗器械的影响。检查和/或测试能够发现不符合并且防止受影响的医疗器械的分销。

失效模式和影响分析等技术(FMEA, 见附录B.5)和危险分析和关键控制点(HACCP, 见附录B.7)可以用来分析制造过程中的关键步骤。

考虑医疗器械生命周期其它阶段的风险控制也很重要，例如医疗器械的储存、分销、安装、维修、停用和处置。

注：应包括外包过程和对采购产品或部件的控制

7.1.3 标准和风险控制

通过应用标准，制造商可以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所有和医疗器械相关的风险。

许多标准阐述了医疗器械的固有安全、防护措施和安全信息。当存在相关的安全标准时，它们可以阐述一些或全部需要处理的特定医疗器械的风险。在缺少相反的客观证据时，制造商可以假定符合相关标准的要求就会使特定的风险降低到可接受水平。见附录E国际标准使用指南。

7.2 风险控制措施实施

ISO14971:20XX要求实施风险控制措施，对实施进行验证以及验证这些风险控制措施的有效性。

风险管理计划规定如何实施这两种不同的验证活动。风险控制措施的实施验证可从设计文档中获得。风险控制措施有效性验证可通过检测单个风险控制措施或通过例如适用性研究，收集临床数据等，来检测完整的医疗器械。风险管理计划可以明确地详述验证活动或引用其它验证活动计划。

7.3 剩余风险评价

采用与初始风险相同的方法并按照相同的风险可接受性准则评价单个剩余风险。剩余风险可以是可接受或不可接受。当进一步的风险控制不可行时，可以进行受益-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，可在医疗器械的整个生命周期内重复进行剩余风险评价。

7.4 受益-风险分析

7.4.1 总则

ISO14971:20XX允许制造商使用风险管理计划中制定的准则，对那些判定为不可接受而进一步的风险控制不可行的风险进行受益-风险分析。

受益-风险分析必须确定使用医疗器械的预期效益是否超过剩余风险。

考虑受益之前应考虑进一步降低风险的可行性(见附录C)。受益是否超过风险的决策本质上需要由有经验的和知识的人作出判断，通常是由医疗、临床与应用方面的专家组成的多学科团队做出判断。剩余风险可

接受性的一个重要考虑因素，就是是否可以通过使用没有风险或风险较小的替代方案来达到预期受益。这涉及到将制造商设计的医疗器械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预期使用医疗器械改善健康的可能性和程度有关。受益可对临床结果的积极影响、患者的生命质量、与诊断相关的结果、诊断器械对临床结果的积极影响或公共卫生的积极影响等方面进行描述。受益的性质和程度取决于患者群体。

有时受益可用产生积极效果的大小进行描述，比如体验受益的患者比例以及受益的持续时间。

受益可从对下列事项的了解程度加以估计：

- 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；
- 与其它治疗方案的风险和受益有关的因素。

受益估计的可信度严重地依赖于阐述这些因素的证据的可靠性，包括认识到受益估计的可能结果很可能是一个范围，还需考虑的其他因素如下：

- 比较不同的结果是有困难的，例如：疼痛与丧失活动能力哪一个更糟糕？不同于初始问题的各种副作用可引起不同的结果。
- 考虑不稳定的结果是困难的。这些结果可由恢复时间和长期效应引起。

由于采用严格的方法的困难，通常有必要做出简单化的假设。因此关注每一方案最有可能的结果及其最为有利的或最不利的结果，通常将证明是权宜之计。

应在策划中考虑下列各方面：

- 对病人或其它人期望的受益类型（例如，在一个给定的医疗情境下急救或者必需的医疗器械）；
- 预期受益的等级（例如，病人经历的治疗或诊断的受益的程度）
- 病人将经历的预期受益的概率（例如，医疗器械在治疗或诊断病人疾病或症状的可能性）；
- 预期效果的周期（例如，对病人的受益预期持续多久？）

受益的估计在设计过程的不同阶段可能是显著不同的。如果可以得到可靠的临床数据证明医疗器械的性能和有效性是一致的，就可以对受益进行可信估计。当临床数据在质和量上都是有限时，不论得到什么相关信息，受益估计具有更大的不确定性。例如有时需要在过程的早期，估计来自设计意图的预期健康改善程度；然而，在缺少相关的临床数据时，必须通过参考质量保证措施和体外或体内的性能特征的方法，来预测达到预期性能和期望的临床效果的可能性。

当重大风险出现、并且受益估计具有高度不确定性时，需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-风险平衡与预期的那样以及防止患者不必要地暴露于较大的剩余风险之中是至关重要的。ISO14155规定了医疗器械临床调查程序和ISO20916^[20]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策的技术、法规、经济和社会学背景。在预期的使用条件下，适用的法规或标准应用于所讨论的产品时，以上所说的理解和考虑可包括对适用法规或标准中陈述的基本要求的解释。由于这种类型的分析是和特定产品高度相关的，不可能有通用性质的进一步指南。换言之，阐述特定产品或风险的标准所规定的安全要求，可以被设想为和风险可接受水平是一致的，特别是在使用那些被现行的法规体系认可的的标准的情况下。需要指出，临床研究可能要求验证医疗受益和剩余风险的平衡是可接受的。

7.4.4 受益-风险比较

直接比较风险和受益是比较复杂的，应考虑以下内容：

- 预期患者疾病或状况的特性描述；
- 数据的不确定性。首先，文献检索所考虑的危险和医疗器械，可以对风险受益比提供重要的了解；
- 已上市医疗器械生产和生产后信息；
- 通过对比开发中的医疗器械的风险和受益与市场上可获得的类似医疗器械的受益和风险相比较，可以获得公认的最新技术水平。

ISO14971: 20XX要求制造商在风险管理文档中记录受益-风险分析的结果。建议记录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 在高频外科器械的回路电极不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烧伤的概率最小化，但仍有发生。然而，使用高频外科器械的受益和其它外科技术相比还是超过烧伤的剩余风险。

示例2 虽然大家知道X射线会对患者造成伤害，常规的诊断成像的临床有效性还是认为其使用是合理的。然而，辐射对患者造成的不必要影响是不可忽视的。现有标准要求患者暴露在不必要的辐射中减至最少。当出现电离辐射诊断成像新的应用与现有标准不适用时，制造商应当验证受益-风险分析的结果至少是和替代医疗器械和治疗的结果同样有利。

示例3 一些耳蜗的植入部件，例如带有电极阵列的植入式接收模拟器，一旦植入，就不能轻易更换。它们预期终生植入，并要求其可靠运行数年，甚至数十年。（这对于年轻人或儿童来说尤其重要。）可以为特定的故障器械进行这些部件的可靠性加速试验。然而，确认这些要延续几十年的部件的可靠性是不切实际的。因此，应将器械故障风险的综合剩余风险与潜在听力改善带来的受益进行权衡。综合剩余风险依赖于部件的估计可靠性和对不能被确认的那些部件的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 风险控制措施引起的风险

为减少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加其他风险，包括那些之前被评价为可接受的风险。例如，消除用户界面中的与某一使用相关的风险会限制使用者使用医疗器械的灵活性，并限制其干预危险情况的能力。第二个示例是为控制某一风险作出的软件变更会无意削弱嵌入在软件架构中的另一风险控制措施。制造商需要评审这些影响，以确保这些风险仍可接受。

可通过若干方法开展评审。对于“设计安全”的风险控制措施，制造商可以在详细或完整设计的风险分析中进行评审。对于制造过程的风险控制措施，制造商可以作为过程风险分析或过程验证的一部分进行评审。

7.6 风险控制的完整性

ISO14971: 20XX要求考虑所有已识别的危险情况，并完成所有风险控制活动。这可通过维护所有危险和危险情况以及相关风险的清单来实现。检查该清单确保所有已识别的危险情况已经得到考虑并且没有忽视任何风险。这一活动的结果应记录在风险管理文档中。

g) 应考虑单一风险的所有受益-风险分析。

h) 当在风险分析中出现对风险的取舍权衡时,应当特别关注对综合剩余风险的影响的分析。存在这样的示例,为了降低另外一个风险而某一个风险被允许提高。例如,对某人(如使用者)的风险允许被提高从而另外一人(如患者)的风险得到降低。这种评价可以采用检查相关重大风险,阐述判定这种取舍平衡的理由,以及在取舍决定中的综合风险水平的可接受的理由。

8.3 综合剩余风险评价的可能方法

用于评价综合剩余风险的方法可以包括下列措施和制造商认定适宜的方法:

a) 权衡与医疗器械预期用途相关的受益和综合剩余风险。受益可通过其大小或程度、预期患者人群中出现受益的概率以及受益的持续时间和频率来描述。评价应考虑预期医疗目标的知识、公认的技术和医学最新技术水平以及可供选择的医疗器械或治疗方法。

b) 剩余风险可视化很有帮助。每一个剩余风险可以在风险矩阵中表示,如图6和图7,图示化风险的分布。如果许多风险在矩阵的高严重度区域或者在高概率区域,或者风险簇在临界线附近,则表明这种分布的剩余风险不可接受,即使每一个单一风险已经判定可接受。

c) 制造商可以将考虑的医疗器械与市场上类似的医疗器械进行比较。主要问题是与类似医疗器械相比,考虑医疗器械的医疗受益是否具备可接受的综合剩余风险。医疗器械的剩余风险可以与类似医疗器械的相应的单一地进行比较,考虑其在预期用途方面的不同。类似医疗器械在预期用途和不良事件方面的最新信息应得到认真评审,包括来自科研文献的信息和临床经验的信息。

d) 制造商在考虑使用的医疗器械的预期受益时,可以请专家提供对综合剩余风险的输入。这些专家可以来自不同的领域并且应包括那些具备临床和使用相似医疗器械经验和知识的专家,且有关专家具备适当的独立性。他们可以帮助制造商考虑利益相关方的关注焦点。培训和经验的要求也应得到关注。

e) 即使所有的单一风险已经识别、控制并判定为可接受,但作为综合剩余风险评价的一部份,有些风险仍需进一步调查。例如,可能存在许多接近不可接受的风险。因此,认为综合剩余风险是不可接受的需进一步调查。

f) 当一些风险就其原因或所采取的风险控制措施互相关联时,也可能需要进一步的调查。应验证风险控制措施的有效性,不仅仅是单独地而是要综合其它风险控制措施。这也适用于旨在同时控制多种风险的风险控制措施。故障树分析或者事件树分析是证明风险和采用的风险控制措施之间存在关系的有用工具。

9 风险管理评审

为了确保风险管理计划得到恰当地执行,风险管理过程的最终结果需要评审,综合剩余风险是可接受的并且已建立合适的方法收集和评审生产及生产后信息的适宜方法。风险管理评审应在综合风险控制措施已经实施和验证后、医疗器械上市前实施。风险管理报告提供该评审的总结,并包含在风险管理文档中。

可能需要修改或更新风险管理报告,具体取决于生产和后期生产阶段可用的新信息。制造商需要确定风险管理计划实施情况的评审及更新风险管理报告的时机。通常在医疗器械的重大变更后,更新风险管理报告。

风险管理计划实施情况的评审不应与由最高管理者按照计划的周期对风险管理过程适宜性的评审混淆。风险管理计划与某一类医疗器械(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有关。

10 生产和生产后活动

10.1 总则

8 综合剩余风险评价

8.1 综合剩余风险评价的一般考虑

ISO14971:20XX要求依据风险管理计划中阐明的准则,对综合剩余风险进行评价。此处剩余风险在一个宽泛的视角中得到评审。基于受益-风险分析,对所有已识别的危险情况进行评价,所有风险均已降至可接受水平或已被接受。此时,制造商需要考虑与医疗器械相关的综合剩余风险是否满足综合剩余风险可接受性的准则。将所有剩余风险的贡献与医疗器械预期用途受益考虑在内,对于复杂的医疗系统和风险数量大的医疗器械特别重要,这种评价可以证明医疗器械是安全的。

综合剩余风险的评价是一件困难和具有挑战性的工作,它不能通过如数添加所有的单一风险来实现,因为每一个伤害发生的可能性与一个不同的伤害严重度有关。这些困难也来自下列原因:

一即使在医疗器械开发的后期阶段,对概率估计的可信度也会有很大的变化。一些来自同类医疗器械历史资料或者测试的概率很精确,而另一些概率只是估计并且不准确,例如专家的判断,或者都不是,如软件故障的概率。同时,不可能在宽泛范围的风险分析中综合众多单一伤害的严重度。

一单一风险的可接受性准则不需要与综合剩余风险可接受性准则相同。准则可以用于评价单一风险包括特定伤害的严重度可能性发生的概率极限。用于评价综合剩余风险的准则经常基于一些附加元素,如医疗器械预期用途的受益超出综合剩余风险。

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可以用来规定评价方法。本指南旨在帮助制造商建立此类准则和方法。

综合剩余风险的评价需要由具备知识、经验和权限的人员来完成。建议具备医疗器械使用知识和经验的应用专家参与。最终,这些评价需要依据具备必要的知识和临床知识的专家的判断。

综合剩余风险评价的结果构成部分风险管理文档。建议对综合剩余风险接受的理由说明形成文件。

ISO14971:20XX要求制造商告知使用者重大剩余风险,并提供披露剩余风险的必要信息。请见附录D剩余风险披露指南。

8.2 综合剩余风险评价的输入和其他考虑

综合剩余风险的评价可以对多个输入进行考虑。下面是输入和使用的一些示例。

a) 不同的事件序列可能导致的危险情况和风险不同,并影响综合剩余风险。例如,一次性使用医疗器械的再使用与再感染、有毒物质的滤过、老化和生物不相容消毒剂残留物引起的机械故障。事件树分析(ETA,见附录B.4)适用于这些风险分析,通过考虑和忽略伤害的概率或严重度来区分事件顺序。在综合剩余风险的评价中这些风险的影响需要综合考虑。

b) 一个对于患者或使用者的特定的伤害可能来自不同的危险情况。在这种情况下,伤害发生的概率可以用来确定基于单一概率组合的综合剩余风险。故障树分析(FTA,见附录B.3)是估计这种特殊伤害发生的概率组合的适宜方法。

c) 适用于独立单一风险的风险控制措施能够引起矛盾的要求,从而引起综合剩余风险的上升。例如,一个处理无意识患者从患者台上跌落的建议可能是“永远不要让一个无意识患者无人照顾”。这可能与“在进行X-射线拍照时请站在保护屏之后”的保护操作者暴露于x-射线的说明相冲突。

d) 一个警示本身被认为能够提供对单一风险的降低。当然,过多的警示能够降低单一警示的效果。可能需要判定是否存在对警示的过度依赖,以及这种过度依赖是否会影响风险降低和综合剩余风险。

e) 全面评审医疗器械的所有操作说明可能会发现,说明具有不一致性或者难以遵守,这也可能影响综合剩余风险。

f) 设计开发确认、可用性研究、临床评价和临床调查可以对综合剩余风险提供有用信息。来自企业家适宜的输入能够提供有用的信息。

	<ul style="list-style-type: none"> -按顾客（医生、医疗机构、患者等） -投诉理由 -投诉代码 -任何伤害的严重度 -涉及部件
服务报告	<ul style="list-style-type: none"> -安装 -首次使用的医疗器械 -维护访问的频率 -维修类型 -维修频率 -使用频率 -更换部件 -服务人员
风险管理	<ul style="list-style-type: none"> -发表的类似医疗器械故障的报告 -利益相关者的关注和普遍可受的最新技术水平 -风险可接受性准则
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"> -患者偏好 -服务响应时间 -索取有关新的或改装医疗器械的信息
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"> -商务期刊中的文章 -医疗信息网站 -贸易杂志、科学期刊和文献的文章
安全数据源	<ul style="list-style-type: none"> -独立安全研究者 -室内测试

生产和生产后信息的监测是确保医疗器械制造商关闭反馈回路和使风险管理成为持续的全生命周期过程。在该阶段，将收集许多不同来源的数据，针对安全性进行评审，恰当时，反馈到风险管理过程的前期阶段，以改进医疗器械的安全性。

制造商被要求建立主动收集和评价医疗器械与安全相关的信息的体系。建立此体系的必需活动必须包括在风险管理计划中（见 4.4.8）。

生产和生产后信息的监测可作为上市后监测体系的一部分，有些司法领域需要该体系。有关上市后监管的更多指南，参见 ISO/TR 20416^[26]。

注：该阶段可以与 ISO13485：2016 第 7 章和第 8 章的相关部分进行比较。ISO 手册（ISO13485：2016 医疗器械应用指南）提供了更多的指导。

10.2 信息收集

数据可能来自于许多来源，每个来源都可以影响医疗器械的安全性。制造商对开发和上市相似医疗器械越有经验，对医疗器械的性能、患者群和在医疗器械使用时出现可合理预见的误用越有一个良好的理解。

生产和生产后的活动可以包括接受关于医疗器械安全和性能的信息。来源通常包括来自使用者、服务人员 and 培训人员的总体反馈。这些信息可能与发生的伤害或者发生的损害或者是无损害的危险情况有关。这些活动也可以包括征集有关医疗器械绩效和相关风险的信息。这些活动可以有从企业所有者获取特殊信息和见解，采用顾客调查，使用专家组咨询（讨论组）以及制造商主导的医疗器械跟踪/植入注册。它也可以包括可获得的公众信息如临床文献、事件报告和和不良事件数据库。

这些活动可进一步包括在上市批准之后的上市后临床跟踪研究（PMCF），其目的是用来提升上市后的医疗器械的安全和功效的临床证据。PMCF 研究通常侧重与安全或者功效（如剩余风险）相关的问题，当医疗器械与其预期用途一致地进行使用时。临床调查的要求见 ISO14155^[25]而关于 PMCF 的深入指南见 GHTF/SG5/N4：2010。

收集到的信息不必与制造商的医疗器械直接有关而具有相同预期用途的其它产品，相同原理的操作或相同的危险也能够产生与制造商的医疗器械相关的风险的有用信息。

表 7 - 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"> -来自对供应商绩效/控制的监测的信息 -过程监测 -过程中的检验/测试 -内/外审
投诉处理	<ul style="list-style-type: none"> -数量 -按医疗器械族

—最新技术水平或者是医疗器械的受益发生变化。需要采取进一步的措施。

有关最新技术水平的变化，应关注对预期患者的医疗状况的诊断和处置的可获得的更替，包括这些更替的安全性、有效性以及相关的风险。对没有得到诊断和治疗的病人的风险和受益也应得到考虑。

制造商也应评价来自预期用途的参与受益或者变化。如果在受益变化时，风险保持不变，则受益与综合收益风险之间的平衡也发生变化。参见 7.4.2 对受益的估计的讨论。

统计技术可以被考虑用来帮助数据的处理，例如趋势分析、可靠性工程预测技术（如 Weibull 分析）和可靠性评价（如医疗器械或部件的失效测试、测试失败部件退回制造商，或者从同一批次或前一批/后一批次）。关于选择和使用统计技术的进一步指南见 ISO/TR10017^[21]。

10.4 措施

如果收集到的信息在得到评价后判定与安全相关，需要采取几项措施。其中一些措施与特定的医疗器械相关，同时其它的措施与风险管理过程相关。

如果呈现的危险或危险情况之前没有得到识别，相关的风险需要被评价和依据需要进行控制，按照 ISO14971:20XX 第 5 章到第 7 章相关步骤。风险评价的结果和实施的风险控制措施必须在风险管理文档中记录。

如果风险不再可以接受，这一特定风险的评价需要更新。已收集的信息对先前实施的风险控制措施的影响需要被评价，查看这些措施是否依旧有效和充分降低风险。这一评价的结果应作为医疗器械更新或提高的输入。如果需要，ISO14971 第 5 章到第 7 章的步骤应得到重复并且新的/附加风险管理措施必须得到实施。更新的风险评价和实施的风险控制措施必须记录在风险管理文档中。

可能需要再次评价与医疗器械预期用途相关的综合剩余风险。也可能需要重复风险管理评审和准备新的风险管理报告。见 ISO14971:20XX 第 8 章到第 9 章。

对某些医疗器械如果需要采取措施，制造商则应考虑：

- 已经分销（即超出制造商的控制范围）的：应考虑纠正或从市场上撤回这些医疗器械；
- 已制造但未分销（即仍在制造商的控制下）的：应考虑停止和纠正这些医疗器械；
- 将要制造的：应考虑改进医疗器械的设计和制造或维修过程的必要性。

对于目前市场上安装和使用的医疗器械，制造商应考虑在制定进一步的风险控制措施并验证其有效性之前，是否应将任何修订或附加信息作为临时措施（例如，ISO13485:2016^[22]中所述的忠告性通知）传达给使用者、患者和其它利益相关方。向用户和其它利益相关方通报新风险或增加风险的紧迫程度应与风险程度相称。在需要对已经使用的医疗器械进行封存、纠正或撤离的情况下，这些措施的速度决定了降低风险的有效性。这些采取的决定和措施应该记录在风险管理文档中。

信息评审的结果可以表明风险管理过程的不充分和不适宜以及这一过程需要的改进。因此，制造商需要评价收集到的信息对先前风险管理活动的影响，查看活动是否需要改进。这一评价的结果必须与最高管理者进行沟通。信息评审的结果可以作为最高管理者计划的风险管理过程的适宜性的评审的输入。最高管理者需要决定风险管理过程的哪个部分或者哪个方面需要改进从而确定其持续有效性。

	-供应商软件或硬件技术 -健康护理设施 -发布与医疗器械有相似技术的事件 -信息共享和分析中心 (ISAC)
--	---

图表 7 呈现了包涵有可用于分析和可能与安全性相关的生产和生产后信息的数据源。这一表格来自 GHTF/SG3/N18: 2010^[2]。

如果收集和评价信息是由不同的部门完成的, 制造商需要在这些部门建立有效的沟通和协调。

10.3 信息评审

收集的信息应得到评审来判断这些信息是否与安全相关。

下列问题可以对评审有所帮助:

- 预期用途是否还有效?
- 参与的受益是否取得?
- 是否有证据表明风险分析过程中最初未发现新的危险或危险情况? 例如, 是否发生了任何不可预见的伤害?
- 是否出现了以前没有预见的误用?
- 是否其有非预期用途的其它应用出现增长的趋势?
- 特定危险情况或损害出现的频率是否意味着损害发生的概率被低估了?
- 是否报告的损害表明损害的严重性被低估了?
- 是否有证据表明风险控制措施失效?
- 综合剩余风险分析是否准确地代表了实际的市场经验?
- 公认的最新技术水平是否发生变化?
- 是否有指标显示风险可接受性准则需要调整?

这些信息的评审可能会导致几种可能的结果例如:

- 正确识别了危险、危险情况和/或伤害, 充分估计风险, 考虑到器械的公认最新技术水平, 风险不变、仍然可以接受; 不需要采取进一步活动。
- 正确识别了危险、危险情况, 风险的经常得到评价并且保持可接受。
- 正确识别了危险、危险情况, 但风险增高并且不可接受。需要采取进一步措施。
- 危险和危险处境没有得到识别。需要采取进一步措施。

附录 A
(资料性附录)
识别危险和安全相关特征

A.1 总则

ISO14971:20XX要求制造商识别那些可能影响安全的医疗器械的特征。考虑这些特征是识别医疗器械危险的基本步骤,其中一种方法是对涉及医疗器械的制造、预期使用者、预期用途、可合理预见的误用和最终处置提出一系列的问题。如果从所有涉及的人员(如使用者、维修人员、患者等)的观点出发,询问这些问题,就会出现一个能够找到可能危险的更完整的概貌。

A.2条款中的问题可帮助读者识别可能影响安全的医疗器械的所有特征。附录H包含了评估体外诊断医疗器械风险所需考虑的附加要点。清单并不详尽,也不代表所有的医疗器械,建议制造商增加那些对特定的医疗器械具有适用性的问题,和忽略那些与特定的医疗器械不相关的问题。也建议制造商不要仅从自己的角度,还需要从相关的其他人员角度考虑每一问题。

制造商可进一步查阅相关临床文献、适用的法规、ISO 16142—1^[31]中的必需性安全和性能基本原则或者是ISO16142—2^[32]对体外诊断医疗器械的要求。涉及网络安全的医疗器械的附加资源参见AAMI TIR 57^[1]。

A.2 问题

A.2.1 医疗器械的预期用途是什么?应如何使用?

宜考虑的因素包括:

—医疗器械的作用与下列哪一项有关:

- 对疾病的诊断、预防、监测、治疗或缓解,
- 对损伤或残疾的诊断、监测、治疗、缓解或补偿,
- 生理结构或生理过程的调查、替代、改进或支持,
- 妊娠控制?

—使用适应症是什么?(如患者群体、使用者信息、使用环境)

—禁忌症是什么?

—医疗器械是否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?

—如果出现安全漏洞(性能下降或可用性丢失),是否会影响基本性能?

—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性?

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、患者群体特征、年龄、体重、身体活动情况、植入物性能老化的影响、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所需要的连接接口(如植入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长和频次。

A.2.4 在医疗器械中利用何种材料或组分,或与医疗器械共同使用或与其接触?

宜考虑的因素包括:

- 与有关物质的相容性；
- 与组织或体液的相容性；
- 与安全有关的特征是否已知；
- 是否使用了动物源材料制造医疗器械？
- 器械是否允许通过可访问的以太网端口、USB端口、串行端口、可移动硬盘驱动器访问器械上的信息、数据等？

注：见ISO 10993—1：2018^[20]附录B，以及ISO 22442系列标准^[41]。

A.2.5 是否有能量给予患者或从患者身上获取？

宜考虑的因素包括：

- 传递能量类型；
- 对其的控制、质量、数量、强度和持续时间；
- 能量水平是否高于类似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提取？

宜考虑的因素包括：

- 物质是供给还是提取；
- 是单一物质还是几种物质；
- 最大和最小传输速率及其控制。

A.2.7 医疗器械处理的生物材料是否以用于随后的再使用、输液/血或移植？

宜考虑的因素包括处理的方式和处理的物质（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使用者灭菌，或其它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；
- 有效期问题；
- 重复使用周期次数的限制；
- 医疗器械灭菌方式；
- 非制造商预期的其它灭菌方式的影响。

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和性能的影响。

A.2.10 医疗器械是否预期改善患者的环境？

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和测量结果的准确度和精密度，以及测量仪器或数据是否会被损坏。

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，所采用的计算方法和置信限来显示结论。宜特别注意数据和计算方法的非预期应用，以及对计算方法和数据未经授权的处理或改变。

A.2.13 医疗器械是否预期和其它医疗器械、医药或其它医疗技术联合使用？

宜考虑的因素包括识别可能涉及的任何其它医疗器械、医药或其它医疗技术和与其相互作用有关的潜在问题（例如，该器械未经授权的访问其他器械造成其他器械基本性能的影响），以及患者是否遵从治疗。

A.2.14 是否有不希望的能量或物质输出？

宜考虑的与能量有关的因素包括噪音和振动、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、电流泄露和电场或磁场。

宜考虑的与物质相关的因素包括制造、清洁或试验中使用的物质，如果该物质残留在医疗器械中具有不希望的生理效应。

宜考虑的与物质相关的其它因素包括化学物质、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、泄漏、对电源和制冷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：

- 对能源和制冷供应的影响；
- 毒性物质的散发；
- 电磁干扰的产生。

A.2.17 医疗器械是否有基本消耗品或附件？

宜考虑的因素包括消耗品或附件的规范以及对使用者选择它们的任何限制。

A.2.18 是否需要维护和校准？

宜考虑的因素包括：

- 是否由使用者或专门人来进行维护或校准？
- 是否需要专门的物质或设备来进行适当的维护或校准？
- 如何决定何时完成保养和再校准；
- 如何验证校准（仍）可接受。

A.2.19 医疗器械是否包含软件？

宜考虑的因素包括软件是否预期由使用者或操作者或专家进行安装、验证、修改或更换，和软件更新的可靠性。

A.2.20 医疗器械是否有贮存寿命限制？

宜考虑的因素包括医疗器械是否受时间、储存条件、原始包装的影响而衰退，超期（标识或指示）的信息传达、超期后的合理使用、超期器械的处置。

A.2.21 是否有延时或长期使用效应？

宜考虑的因素包括人机工程学和累积的效应。比如，包括含盐流体泵随着时间推移造成腐蚀、机械疲劳、皮带和附件松动、振动效应、标签磨损或脱落、长期材料降解。

A.2.22 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使用者的控制之下，或者和其他人员的相互作用来控制。

A.2.23 什么决定医疗器械的寿命？

宜考虑的因素包括电池损耗、材料老化和由于老化、磨损、疲劳和重复使用引起的部件故障。

A.2.24 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？是否可以明显看出医疗器械已使用过？

A.2.25 医疗器械是否需要安全地退出运行或处置？

宜考虑的因素包括医疗器械自身处置时产生的废物，或者对医疗器械所有敏感信息的适当处置。例如医疗器械是否含有毒性或有害材料，或材料是否可再循环使用。如果器械存储数据，则应考虑以适当、安全的方式处理数据。

A.2.26 医疗器械的安装或使用是否要求专门的培训或技能？

宜考虑的因素包括医疗器械的复杂性与新颖性，以及对医疗器械的安装人员、维护人员和使用者进行合适的技能培训。

A.2.27 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使用者或涉及的第三方参加者是否需要培训，第三方参加者包括：安装人员、维护人员、医疗卫生保健专家或药剂师；
- 试运行和向最终使用者的交付，以及是否很可能/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，是否要求对操作者或服务人员进行再培训或再认定。

A.2.28 是否需要建立或引入新的制造过程？

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改变。

A.2.29 医疗器械的成功使用，是否取决于用户接口的可用性？

A.2.29.1 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、所使用的符号、人机工程学特性、物理设计和布局、操作层级、驱动医疗器械软件的菜单、警示的可视性、报警的可听性、色标编码的标准化。可用性附加指南参见 IEC 62366—1^[6]，报警附加指南参见 IEC 60601—1—8^[7]。

A.2.29.2 医疗器械是否在因分散注意力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；
- 使用者是否可能受到不常见分散注意力情况的干扰；
- 重复压力是否会降低使用者的意识或注意力。

A.2.29.3 医疗器械是否有连接部分或附件？

宜考虑的因素包括错误连接的可能性、与其它的医疗器械连接方式的相似性、连接力、对连接完整性的反馈以及过紧和过松的连接。

A.2.29.4 医疗器械是否有控制接口？

宜考虑的因素包括间隔、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活动的可逆性。

A.2.29.5 医疗器械是否显示信息？

宜考虑的因素包括在不同环境下的可视性、方向性、使用者的视力、视野和透视、显示信息的清晰度、单位、色标编码以及关键信息的可达性。

A.2.29.6 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数量、状态认知、位置设置、导航方法、每一活动的步骤数、顺序的明确性和储存问题，和与可访问性相关的控制功能的重要性，以及偏离规定的操作程序的影响。

A.2.29.7 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：

- 用户、用户的心理和体能、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；
- 能够影响预期用户与医疗器械成功交互的能力的个人特征。参见IEC/TR62366—2^[7]。

A.2.29.8 医疗器械是否由具有特殊需要的人使用？

宜考虑的因素包括：

- 对于有特殊需求的使用者，例如残障人士、老人和儿童，可能需要他人帮助才能使用医疗器械；
- 具有宽泛技能水平和不同文化背景和期望的用户，这些区别可能导致医疗器械在适当的应用方面存在差异。

A.2.29.9 用户界面能否用于启动未经授权的活动？

宜考虑的因素包括：用户界面是否允许用户以受限的访问进入操作模式（例如，为维护或者特殊目的的使用），这会增加使用错误的可能性因此增加相关风险，并且是否会引起使用者意识到已经进入这种操作模式。

A.2.30 医疗器械是否使用报警系统？

宜考虑的因素是错误报警、不报警、报警系统断开、不可靠的远程报警系统的风险和医务人员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.2.31 医疗器械可能以什么方式被误用（故意与否）？

宜考虑的因素是连接器未正确使用、丧失安全特性或报警不能工作、忽视制造商推荐的维护，对医疗器械或医疗器械功能未经授权而进行访问。

A.2.32 医疗器械是否储存患者护理的关键数据？

宜考虑的因素包括修改或破坏数据的后果，未经授权的数据访问以及对患者的后果。

A.2.33 医疗器械是否预期为移动式或便携式？

宜考虑的因素是必要的把手、手柄、轮子、制动、机械稳定性和耐久性。

A.2.34 医疗器械的使用是否依赖于基本性能？

宜考虑的因素例如是生命支持医疗器械的输出特征或报警的运行。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.2.35 医疗器械的使用是否有一定程度的自主性？

宜考虑的因素包括：

—用户对具有一定程度自主性的医疗器械发生错误、警报或故障时的意识；

—用户对需要干预自主执行的操作时的意识；

—用户干预或中止自主执行的操作的能力；

—用户选择和执行适当纠正措施的能力。

更多的关于具有一定程度自主性的医疗器械的指南，见IEC TR 60601—4—1^[6]。

A.2.36 医疗器械是否产生作为确定临床操作的输入的输出？

宜考虑的因素包括错误或延迟的输出是否会对患者造成直接或间接的风险，如错误诊断导致患者延迟或遗漏治疗。见附录H体外诊断医疗器械的指南。

附录 B (资料性附录)

风险分析技术

B.1 总则

本附录为风险分析提供了一些可用的技术指南。这些技术指南是互补的,为了执行彻底的完整的风险分析,并且可能有必要使用不止一个技术。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,分析可能导致伤害的后续事件。其基本原则是对事件链一步一步地进行分析。

需要强调的是,这些风险分析只是 ISO14971:20XX 中描述的风险管理过程中的一步。因此,在此附件中阐释的技术没有关注风险分析的所有元素,而是只提供了支持信息。例如,在所有技术中没有包括对危险情况的识别。这些技术是补充性的,可能需要使用其中的多项技术来支持一个完整地贯穿的风险分析。

- 初步危险分析 (PHA) 是早在开发过程中对于医疗器械设计细节所知甚少时,用于识别危险、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) 是早在开发阶段,在安全工程中,对于危险、危险情况和可行的风险控制措施的识别和排序以及分析不良事件后果是特别有用的。
- 失效模式和效应分析 (FMEA) 是用于系统性地识别单一部件的效应或后果的技术,更适合于设计的成熟期。
- 危险和可运行性研究 (HAZOP) 通常用于开发阶段早期,以研究偏离预期性能的情况。
- 危险分析和关键控制点 (HACCP) 是典型的用于开发阶段晚期的验证和随后的设计概念的优化和变更。

B.2 初步危险分析 (PHA)

PHA 是一种归纳的分析方法,其目的是识别对给定的活动、设备或系统可造成伤害的危险、危险情况和事件。早在项目开发阶段设计细节或运行程序信息很少,PHA 最为常用并通常是进一步研究的先驱。分析现有系统或对危险优先排序时,环境因素阻碍使用更多的技术,这种方法可能是有用的。

在初步危险分析 (PHA) 中,通过考虑诸如下列特征列出危险和一般危险情况的清单:

- 使用或生产的物料及其反应;
- 使用设备;
- 运行环境;
- 布局;
- 系统部件之间的接口。

此方法包括识别事故发生或导致伤害的概率、定性评价可能造成的伤害的程度、以及识别可能的风险控制措施。所得结果可以不同的方式提供,如表格和树状图。

B.3 故障树分析法 (FTA)

FTA 主要是一种用来分析已由其它技术识别的危险的手段,它从一种设定的不希望的结果(即一个可能性伤害,亦称“顶级事件”)开始。以演绎的方式,从顶级事件和询问“为什么?”开始,识别产生不希望后果的下一个较低功能系统层次的可能原因或故障模式。接下来逐步识别不希望的系统运行(其通常是部件故障模

式或可应用风险控制措施的最低层次)至再下一层次系统等级,这样做即可达到所希望的系统层次。这将揭示最可能导致假定结果的故障模式组合。其结果以故障模式树的形式绘制成图,在树的每一个层次,故障模式的结合用逻辑符号(与门、或门等)描述。树中识别的故障模式可以是导致不希望事件发生的与硬件失效、人为错误或任何其它相关事件有关的事件。它们不仅仅局限于单一故障条件。

FTA 提供了一个系统的方法,它同时对分析各种因素,包括人的相互作用,具有充分的灵活性。在风险分析中,FTA 是用作估计故障概率和识别导致危险情况的单一故障和多重模式故障的工具。此种图形的表示法可使系统行为和所包括的因素容易理解,但在故障树变得很大时,可能要求使用计算机系统对故障树进行处理,这样易于实现。

有关 FTA 程序的更多信息见 IEC 61025^[10]。

B.4 事件树分析法(ETA)

ETA 是一种分析技术,用于评估导致负面结果的事件。它是一种因果分析技术,它基于对可能导致负面结果的一系列活动和事件的分析。ETA 使用与 FTA 相同的逻辑和数学技术。然而,当故障树分析如何发生不可取的顶级事件时,事件树会考虑系统中特定部件或项目的故障的影响,并计算出故障对整个系统风险的影响或可靠性。ETA 使用归纳法,而 FTA 是演绎法。

事件树中的初始事件通常属于以下四个类别之一:

- a) 医疗器械中的故障或不安全状况;
- b) 人为错误;
- c) 公用设施故障(例如断电);
- d) 外部事件(如飓风或地震)。

事件树分析的目标是确定可能导致伤害的可能的负面结果的概率以及所选择的初始事件的结果。有必要使用有关系统的详细信息来理解构造事件树图的事件顺序。事件树以初始事件开始,其中此事件的后果以二进制(成功/失败)方式进行。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,其中可以计算该路径的总发生概率。

事件树分析法的更多信息见 IEC 62502^[10]。

B.5 失效模式和效应分析(FMEA)

FMEA 是一种系统识别和评价单一故障模式后果的技术,是一种使用提问“如果……,会发生什么?”的归纳技术。部件分析每次只分析一个部件,因而通常着眼于一个单一故障条件。以“自底向上”模式进行,即随着程序进到下一个更高的功能系统层次。

FMEA 不仅限于部件设计的故障,也可包括部件在制造和装配过程中的故障(过程 FMEA),以及最终使用者对医疗器械的使用或误用造成的故障(应用 FMEA)。FMEA 可以延伸到包括单个部件故障模式、其发生概率和可检测性(仅限于检出可启动 ISO14971:20XX 预防措施的程度)在内的调查,以及后果的严重程度。为实施这一 FMEA,应相当详细地了解医疗器械的结构。

FMEA 也是一种处理使用错误的有效技术。这种技术的缺点既源于其仅限单一故障条件又源于处理冗余和结合修理或预防性维护措施的困难。

有关 FMEA 程序的更多的信息见 IEC 60812^[10]。

B.6 危险和可运行性研究 (HAZOP)

HAZOP 的基础理论是假定危险情况和伤害是由偏离设计, 运行变化引起的。只有定义了设计和开发输入时, 才能在开发过程早期执行 HAZOP。它是一种识别危险和可运行性问题的系统技术。最初开发它是用于化学加工工业。虽然 HAZOP 在化学工业中的研究的使用集中在对设计目的的偏离, 但是为医疗器械的开发者提供了可供选择的应用。HAZOP 可以应用于医疗器械的运行/功能 (例如用于作为“设计目的”的疾病诊断、治疗或缓解的现行方法/过程), 或应用于对医疗器械的功能有重大影响的医疗器械的制造或维修/服务过程 (例如灭菌)。HAZOP 的两个特点如下:

- 一要用具备医疗器械设计及其应用的专业知识的一组人员;
- 一用引导词汇 (无部、部分, 等) 帮助识别对正常使用的偏离。

这种技术的目标是:

- 一做出对医疗器械及如何预期使用的全面描述;
- 一系统地评审预期用途的每个部分, 以便检出对正常运行条件和预期设计的偏离如何发生;
- 一识别此种偏离的后果, 并决定这些后果是否会导致危险或可运行性问题。

应用于制造医疗器械的过程时, 最终目标对医疗器械特性依赖于制造过程的情况特别有用。

关于 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 是一种识别、评价和控制危险的系统性方法, 通过对生产过程中关键控制点的关注。它基于一组原则和规定的术语。应用于医疗器械时, HACCP 可用于来自过程, 特别是生产过程的, 医疗器械危险的初始原因的控制和监测。

HACCP 的核心内容包括下列七项原则:

1. 进行危险分析并识别预防措施;
2. 确定关键控制点 (CCP);
3. 建立关键极限;
4. 监测每一个关键控制点 (CCP);
5. 建立纠正措施;
6. 建立验证程序;
7. 建立记录保持和文件编制的程序。

每一个产品都有和预期用途有关的自身危险。危险情况可能由生命周期不同阶段的事件 (原因或者影响因素) 所引起, 例如设计、制造、服务、使用处置等。

一项有效的 HACCP 系统的核心是集中在对已识别危险的持续控制和监测 (HACCP 原则 2、3 和 4)。制造商以建立系统的形成文件的过程图、过程危险分析、和关键控制计划 (HACCP 原则 7) 的方法证实已建立的控制措施 (HACCP 原则 5 和 6) 的有效性。

HACCP 体系使用下列工具作为保持记录的书面证据:

a) 过程流程图

该图的目的是为过程中所涉及的步骤提供清晰而简单的描述。流程图对 HACCP 小组在随后的工作中是必要的。流程图也可为那些为了其验证活动而需要了解过程的其他人提供接下来的指南。流程图的范围宜覆盖制造商直接控制的所有加工工序。

b) 危险分析工作表

危险分析识别危险及其初始原因。分析记录包括:

- 发生重大危险的过程中的各步骤的识别和列表;
- 和每个步骤相关的所有识别的危险及其重要性的列表;
- 控制每个危险的所有预防措施的列表;
- 所有关键控制点的识别及其监测和控制。

c) HACCP 计划

该书面文件是建立在 HACCP 七项原则基础上, 描绘所要遵循的程序, 以确保特定的设计、生产、过程或程序的控制。计划包括:

- 识别关键控制点和明确关键极限;
- 监测和持续的控制活动;
- 识别和监测纠正措施、验证和记录保持活动。

附录 C

(资料性附录)

方针、风险可接受性准则、风险控制和风险评价之间的关系

C1. 总则

本附件阐述了最高管理规定的方针和建立在方针基础之上的风险可接受性准则。这一阐述包括作为方针的组成部分。它也解释说明了风险可接受性准则在风险控制和风险评价中的应用。方针、准则和风险评价之间关系的示例给出了几个方针的组成部分。

C2. 建立风险可接受性准则的方针

方针必须提供建立风险可接受性准则的框架。这一框架需要引领并指导准则的建立。它关注于单一剩余风险和综合剩余风险的接受性准则。

用于建立风险可接受性准则的方针需要形成文件，例如作为制造商质量管理体系文件的部分，但不需要作为风险管理文档的部分。

建立风险可接受性准则的方针可能包括下列因素：

- 目的
- 范围
- 风险控制措施
- 其它因素和考虑
- 批准和评审的要求

强调这一方针和其组成要素应进行调整适应制造商组织的特殊要求很重要。每一个要素的详细讨论如下：

-目的。此目的用来说明建立风险可接受性准则的方针的目标。

示例 1：方针的目的是为了建立风险可接受性准则提供指南。这些准则可以用于与制造商在[]制造的医疗器械相关剩余风险的评价。这些准则将确保医疗器械有企业家期望的高水平的安全性。

-范围。此范围将规定方针实施的对象、场合和时间。

示例 2：此方针可应用于参与建立、评审、更新和批准的在风险可接受性准则的所有人。此准则列入医疗器械的设计开发和/或生产的用于商业分销过程的风险管理计划。

-风险控制的措施。可以依据 ISO14971: 2019, 4.2 的第一条来规定措施。这些措施包括实用性的考量，如合理实际地尽可能低的降低风险，合理可实现地尽可能低地降低风险，或者对受益-风险比无任何不良影响地尽

可能地降低风险。另一个风险控制的可能性办法与风险的等级有关，例如，风险控制可以不追踪低于一定界限的小风险。这是一个进一步解释的错误！没有发现参考资料。

示例 3：对受益-风险比不存在不良影响地尽可能地降低风险。这需要考虑是可降低风险的技术性可操作的措施，对医疗器械的预期用途和受益不产生影响。

示例 4：合理可实现地尽可能低的降低暴露在辐射下的风险时，考虑技术性可实际操作的风险控制措施。

-其它因素和考量。这一方针可能要求在建立风险可接受性准则时考虑下列因素：

医疗器械上市地区的适用法规的要求：

- 特殊类型医疗器械适用的国际标准，包括含有批准/拒绝限制的特殊性能的检测标准（见附录 E）；
- 最新技术水平，可以来自对国际标准评审、良好技术规范、已公认的科学研究成果、监管部门的印刷物、与相似的医疗器械或者产品的信息。
- 来自利益相关方证实的关注，例如直接从与使用者、临床技师、患者或者监管方的直接交流中，或者间接从新闻报道、社交媒体或者患者论坛中获得的信息。重要的一点是需要考量不同的利益相关方对风险识别和理解可因群体而改变，受到他们的背景和兴趣特性的影响。
- 批准和评审的要求。这一方针可以规定谁需要被批准，如果需要，需要多少次的评审。

示例 5：建立可接受性准则的方针由[头衔/职能最高管理者]批准并且每年至少培训[X]年由[评审机构的名称]。

C3. 风险可接受性准则

风险可接受性准则建立在制造商的判定可接受风险的方针上。当损害的概率无法估计时，它也与可风险可接受性准则有关，此时准则只是建立在损害的严重度之上。风险可接受性准则必须在风险管理计划中形成文件。

每种类型的医疗器械的特定的准则[或者医疗器械族]，与其特征和预期用途有关，或者是与已经建立的全部的医疗器械有相同的准则。风险可接受性准则可以包含对特殊特性的定性要求和定量要求限度的组合，偏好依据国际标准。

综合剩余风险的可接受性准则也需要建立。它可以与单一的可接受性风险准则相同或不同。评价综合剩余风险的方法和可接受性准则应在风险管理计划中文件规定。第 8 章提供了更详细的关于准则的指南。

C4. 风险控制

风险控制是一个过程，在此过程中做出决定并且实施措施从而风险得到降低或者保持在特定的水平。这一过程可以由建立风险可接受性准则的方针中包含的措施来指导（见 C 2）。下面讨论两种风险管理的措施。

一种可能的措施是考量风险控制措施的可行性。可行性（可行）是指风险控制方案可行或者可操作。这不应与实用性（实用）混淆，其是指措施有可用性和方便性。可行性有两个组成成分，称之为技术可行性和经济可行性。

技术可行性是指不计成本降低风险的能力。下面几个示例的技术可行性值得质疑：

- 包括需要警示和警告使使用者在操作医疗器械时受阻；
- 众多警告使使用者的操作受阻或迷惑；
- 公布过多的剩余风险使使用者对哪一个真正重要产生理解困难；
- 过度复杂的医疗器械使用程序使使用者的失误增加或者预期用途损害，对受益和风险的平衡产生负面效应（见 ISO14971: 20XX, 4.2 条款 1）；
- 采用的风险控制措施降低了医疗器械的有效性或者损害了预期用途（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副作用。

经济可行性是指在没有使医疗器械带有不合理的经济要求下的降低风险的能力，因为风险控制措施将会使医疗器械过于昂贵因此无法获得。

这些决策必须涉及接受风险和处置或判定之间的互动。成本和可用性的影响在决定应用对维护、提升和改进人类健康方面的影响需要进行考量。这种决策中的经济可行性与对公众健康和整个社会的受益相关。然而，可行性也不能够作为接受不必要的风险的理由。

另外一个可能的风险控制措施是考量剩余风险的等级。这包括依据其等级将风险分为三个等级：

- a) 剩余风险的等级超过制造商的风险可接受性准则；
- b) 剩余风险过小可以不计或忽略（例如，去除它不会降低剩余风险）；或
- c) 在 a) 和 b) 两种状态之间的剩余风险；

此方针可以指导归为 b) 类的某一剩余风险，在开展风险评价之前，是否需要进一步降低。

在此方法中，制造商可以使用半-定量风险图或者风险矩阵如图 C.1 来辅助风险估计（也见错误，文献来源未见）。这一风险图可以分为三个区域 a) 不可接受风险，b) 微小或者可忽略的风险，c) 需要调查进一步降低的风险。估计的风险 (R_1, R_2, R_3, \dots) 被放入适宜的格中。风险 R_1 到 R_6 不可接受。风险 R_7 和 R_8 需要进一步降低调查，而 R_9 微小，并且依据制造商的方针可接受。

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	R1	R2			
	偶尔的		R4		R3	
	很少发生	R6				
	不大可能			R5		

图 C.1-风险矩阵三区域示例

c. 5 风险评价

在这一步骤制造商将估计的风险与在风险管理计划中规定的风险可接受性准则进行比较并判定风险是否可接受。在图 C.1 中展示了风险矩阵可以辅助风险的估计与评价,特别是对那些在国际标准中没有要求或技术解决方案的。

C. 6 示例

风险可接受性准则建立在最高管理者定义的方针之上。这个准则随之可以应用在风险控制和风险评价中。这一方针包括几个要素和方法。这一方针、准则和风险评价之间的关系要素示例在表 C.1 中展示。

表 C.1 方针各要素、风险可接受性准则和如何在风险估计中应用准则的关系示例

<p>监管要求</p> <p>方针: 准则满足医疗器械上市或预计上市的每一个市场的适用法规的安全要求。例如, 法规要求在单一错误情况下医疗器械保持安全, 同样适用于软件失误。</p> <p>准则: 医疗器械需要在单一错误情况下保持安全, 包括软件失误。</p> <p>评价: 医疗器械得到检测并且依据法规或标准中的测试极限而建立的准则得到实施。风险评价包括评审检测结果、标准符合报告或者证书。</p>
<p>国际标准</p> <p>方针: 基于适用的国际产品和过程标准而建立的准则。</p> <p>准则: 1) 来自国际产品标准的测试极限得到应用。 2) 依据 IEC62366-1^[10]的过程开用户界面。</p> <p>评价: 1) 评审每个标准的符合性报告 2) 评审可用性工程文档。</p>
<p>最新技术</p> <p>方针: 基于最新技术水平的准则, 来自可获得的市场上相似医疗器械的和预期用途和任何替代治疗或者医疗器械的文献评审。</p> <p>准则: 1) 医疗器械漏电流是最新的, 被证明符合依据 IEC60601-1 漏电流的极限和测试。 2) 传送装置的计量精度是最新的, 被证明符合 ISO11608-1 的计量精度的极限和测试。 3) 对由于碰撞引起的医疗器械失效的防护与类似医疗器械在一个水平或者好于, 可以由对比试验如下降实验证明。</p> <p>评价: 对证明医疗器械符合或者超越基于最新技术水平极限、基于国际标准或与市场上医疗器械相比的数据和信息进行评审。风险评价包括评审和对比设计特征或者比较性的测试结果。</p>

来自利益相关方的关注

方针：在对医疗器械的预期用途的医疗和科研文献的评审中识别的已知的相关方的准则或者可用性研究，专家团和/或讨论组，或者在生产后的监测中。

准则：1) 与牛相关的材料的风险是公众的关注因此在设计中应避免

2) 与多患者事故性共用传递药物的针头相关医疗器械是临床机构的关注，因此对此风险的警示是可以接受的。

评价：风险评价可以包括对利益相关方要求的极限的医疗器械的绩效的评审，或者是利益相关方的直接参与（讨论组或相似的）在风险评价中。风险评价可以将风险估计与利益相关方可以接受的风险水平相比较。

附录 D

(资料性附录)

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“剩余风险公示（以下同此）”之间的差异，还提供了有关如何将安全信息作为风险控制措施以及如何以提高风险意识的方式披露剩余风险的指导。

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（进一步）通过其他措施降低风险后才能使用。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征，如果不可能的话，考虑公认的现有技术水平的保护措施。即使这样，患者、使用者或其他人的安全仍然可能取决于要采取或避免的某些动作，有关这些活动的说明构成了安全信息。

安全信息具有指导性，需要向用户明确说明应采取或避免采取的措施，以防止发生危险情况或危险。这些信息可以以警告、（预）警示、禁忌症、使用说明（包括安装、维护和处置）或培训的形式提供。ISO 14971:20XX 要求验证安全信息的有效性（例如通过应用可用性工程过程）并可在风险管理文件中进行跟踪。

某些情况下，安全信息的文本由当地法规规定。

在制定安全信息时，重要的是确定要向谁提供这些信息以及如何提供这些信息，制造商应提供风险、暴露后果以及应采取或避免的措施以防止任何伤害的解释。制造商应考虑：

- 基于其风险水平，对安全信息进行分类的需求；
- 传递安全信息的必需的细节程度；
- 安全信息的位置（例如医疗器械上的警告标签）；
- 用于确保清晰度和可理解性的措辞、图片或符号；
- 预期接收者（例如使用者、服务人员、安装人员、患者）；
- 提供信息的适宜媒介（例如用户界面中的使用说明、标签、警报、警告）；
- 监管要求。

安全信息可能需要以不同的方式进行传递，这取决于在医疗器械生命周期中何时传递信息，例如作为附带文档、咨询通知或菜单驱动设备的用户界面中的警示性声明。

安全信息可以附在医疗器械上以警告标签的形式给出，或作为使用说明中的警告声明。下面给出一些例子。

- 警告：不要踩到表面。
- 警告：请勿拆下盖子，否则有触电的危险。

—警告：不要使用含有超过 60 mg/dL 血红蛋白的溶血血清样本，因为这些会干扰测量并影响结果的准确性。

D.3 剩余风险披露

剩余风险是指在采取所有风险控制措施后仍然存在的风险。剩余风险与使用医疗器械可能产生的副作用或后遗症有关。ISO14971:20XX 要求制造商向使用者告知剩余风险。

披露剩余风险是描述性的，并为用户提供解释与医疗器械相关的剩余风险所必需的信息。目的是在随附的文档中公开信息，以使用户和潜在的患者能够做出明智的决定，权衡剩余风险与使用医疗器械的好处。制造商需要检查剩余风险并确定用户需要接收哪些信息，制造商关于披露剩余风险的决定应记录在风险管理文件中。

所公开的信息在临床决定过程中可能是重要的。在预期用途的框架内，使用者可以决定医疗器械可以用于哪种临床设定以实现患者的某种受益。剩余风险的公开对于使用者或医院组织做好准备，以应对患者在使用医疗器械期间或之后可能发生的副作用或危险。注意，操作者、用户和患者可以是同一个人，例如用于家庭医疗保健环境中的医疗器械。

在制定有关风险披露的信息时，重要的是确定要传达的内容以及针对哪些风险。制造商应考虑：

- 信息的详细程度；
- 要用于确保清晰度和可理解性的措辞；
- 预期接收者（例如使用者、服务人员、安装人员、患者）；
- 要使用的手段和媒介。

在确定适当的详细程度时，制造商可以考虑汇总信息，而不是简单地从风险管理文件中复制细节。详细程度应与剩余风险以及该信息的预期接收者的知识和经验相称。下面给出一些示例以说明与使用医疗器械相关的剩余风险和通常披露的副作用。

- 线性加速器可用于治疗肿瘤。肿瘤放射治疗的剩余风险包括可能导致红斑或脱毛。
- 进行磁共振成像（MRI）时，患者需要在封闭的空间中，一些患者可能会出现幽闭恐怖症。
- 辅助或替换自主呼吸的机械通气器械可能导致并发症，如气道损伤、肺泡损伤或气胸。
- 在对肾结石进行碎石术后，大约 10% 的患者尿液中有血液，或者当小石块通过时感到肾脏疼痛，而约 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% 的患者出现轻度的光敏感。
- 带有植入式心律转复除颤器（ICD）的患者可能经历在不恰当的休克、想象性休克（幻觉）、依赖、压抑、清醒时对休克的恐惧。

附录 E

(资料性附录)

标准在风险管理中的作用

E.1 总则

标准（“国际标准”在此均译为“标准”，代表国际标准、国家标准、行业标准，以下同此）在风险管理中发挥着重要的作用，针对医疗器械安全及生产过程提出了要求。此标准根据 ISO/IEC 指南 63^[30] 设立，为国际医疗器械标准的发展以及对安全方面的涵盖提供了参考。国际标准由该领域的专家设定，代表着公认的最新技术水平。

在实施风险管理时，制造商需要首先考虑所设计的医疗器械的预期用途、安全方面的特性以及与之相关的危险或危险情况。制造商可选择并应用包含特定要求的标准，帮助在医疗器械生命周期内对与这些危险或危险相关的风险进行管理。

对于符合国际标准和规范性标准要求医疗器械，在无相反的客观证据时，则其与危险或危险情况相关的剩余风险为可接受风险。潜在的客观证据包括：对于不良事件、产品召回以及投诉的报告。国际标准的要求（例如：工程或分析过程、特定输出限制、警告声明或设计规范）可被视为标准撰写者为解决特定危险或危险情况的风险控制措施。

在许多情况下，标准撰写者已经进行并完成了风险管理的相关要素，并以设计要求、测试方法等形式为制造商制定了合规性标准，以此提供解决方案。风险管理时，制造商可以直接参考标准撰写者的成果，无需重复在制定标准的过程中（已由撰写者完成的）必要的分析。因此，国际标准对于风险的可接受性提供了有价值的参考信息。这些信息均已在全球范围评价的过程中，通过多轮评审、评论和投票，得到验证。

E.2 产品安全标准在风险管理中的应用

在实施国际产品安全标准建立的要求时，其为特定危险或危险情况提供了可接受风险的准则（如：设计方案、安全界限）。制造商可在风险管理时以下列方式应用此标准：

a) 如果国际产品安全标准规定了针对特定危险或危险情况的技术要求，并结合具体的验收标准，则默认遵守这些要求后，剩余风险已降至可接受的水平，除非有相反客观证据。例如：泄露电流必须被控制在可接受的风险水平。IEC 60601-1^[31] 规定了漏电流限值，在规定条件下测量时，这些限值即被认可为可接受的风险水平。因此，在这种情况下，没有必要进一步的风险管理。此类情况下，需要采取以下步骤：

1. 确定安全方面的特征，并识别与医疗器械相关的危险或危险情况。
2. 确定国际产品安全标准所涵盖的具体的危险或危险情况。

3. 对于国际产品安全标准所涵盖的已识别的危险或危险情况，制造商可以依靠国际标准中的技术要求来阐明可接受风险。

4. 制造商应尽可能确保医疗器械的设计规范符合作为风险控制措施的标准中的技术要求。

注：对于某些国际产品安全标准，识别所有特定风险控制措施的可能被局限。例如：IEC60601—1—2^[6]中针对复杂医疗器械的电磁兼容性测试。

5. 风险控制措施的实施情况，可以通过对设计文件的评审来验证；而这些措施的有效性，可以从测试和测试结果中获得，并证明医疗器械符合国际产品安全标准的相关技术要求。

6. 如果满足相关要求，则相关的剩余风险被认为是可接受的。

- b) 如果国际产品安全标准没有完全规定技术要求和相关试验以及试验验收标准，则情况更为复杂。在某些情况下，该标准仅提供了与已知危险或危险情况相关的特定测试，但没有该测试的验收标准（例：IEC 60601—2—16^[6]）。在某些其他情况下，该标准仅识别了特定危险或危险情况（例如 IEC 60601—1—1 中的某些条款^[5]）。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导。但是，制造商仍应尽可能在特定医疗器械的风险管理中参考这些标准。
- c) 对于未在任何国际产品安全标准中明确提出，但对于特定医疗器械确实存在的危险或危险情况，制造商仍需要在风险管理过程中应对这些危险或危险情况。制造商需要估计和评价风险，并在必要时控制这些风险。

有关使用国际产品安全标准的过程图和示例，请参见图 E.1。

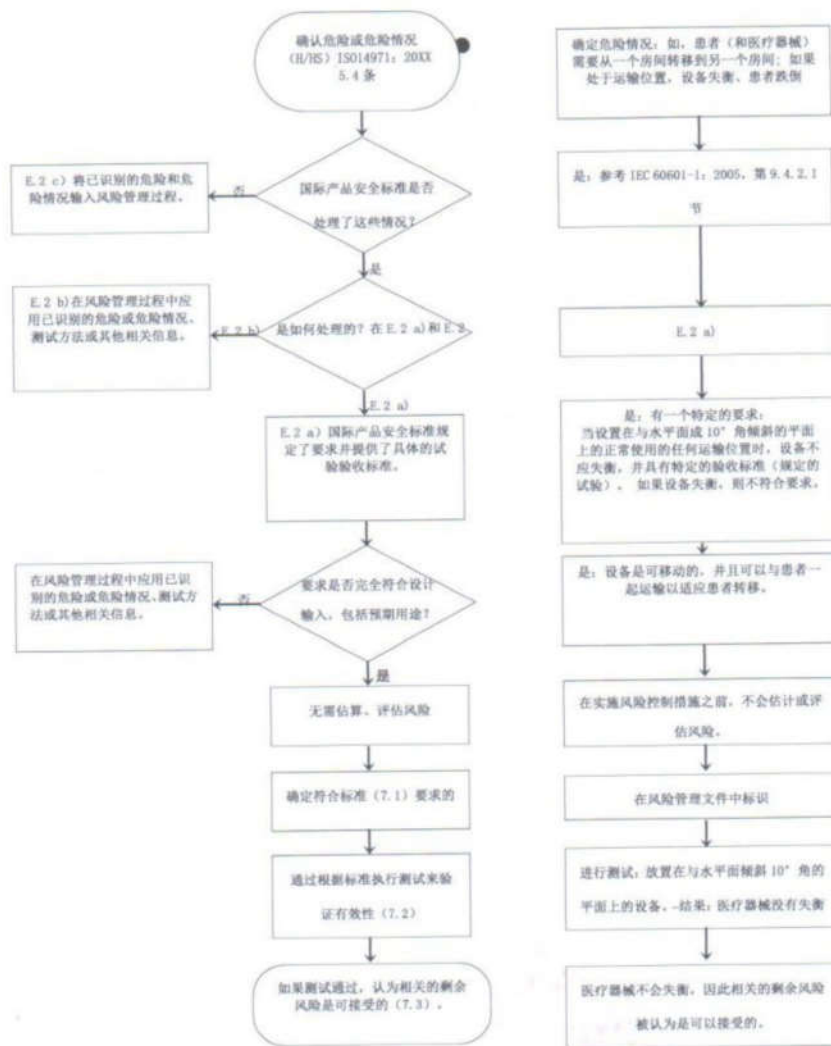


图 E.1 国际产品安全标准的运用和该标准规定的要求和提供的特殊测试可接受性准则的示例

E.3 国际过程标准与 ISO 14971

如下面示例所示，国际过程标准通常可以与 ISO 14971 结合使用。这可以通过以下两种方式之一执行：

- 国际过程标准要求将 ISO 14971 作为实施该标准的一部分。例：关于软件生命周期过程的 IEC 62304^[145]；
- 国际过程标准旨在用于风险管理，例：关于可用性工程的 IEC 62366-1^[146]、用于临床试验的 ISO14155^[147]和关于生物评价的 ISO 10993-1^[148]。

在以上任意一种情况下，正确使用国际过程标准需要注意该标准与 ISO 14971 的衔接，以便医疗器械达到可接受的风险水平。应协同使用两个标准，优化输入、输出和时机。下面给出三个示例以阐明这种理想情况。

a) IEC 62304，医疗器械软件 软件生命周期过程

IEC 62304 和 ISO 14971 之间的关系在 IEC 62304：2006 和 AMD1：2015^[145]的引言中有详细描述。

“假设医疗器械软件是在质量管理体系内（见 IEC 62304：2006，第 4.1 条和 AMD1：2015）和风险管理过程中（见 IEC 62304：2006，第 4.2 条和 AMD1：2015^[145]）开发和维护的。国际标准 ISO 14971 已经很好地规定了风险管理过程。因此，IEC 62304 只需通过对 ISO 14971 的规范性参考而利用这一优势。除此以外，对于软件还需要设立一些较小的额外风险管理要求，尤其在识别与危险、危险情况有关的因素上。这些要求在 IEC 62304：2006 第 7 条和 AMD1：2015^[145]中作为软件风险管理过程有所提及和总结。

在风险管理过程的危险识别期间，确定了软件是否导致了危险情况的发生。此外，还需要考虑可能由软件间接引起的危险情况（例如，软件提供的误导性信息可能导致不适当治疗）。进行风险控制时，将决定是否使用软件来控制风险。根据 ISO 14971，此标准所要求的设备风险管理过程必须包含对软件的风险控制。”

IEC 62304 对 ISO 14971 进行了规范性参考，特殊要求如下：

—对于软件开发计划（见 IEC 62304：2006，第 5.1 条和 AMD1：2015），其要求与 ISO 14971 要求的风险管理计划一致；

—对于软件风险管理过程（见 IEC 62304：2006，第 7 条和 AMD1：2015），其要求基于 ISO 14971。

b) IEC 62366-1，医疗器械-可用性工程在医疗器械中的应用

IEC 62366-1：2015^[146]图 A.4 中的流程图阐述了风险管理和可用性工程两个并行且互相关联过程的关系和互联。除了对 ISO 14971 进行规范性引用外，IEC 62366-1 还确定了几个特定条款，可用性工程的过程可以因此补充 ISO 14971 中描述的风险管理并与之交互：

—IEC 62366-1：2015^[146]第 5.1 条要求制造商提供使用规范，该规范可根据 ISO 14971 确定预期用途。

—IEC 62366-1：2015^[146]第 5.2 条要求制造商识别安全方面的用户界面特征，作为根据 ISO 14971 执行的风险分析的一部分。

—IEC 62366-1：2015^[146]第 5.3 条要求制造商识别可能影响患者、用户或其他与使用医疗器械相关的已知或可预见的危险和危险情况，根据 ISO 14971 作为风险分析的一部分。

—IEC 62366-1：2015^[146]第 5.9 条要求制造商对医疗器械的最终用户界面进行总结性评估，以作为风险管理的一部分。

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

ISO 10993-1^[22]引言指出, ISO 10993 旨在成为风险管理过程中医疗器械生物评估的指导文件, 作为每个医疗器械整体评估和开发的一部分。

ISO 10993-1: 2018^[22]的附录 B 提供了依据 ISO 14971 的风险管理方法指南, 用于识别与医疗器械相关的生物危险、风险的估算和评估、风险的控制以及监测风险控制措施的有效性。

这种方法结合了对来自所有来源的现有数据的评审和评价, 以及(在必要时)应选择和应用的额外的测试, 从而能够对每个医疗器械的生物反应进行与使用安全相关的全面评估。

生物评估应采用与其他产品风险相似的方式进行, 并应包括风险分析(有哪些危险以及相关风险?)、风险评价(这些风险是可接受风险吗?)、风险控制(如何控制风险?)、综合剩余风险的评价。生物学评价应考虑:

- 不同选择材料的物理和化学特征;
- 任何临床使用和人类接触的信息的历史;
- 产品和组成材料的任何存在的毒理和其它生物安全信息;

调查要求的信息的数量与深度依据预期用途和患者接触的特点与时间长度而改变。

根据ISO 10993-1^[22], 专家评价员应确定现有信息或数据是否足以确定与生物危险相关的综合剩余风险是否为可接受风险。该结论记录在生物评估报告中, 并成为风险管理文件的一个元素。根据ISO 14971中定义的过程, 如果剩余风险的总体评价从现有数据(即被识别的风险为可接受风险)中得出结论, 则无需进一步的风险控制。否则, 应采取适当措施进一步控制风险。

d) ISO14155, 用于人体的医疗器械的临床调查-良好的临床实践

ISO14155^[23]阐述了基于人体的可用于设计、生产、上市前的记录和报告以及上市后的临床调查, 以评价医疗器械的性能或者有效性和安全性。它与临床风险评价和受益-风险医疗器械的受益-风险平衡相关(但不适用于体外诊断试剂)。

附录 F
(资料性附录)
与(信息)安全相关风险的指南

F.1 总则

ISO14971 的风险管理过程也适用于与安全相关的风险管理,因为安全漏洞和保密性、完整性或可用性缺失可能导致伤害,继而被视为危险。

本标准中的安全包括网络安全以及数据和系统安全。

F.2 在安全风险管理中使用的术语

尽管安全风险管理与 ISO14971:20XX 通常使用不同的术语。但是,可以指出安全风险管理和 ISO14971:20XX 中使用的术语之间的对应关系。以下术语来源于《AAMI TIR57》^[1],常用于安全风险管理的。

—**数据和系统安全**:通过建立和维护相应的保护措施而达到一种在系统受到故意或无意的(参见《IEC Guide 120,第3.13条》^[4])恶意攻击或感染时处于不可侵犯的状态,或者是医疗器械的信息资产(数据和系统)在保密性、完整性、可用性退化时受到合理的保护(参见《AAMI TIR57,第2.6条》^[1])的一种运行状态。这对应于安全,比如,免于不可接受的风险(参见《ISO 14971:20XX,第3.26条》)。

—**威胁**:当存在可能违反安全,并造成伤害的情况、能力、活动或事件,即存在违反安全的潜在因素(参见《IEC Guide 120,第3.16条》^[4])。威胁对应于导致危险情况的事件或事件顺序(参见 ISO 14971:20XX,第3.5条)。

—**威胁事件**:有可能造成不良后果的事件或情况。威胁事件通常被认为是一种特殊类型的危险情况(参见 AAMI TIR57^[1])。

—**漏洞**:系统设计、实现或运行和管理中的故障或弱点,可以被用来违反系统安全策略(参见 IEC Guide 120,第3.18条^[4])。漏洞可以被视为一种危险源(参见 ISO 14971:20XX,第3.4条)。

—**漏洞利用**:已存在一个或多个漏洞,并可能影响医疗器械的基本临床性能,或可能通过使用该医疗器械作为载体而伤害连接设备或系统的性能。

—**保密性**:保留对信息访问和披露的授权限制,包括保护个人隐私和专有信息的手段(参见 AAMI TIR57,第2.6条^[1])。

—**完整性**:防止错误的信息修改或销毁,包括确保信息抗抵赖性(参见 AAMI TIR57,第2.15条^[1])。

—**可用性**:确保及时可靠地访问和使用信息(参见 AAMI TIR57,第2.5条^[1])。

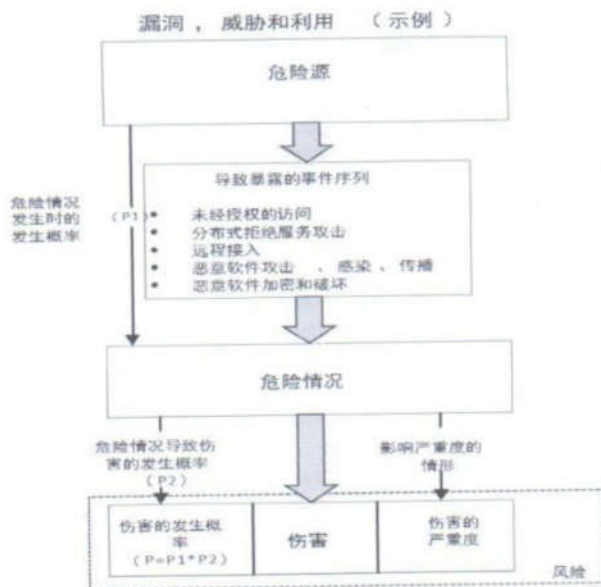


图 F.1-危险源、危险情况、伤害和安全术语的关系

F.3 ISO14971 与安全风险之间的关系

一个对 ISO14971 常见的错误认知是，一些人认为这个标准只适用于人体的健康，而忽略了危险源的定义包括对财产和环境的伤害。这个错误认知经常出现在对网络安全的讨论中，因为一些人坚持认为 ISO14971, 20XX 仅仅是关于“使用者和患者的安全”，而不是“安全”相关风险。

需要指出的是，IEC Guide 120^[5]中关于数据和系统安全的定义与安全性的定义不是同一水平的，安全性与最终结果相关，而安全则关注对系统特性和性能的影响。

ISO14971 中伤害的定义适用于人体、财产和环境，可能存在一部分重叠。例如，对电子健康记录（财产）的伤害可能会导致错误的诊断，从而导致患者（人身）伤害。必须注意的是，安全风险管理的范围往往更广。

几个可以引发损害的安全危险的示例(对人体健康的伤害或损伤)在表 F.1 中列出：

表 F.1-危险、事件序列、危险处境和在安全危险处境引发的损害之间的关系

危险	事件序列	危险情况	损害
丧失数据完整性	1) 不必要的网络接口的弱点被开发 2) 注入泵的注入设定信息被非授权修改	不正确的剂量信息导致注射液输入非预期	健康恶化 死亡
丧失数据完整性	1) 不必要的网络接口的弱点被开发 2) 病人信息或诊断结果被非授权修改	修改信息导致不正确的临床判断或者程序或缺少治疗	健康恶化 不必要的手术
丧失数据可获得性	1) 不必要的网络接口的弱点被开发 2) 医疗器械的操作由于受到 DDoS 攻击或勒索而降低或者终止	延误治疗。无法诊断。	医疗器械失效 健康恶化
丧失数据保密性	1) 不必要的网络接口的弱点被开发 2) 泄露个人健康信息	否认保险覆盖导致缺乏治疗	生理压力 健康恶化

此外，在区分这些领域时，有时会使用术语“安全风险管理”和“网络安全风险管理”。本标准遵循 ISO/IEC Guide 63 [20] 的建议，其中术语“安全”不作为形容词使用。相反，本附录将使用“健康风险管理”和“网络安全风险管理”。

需要指出，IEC Guide 120 [4] 中的数据和系统安全的定义包括无意的行为，例如在非恶意攻击的情况下个人健康信息的意外泄露；正常使用时的网络安全风险也应接受评价，例如因非临床需求而在显示器上显示个人健康信息。

F.4 安全风险管理特征

健康风险管理和网络安全风险管理都遵循着一个识别过程，这个过程步骤包括建立风险可接受性准则，执行风险分析，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以是不同的，但是整体过程是一样的。

ISO14971:20XX 要求评价风险控制措施引起的风险。网络安全风险控制措施可能会带来新的（健康）风险，反之亦然。例如，一个网络安全风险控制措施是要求用户在使用前输入密码，但在生命维持器械（如自动体外除颤器）上，由于忘记密码而导致的延迟可能是不可接受的，因此需要考虑不同的选项，图 F.1 说明了这种关系。此外，危险、事件序列、危险情况和与安全相关的伤害之间的关系如图 F.2 所示。

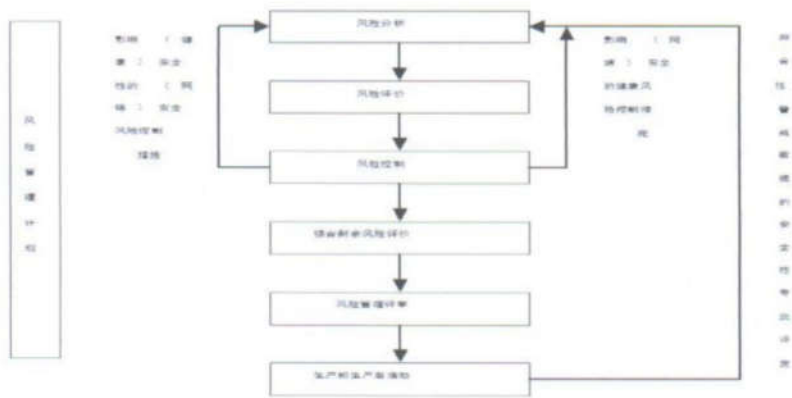


图 F-2 - 风险管理过程 (网络) 安全风险控制措施可以影响 (健康) 安全, 健康风险控制措施可以影响 (网络) 安全

与纯技术风险管理相比，网络安全风险的管理可以要求用不同的方法和途径，这类似于可用性或可靠性相关风险控制方法的差异性。严重度定义为“危险源可能后果的度量”（参见 ISO14971: 20XX, 第 3.27 条）。在健康风险管理中，严重度表现为一个人的健康恶化程度。低严重度可以定义为暂时的不适或不需要医疗干预的轻伤，中等严重度可以定义为需要医疗干预的伤，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伤。在网络安全风险管理中，安全数据系统保持高度保密性，完整性和可用性。因此，安全系统的严重度可以用这三个因素的退化来表示，而非人的健康。

健康风险管理中，严重度通常与基本安全（例如电击）或者设备的预期用途（例如 X 射线成像时的辐射暴露）相关。在网络安全风险管理中，严重度通常与设备本身的信息（例如个人健康信息的泄露、软件或数据的修改或损坏）或连接设备的信息相关（例如，连接丢失、信用卡信息的访问）。

健康风险管理中，可能性（概率）通常是设计和制造、材料选择、公差、设计余量等的函数。这些因素通常可以用高水平置信度来预测。在网络安全风险管理中，可能性（概率）通常是动机、经济受益、故意伤害、机会、开放漏洞的函数。这些事情都不容易估计。此外，一旦漏洞利用在互联网上进行公开后，网络安全风险管理中的可能性可能迅速从“极少”转变为“每次”。

F.5 机密性、完整性、可用性优先顺序

在评价与网络安全相关的风险时，需要确保安全优先级（机密性、完整性和可用性）的制定适当地考虑了医疗器械的预期用途。对于某些应用，信息的完整性受到高度重视，完整性的丧失可能导致患者病历的篡改（如医嘱或者医疗数据/图像的篡改）。在其他情况下，失去机密性可能更为重要，因为披露个人健康信息可能会导致敲诈勒索。机密性的另一个示例是设计功能未加密时（静态或传输中的数据）。这些特征的逆向工程可能会危及医疗器械的操作，从而导致对患者的伤害。医疗器械可用性的丧失可能导致诊断延迟或延误治疗。特别是对于生命支持或救生医疗器械而言，可用性的丧失或有效性的降低对于健康人来说十分重要。这些示例表明，与安全相关的风险可能会影响患者的健康，具体取决于医疗设备的预期用途。

(资料性附录)

未采用 ISO14971 设计的部件和器械

G.1 总则

本指南并不替代 ISO 14971: 20XX 中的要求, 并假定制造商已经建立了符合 ISO 14971: 20XX 的风险管理过程。

有些情况下, 针对医疗器械的每个部件, 制造商可能并未遵循 ISO 14971: 20XX 中描述的医疗器械每个组成部分的所有过程和要求, 例如专利部件、软件部件、原本非医疗用途的子系统或已上市的医疗器械。在这种情况下, 制造商的风险管理文档用以证明符合 ISO 14971: 20XX 可能是有限的和不充分的。然而, 在大多数情况下, 关于医疗器械及其部件的大量信息是可以获得的。例如, 通过评审器械或市场上类似器械或技术的生产后数据可以获得关于器械实际使用情况的信息。有关的生产数据和以前编制的与安全有关的文件也可以获得。

本附录旨在为制造商提供指南, 说明如何利用现有信息建立一个今后可维护的初始风险管理文件。

注: 本附录中的“医疗器械”包括医疗或非医疗来源的子系统、部件和软件部件。

使用上述可获得的信息, 制造商可以建立风险管理文档, 作为特定器械建立初始风险管理文件的基础。该文档可以作为充分的证据, 证明特定器械的风险是可以接受的, 并且该器械对于其预期用途是安全的。另一方面, 制造商可以决定适当采取额外的风险控制措施。例如, 与公认的技术水平相比, 为了全部符合 ISO 14971: 20XX, 需要采取额外活动。

G.2 风险管理计划

ISO 14971: 20XX 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件以证明器械对于其预期用途是安全的活动。风险管理计划的强制性条款在 ISO14971: 20XX 中给出。

在建立风险管理计划时, 应特别注意:

- 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、停用和处置, 如适用);
- b) 责任和权限的分配;
- c) 今后风险管理活动评审要求;
- d) 医疗器械的风险可接受性准则, 基于制造商确定的可接受风险方针;
- e) 评价综合剩余风险和其可接受性准则的方法;

注 1: d) 和 e) 下的准则可以由生产和生产后信息支持。

f) 验证活动, 对现有风险控制措施和认为必要的新风险控制措施进行的验证活动。

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器械相关的风险是否可以接受;

注 2: 设计文档或其他文档可包含一些验证证据。

G.3 风险管理文档

由于医疗器械没有按照 ISO 14971: 20XX 设计, 制造商需要开始为医疗器械建立一个风险管理文档。普遍认为, 在没有与器械有关的危险和危险情况的可追溯性记录的情况下, 若干风险控制措施已经可以实施。因此, 一种途径可以从识别该医疗器械已采用的技术方案开始, 然后识别由技术方案控制的危险和危险情况。这些技术方案可以是固有的安全设计、防护措施或安全信息。换句话说, 从现在起, 它们被视为风险控制措施。

这样建立风险管理文档的方法由下列几个步骤组成:

1. 需要将器械的预期用途、可合理预见的误用以及与安全有关的特征形成文件。可合理预见的误用可以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有关的特征。
2. 需要识别医疗器械已经采用的所有技术方案, 这些技术方案可以被考虑为风险控制措施。
3. 需要识别与器械相关的所有危险和危险情况, 以及可能造成的伤害。
4. 需要验证是否存在未实施风险控制措施的危险或危险情况。这种情况下, 制造商需要估计和评价风险, 并从现在起应用 ISO 14971: 20XX。对于已实施风险控制措施的危险和危险情况, 制造商需要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没有判定为可接受的剩余风险, 制造商需要考虑进一步的风险控制并应用 ISO 14971: 20XX。

5. 需要对每个被识别的危险和危险情况提供风险控制措施的可追溯性。可追溯性可以通过以下要素形成文件:

- 已识别的危险和危险情况;
- 可能发生的伤害;
- 风险控制措施;
- 实施的验证;
- 任何剩余风险的可接受性。

6. 需要根据 ISO 14971: 20XX, 第 8 条评价综合剩余风险, 并根据 ISO 14971: 20XX, 第 9 条对风险管理计划的执行情况进行评审。

这些步骤中产生的记录与文件形成了初始风险管理文档。

附录 H
(资料性附录)
体外诊断医疗器械指南

1 总则

H.1.1 体外诊断医疗器械风险管理

本附录的目的是为 ISO 14971:20XX 体外诊断医疗器械的特定应用提供指南。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,旨在补充本文档提供的通用指南。对医疗器械使用者、其他人员和环境的风险在本文的其他部分进行了说明。(本指南中的)这些指导原则可能对其他诊断医疗器械的制造商也有帮助。

本附录中,“临床医生”作为一般术语,指的是医疗卫生保健提供者,为患者看诊,申请、解释体外诊断检查结果,并依据检查结果采取活动。有关体外诊断行业和实验室医学中常用的其他术语定义参见 ISO 18113-1^[36]。

由于体外诊断医疗器械及其预期用途的多样化,本附录只能提供通用性指南,旨在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,制订和实施有效的体外诊断医疗器械的风险管理计划。它们并非详尽无遗,也不一定代表所有体外诊断医疗器械的最佳实践。制造商需要确定适用于各自特定体外诊断医疗器械的内容。

H.1.2 体外诊断医疗器械风险管理的背景

对于体外诊断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”的扩展事件顺序为特征,“合格中间人”如,经过培训使用体外诊断医疗器械进行体外诊断检查的操作者和依赖检查结果的临床医生。国际医学实验室质量和能力标准对医学实验室实施风险管理过程提出了要求(参见 ISO 15189:2012^[36])。为支持这一要求,ISO 22367^[40]正在制订中,它将使医学实验室的风险管理过程与 ISO 14971:20XX 保持一致。

源自于制造商风险管理过程的安全信息和剩余风险披露是实验室风险管理过程的重要输入。体外诊断医疗器械用户对公示剩余风险的性能数据和控制风险的安全信息的需求,以及实验室使用体外诊断医疗器械的反馈,是制造商设计控制和风险管理过程的重要输入。在开发或更改体外诊断医疗器械时,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体外诊断医疗器械时,任何无法通过设计或防护措施控制的风险,都会连同控制这些风险所需的安全信息一起转移给实验室。制造商还在随附文件中披露了任何剩余风险,以便实验室主任评估这些风险并确定其可接受性。

制造商提供安全信息告知体外诊断医疗器械的操作人员,但不能影响对检查结果预订、接收和采取措施的临床医生的行为。

某些体外诊断医疗器械预期由临床医生用于床旁,而自测体外诊断医疗器械实际由患者使用。虽然这些医疗器械也可能存在类似的风险场景,但是这类用户控制风险的能力可能会更加有限。床旁和自测器械的设计需要有适合于预期用户和实验室外预期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用

大多数体外诊断医疗器械有两种使用者需要考虑:

- a) 完成全部或部分检查的使用者(“分析用途”);
- b) 接收、解释检查结果并根据结果采取行动的临床医生(“临床用途”)。

预期用于自我测试的体外诊断医疗器械,患者可能是唯一的使用者。

确定临床应用时需要考虑的其他问题包括：

- 检查结果是否用于：
- 诊断以治愈、减轻、治疗或预防疾病或其他病症？
- 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？
- 筛查人群存在或缺失特定标记？
- 预测替代疗法的有效性？（“伴随诊断”）
- 预测罹患疾病的风险？
- 其他临床应用？（包括潜在的“标签外”用途）
- 结果用于检测、诊断、预测或监测的损伤、疾病或病症是什么？
- 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？
- 检查结果在医疗决定中所扮演的角色：
 - 作为立即作出医疗决定的依据？
 - 结合其他相关信息以指导医疗决定？
- 哪些患者群体将主要受益于体外诊断检查？
- 是否有明确禁忌的患者群体？

H.2.2 与患者安全有关的特征

H.2.2.1 总则

除了与其它医疗器械相同的化学、机械、电气和生物学特征外（见附录 A），体外诊断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征。一些体外诊断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体外诊断医疗器械还可以具有与将检查结果或辅助信息发送到医疗决策所需位置的能力相关的特征。不满足性能、可靠性或通信要求可以引发可能对患者造成伤害的事件序列。

H.2.2.2 患者安全相关的性能特征

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、假性正常或假性降低的结果可能会影响诊断，导致不适当或延迟的治疗，并导致患者伤害。伤害的类型和严重程度取决于医学决定水平的偏差大小。

定量体外诊断医疗器械的相关性能特征可以包括：

- 测量值的准确度（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）；
- 检测限（可以可靠检测的最低量）；
- 定量限（可以准确测量的最低量）；
- 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。值通常根据分类度量表给定或报告为数量范围，并且可以用数字表示（例如在指定值的范围内，或者大于或小于特定的量，效价或连续稀释），或相对表示（例如，+3、+2、+1 或微量）。半定量检查的常见示例如尿液“试纸”、检测酮存在的片剂和血清学凝集程序。

如果检查结果报告为在低功率或高功率场中观察到的细胞数量，则显微镜检查也可以被认为是半定量的。例如，尿液显微镜检查可能在高倍视野下显示 0 到 5 个红细胞。

半定量体外诊断医疗器械的性能特征包括：

- 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）；
- 检测限（可靠检测的最低数量）；
- 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，报告结果为阳性、阴性或不确定。截止值和相关数据库可以定义阳性或阴性结果。当分析物不存在时的阳性结果或当分析物存在时的阴性结果会影响诊断或治疗。

定性体外诊断医疗器械的性能特征包括：

- 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征

当临床医生依靠体外诊断检查结果作出紧急医疗决策时，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。

体外诊断医疗器械的可靠性特征包括：

- 系统可靠性（平均故障间隔时间、平均故障时间）；
- 部件兼容性（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 患者安全相关数字信息技术特征

正确的患者和样本标识显然是必须的。有些检查还需要患者、样本或检查的辅助信息，以便正确解释结果。如果体外诊断医疗器械设计目的为收集并报告具有检查结果的此类信息，导致数据损坏或更改的医疗器械特征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包括：

- 正确的患者姓名和样本标识；
- 患者详细资料（年龄、性别、人口、遗传因素、药物、营养状况）；
- 样本详情（样本类型、描述、采集时间）；
- 测量详情（测量程序、测量单位、测量不确定度）；
- 解释（诊断、治疗建议）；
- 使用详情（分割值、参考区间）。

影响患者安全的数字信息技术特征包括：

- 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（联网或移动）；
- 模拟体外诊断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）；
- 无防护的数据传输（例如，静电放电敏感性）；
- 数字数据存储（例如，易受损坏、操控或删除）；
- 中断其他的连接设备（导致额外的危险）。

H.2.3 对患者已知和可预见的危险

H.2.3.1 危险识别

从患者的立场看，体外诊断检查结果被视为危险，如果它导致：（1）可能导致伤害的不适当的医疗措施；（2）缺乏预防伤害的必要的医疗措施。以下一般危险（源）可能引起或促成潜在的有害的医疗决策。具体的危险源需要根据偏差的幅度和方向、延误的程度，或不正确或缺失的辅助信息来确定。

a) 不正确的检查结果

对于定量和半定量检查，如果检查结果与正确值的偏离超出临床应用所需的偏差限度，则可认为结果是不正确的，分析性能需求通常建立在设计输入过程中。

一些医学决策可能会受到检查结果大小的影响，因此错误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

b) 延迟的检查结果

检查结果或其辅助信息被认为是延迟的，如果它是医疗决定所需要的，并且临床医生没有及时收到它以支持关键的治疗或干预决定。可以建立标准定义临床上显著的医疗应用（例如，紧急护理情况）延迟的构成。

c) 伴随结果的错误信息

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

H.2.3.2 识别故障条件下的危险

体外诊断医疗器械在使用过程中发生故障会导致 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，试剂盒、校准品、质控品）；
- 无溯源的赋值（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（例如，移液器）；
- 测量不精密度（例如，系统级）；
- 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、部件、附件）；
- 软件/固件易被入侵（例如，数据修改或被盗窃）。

H.2.3.3 识别正常使用时的危险

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，体外诊断医疗器械技术的固有局限性有时仍会导致 H.2.3.1 中描述的一种或多种对患者的一般危险。每个检查结果都会受到不可避免的变异来源的影响。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有可能成为个别患者的危险。

正常使用中可能发生的危险可能包括由于以下原因导致的不准确的结果：

- 由统计分配的分割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；
- 与定量检查程序相关的测量不确定度（性能宣称通常代表 95% 的测量结果处于医学上定义的目标限度内）；
- 将结果错误分类为“异常”或者超出“正常”参考区间（依据“正常”人群研究结果的中心 95% 而经验确定）；
- 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）；
- 患者样本基质的多变性（即“基质效应”）；
- 仪器部件的可靠性有限。

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。正常使用中危险情况的发生被认为是不可避免的剩余风险。

H.2.3.4 识别使用错误的危险

使用错误可能导致一个或多个 H.2.3.1 中描述的一般危险。非常规的实验室过程特别容易导致使用错误。在体外诊断医疗器械设计和开发过程中，可用性工程过程可以识别和潜在预防可合理预见的的使用错误（例如，由易于预测的人类行为所导致）。有关信息和指导参见 IEC 62366-1^[17]。

在医学实验室或床旁，可能导致体外诊断危险的使用错误包括：

- 忽视特殊要求（例如，在正常实验室规程之外的要求）；
- 未按顺序执行操作（例如，指令不清楚，用户界面混乱）；
- 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，在器械准备好测量前）。

H.2.3.5 识别可合理预见的误用导致的危险

可用性工程过程还可以帮助体外诊断医疗器械制造商预防可合理预见的误用的危险和危险情况。指南参见 IEC 62366-1^[17]。

可合理预见的误用的示例如下：

- 在阅读说明书或完成培训前使用体外诊断医疗器械；
- 无视明确的警告、指示或其他安全信息；
- 采集不适当的样本类型（例如，应为枸橼酸钠血浆时，用为血清）；
- 报告了禁忌或临床用途未经确认的检查结果；
- 在重症监护病房内使用自测体外诊断医疗器械（例如，准确度可能不足）；
- 使用未经验证的第三方校准品、试剂盒、质控品或者附件；
- 在不正确的条件下储存材料（例如，应冷藏时使用室温）；

- 在指定环境条件以外操作体外诊断器械；
 - 禁用、覆盖、或未能启用安全功能（例如，减少使用者的烦恼）；
 - 忽视执行规定的仪器维护工作；
 - 连接至不具备充分网络连接性和安全性的信息系统。
- 患者进行自我检测时，可合理预见的误用包括：
- 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储存试纸条（例如，过热的车辆）。

H.2.4 识别潜在的伤害

ISO 14971: 20XX 要求制造商依据可能发生的伤害概率和严重度，估计每种已识别的危险情况相关的风险。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（例如受伤）以确定合适的严重度水平。

对于某些检查，单个危险情况可能导致几种不同的伤害，表现为一系列严重程度。制造商需要确定应将哪些伤害包括在风险分析中，以确保对健康的高度保护和安全性，并记录理由。所有经过合理判断可能发生的伤害都应包括在内。如果上市后监测显示有其它伤害发生，它们也可以增加到风险分析中。

注：进行风险分析而识别潜在伤害并确定其严重程度和发生概率需要了解体外诊断检查结果的医学用途。

因此，有资格的医学专家参与风险分析是必不可少的。

有助于识别和分类潜在伤害的问题包括：

- 预期用途是否是严重医疗状况下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人群中的其他人？
- 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、阿尔茨海默病易患体质、乳腺癌风险增加等）如果是，假阴性结果是否会导致可预防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措施和潜在的伤害？
- 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效果丧失和随后的伤害？假阳性结果会产生有害后果吗？
- 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斥反应？
- 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显著延迟会带来什么伤害？
- 如进行医疗干预，结果不可逆（例如，手术切除、堕胎），还是结果可逆（是否需要进一步的医疗干预）？
- 医疗器械是否需要连接互联网，是否会发生患者数据的修改或被盗（例如，安全性不足）？

确定伤害严重度的指南见 5.5.4。

H.2.5 危险情况识别

ISO 14971: 20XX 要求制造商编制出一套全面的危险情况以进行风险分析，但由制造商负责确定用于风险分析目的的危险情况的构成因素（见指南 ISO 14971: 20XX，附录 C.4）。一种方法是评审事件顺序。参见 H.2.6 章节以识别（1）使患者暴露于危险中的事件或情况；（2）超出制造商或设备用户任何合理控制手段的事件或情况；以及（3）使制造商能够开展客观风险分析的事件或情况。

体外诊断医疗器械危险情况示例包括以下事件：

- 临床医生收到不正确的实验室结果；

- 延误治疗（例如，体外诊断医疗器械故障）；
- 延迟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）；
- 报告患者结果的不正确信息（例如，网络故障）。

以下问题有助于分析与不正确结果有关的危险情况：

- 在存在其他诊断指标的给定场景中，体外诊断检查的重点是否为假阴性或假阳性结果仍然显得“可信”，因而在决定临床行动/无行动处置的过程之前不会做进一步确认？
- 是否只有少量的、有限的或没有有其他诊断工具有效地去确认或否认可能的假阳性或假阴性体外诊断检测结果？

H.2.6 可预见的事件序列识别

H.2.6.1 总体考量

识别和分析可以导致危险情况和潜在的伤害过程的可合理预见的事件序列或者事件组合，对于评估可能发生的伤害概率是必需的。理解这些活动和事件还可以帮助制造商选择危险情况进行风险分析，并识别降低风险和风险控制的机会。

待分析的特定事件序列取决于特定体外诊断医疗器械及其预期用途。在概述事件序列时，考虑预期用户的知识、技能和能力，预期使用环境，以及任何其他可能促成风险或降低风险的因素。

虽然医学实验室采用对检测错误的控制程序，但要考虑其在检测特定失效模式方面的有效性。零星的随机故障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，并且如果它影响诊断或治疗决定，则可能导致不适当的或延误的治疗并且可能对患者造成伤害。

体外诊断医疗器械的故障如果导致关键医疗决定所需的体外诊断结果的可用性显著延误，则可能产生危险情况。用户承担着制定备份和恢复计划的主要责任，但设备故障可能是一个促成因素。临床上明显的延迟更可能发生在床旁或支持紧急护理的实验室中，而不是在进行常规检查的实验室中。

H.2.6.2 事件序列的描述

体外诊断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，例如由器械使用者（例如，医学实验室或床旁操作员）执行的活动，以及由申请检查结果的临床医生作出的医疗决策和活动。

描述应从初始事件（通常是正在分析的危险的原因）和直接受制造商控制的事件开始，过程逻辑经由器械用户可预见的决策和活动，以导致每种已识别伤害的临床决定和活动作为可预见的输出而结束。

描述应尽可能详细以捕捉主要的促成因素和降低因素，但不能过于详细，以免无关紧要的原因妨碍分析。将复杂序列划分为较短的片段有助于确保分析由具备专业知识的人员开展。这种方法在 H.2.7.2 中讨论。图示（例如流程图、事件树）有助于记录和沟通复杂的事件顺序。

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通常是制造商的质量管理体系失控而发生。制造商直接控制的可能导致故障条件或潜在使用错误的活动：

- 设计和开发；
- 器械标签；
- 制造和供应商管理；

- 产品库存和分销；
- 设备维修；
- 培训和产品支持。

b) **体外诊断医疗器械用户控制的事件**

使用错误和设备故障可能发生在实验室或床旁的器械运行期间。用于预防或检测危险的活动以及使用者采取的响应活动由实验室或护理场所直接控制。这些器械使用者将制造商提供的保护措施和安全信息纳入其自身的风险管理过程。

体外诊断医疗器械的使用者也可能通过误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，或网络安全保护。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体外诊断医疗器械的其他使用者控制之下。当在体外诊断医疗器械用户的控制下分析事件顺序时，需要考虑预期使用者的能力和使用环境。

使用体外诊断医疗器械制造商提供的信息、材料和支持，通常由用户控制的活动示例包括：

- 使用 IVD 医疗器械用于选择、使用和收集样品的收集器
- 样品采集、处理和储存患者样品；
- 系统的安装和建立，包括操作人员的培训和性能验证；
- 对附件、耗材和零件（包括过期日期的管理）的选择、准备、使用和储存
- 校准活动和计量溯源性；
- 试剂的储存和制备；
- 质量保证活动（例如，质量控制、能力验证、患者结果差值控制）；
- 审核和报告检查结果；
- 与临床医生沟通（预期用途、禁忌症、召回结果、监测）；
- 本地网络和互联网连接；
- 生物危险废物处理；
- 设备保养、维修、退役和废弃处置；
- 应急和恢复计划（例如，备份系统）。

c) **临床医生控制的事件**

临床医生控制下的事件通常从接收和审查检查结果开始，并决定是否接受检验有效。较大的偏差可能会被质疑和拒绝（例如，与其他诊断信息相矛盾的结果、不符合生理的异常结果），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：明确排除在 ISO 14971:20XX 范围之外的“临床决定”，是指是否使用特定医疗器械或体外诊断医疗器械的临床决定，而不是指受体外诊断不正确的或延迟的结果影响的临床决定。

当在床旁使用体外诊断医疗器械时，如医生办公室、诊所或专科医院，临床医生通常参与收集、处理、清点和存储患者样本，并可以执行许多或全部的体外诊断医疗器械使用者的活动。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以更大。为风险分析识别的事件序列需要反映体外诊断医疗器械在实际使用环境中的使用。

风险分析应考虑任何可合理预见的临床使用。临床使用禁忌或未在随附文件中明确说明的临床使用可被视为可合理预见的误用，用于风险管理。需要考虑的是，为医学实验室的体外诊断医疗器械使用者编写的随附文件并不总是能够到达申请并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策和活动示例，如下：

- 将结果与预期值进行比较；
- 要求确认或证实检查；
- 在无检查结果下进行（如果延迟）；

- 建立临床诊断;
- 开始或停止治疗。

H.2.7 伤害发生总概率评估

H.2.7.1 总体考虑

风险分析应当考虑 H.2.6.2 中描述的完整事件序。患者受到伤害的总概率是与特定危险和潜在伤害相关的事件序列中每个事件的累积概率。用于评估总概率的最佳方法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通用知识和与正在分析的体外诊断医疗器械相关的专业知识的人员完成,专业知识包括体外诊断医疗器械的分析和临床用途以及所涉及的技术。H.7 给出了将不同风险分析方法应用于常见体外诊断医疗器械场景的示例。

对于涉及短事件序列的器械,例如自我检测或床旁设备,风险分析可以相对明确。可以组建一个跨职能的专家团队,基于他们的集体专家判断,加上可获取的分析和临床信息(例如,上市前的研究、类似产品的经验、相关的上市后监管),对每一种识别的危险情况进行伤害概率评估。跨职能团队需要包括熟悉该器械的设计、结构、使用和服务、使用环境(如医学实验室、床旁、患者家中)以及检查结果临床用途的专家。对于设计用于与其他设备和/或网络通信的包含软件的设备,可能还需要连接性和安全性方面的专家意见。

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家意见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,在下面章节会有详细解读。

H.2.7.2 使用“ $P_1 \times P_2$ ”方法的特别指南

ISO 14971:20XX 图 C.1 所示的方法可用于具有扩展事件序列的复杂风险场景。危险情况发生的概率(P_1)和危险情况导致的伤害概率(P_2)由相应的专家分别评估,然后 P_1 和 P_2 结合得到伤害的总概率。

对于预期用于医学实验室的体外诊断系统,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 (改编自 ISO 14971:20XX 图 C.1) 以医学实验室的血液分析仪进行血糖测试为例说明“ $P_1 \times P_2$ ”方法对体外诊断医疗器械的应用。

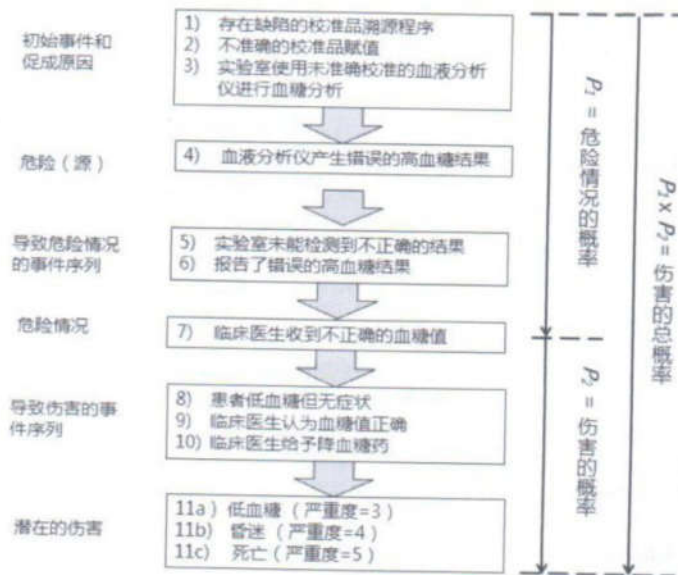


图 H.1 - 使用体外诊断医疗器械产生不正确血糖测量的医学实验室的危险，危险情况和伤害之间的关系以及促成事件顺序的示例

该示例中的危险是由制造商未准确赋值的校准品值导致不正确（假性升高）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，但是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，体外诊断医疗器械随附件中的安全信息可能会减轻这些事件。存在的后续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）定义为超出了制造商或医学实验室的合理风险控制措施的事件。在涉及不正确体外诊断结果的案例中，用于支持有效风险分析的危险情况的合理定义是临床医生收到不正确的结果。

在此风险分析中，危险情况（ P_1 ）的概率和伤害（ P_2 ）的概率可以由相应方向的专家分别评估，如上所述。然后将这两种概率结合起来，给出伤害总概率的评估。

P_1 : 危险情况发生概率

负责评估 P_1 的人员需要熟悉该器械的设计、结构、使用和服务，充分理解使用环境（如医学实验室、床旁、患者家中）。分析 P_1 事件通常不需要医学应用的详细知识。

P_2 : 危险情况下发生伤害的概率

负责评估 P_2 的人员需要熟悉体外诊断结果的医学应用。 P_2 可以通过专家临床判断和类似体外诊断检查的经验来评估，通过不良事件数据、医学文献和上市后监测来获知。评估 P_2 时通常不需要详细了解体外诊断医疗器械的性能或结果是如何产生并报告的。

H.2.7.3 伤害发生概率评估指南

表 H.1 中的问题旨在促进对事件顺序的系统分析和指导适当的概率评估的开展。这些问题应根据体外诊断医疗器械的类型、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-问题 4 与事件顺序的分析部分有关,可以帮助制造商评估 P_1 。问题 5-问题 8 与事件顺序的临床部分有关,可以帮助制造商评估 P_2 。

表 H.1 一帮助评估伤害发生概率的问题

有多大可能性……	考虑点	带格式表格
1. 初始事件会发生 (例如器械故障或使用错误)?	<ul style="list-style-type: none"> —预防/检测措施效果如何? —可以估算概率吗?如果不能,则设定概率=100% —频率是否取决于使用环境?估算最坏情况。 —可以在可合理预见的组合中发生特定故障、失效模式和/或使用错误从而形成危险吗? 	
2. 体外诊断医疗器械故障或使用错误会产生不正确的结果?	<ul style="list-style-type: none"> —旨在确保准确结果的措施效果如何?或者能否检测出分析性能的不可接受的变化? —常规的质控程序是否会拒绝不正确的检查结果? —在预期使用的环境中(例如医学实验室、床旁、患者家中),是否有促成或减轻的因素?分别分析不同的使用环境。 —器械是否及时提示使用者改正问题(例如:“血量不足”),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会被报告给临床医生?	<ul style="list-style-type: none"> —异常的检查结果是否与危急值比对审核,或向临床医生报告之前是否已经过核实? —报告前是否会自动确认结果是罕见或非预期的(例如新生儿筛查程序)? 	
4. 报告检查结果(或辅助患者信息)时会出现临床上明显的延误?	<ul style="list-style-type: none"> —结果对于及时的诊断或治疗决策是否至关重要? —延误多久会造成危险的情况? —排除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误? —确保及时获得结果的备份程序是否是标准实验室/医疗实践的期望? —是否可以进行第二次检查,且在关键结果所需的时间内报告检查结果? 	
5. 临床医生会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,诊断 II 型糖尿病需要两个独立的糖化血红蛋白测量)? 	
6. 由于结果不正确会出现不正确的医疗决策和/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? —结果是否会成为作出特定医疗决策的首要依据?还是仅用于体征、症状、其他检查结果和患者病史的场景? —阳性或“异常”结果是否总会导致特定的医疗决策或治疗,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医疗条件? 	
7. 会因未能及时得到体外诊断结果而导致一个不适当的医疗决策或活动?	<ul style="list-style-type: none"> —考虑到临床医生可获得的体征、症状、病史和其他检查结果,用来指导干预或治疗的结果需要到何种程度? 	
8. 会因不适当的医疗决策或活动导致对患者的伤害?	<ul style="list-style-type: none"> —对患者立即做出决策或干预有多紧急? —不适当的活动或延误采取必要活动会产生什么医疗后果? —患者的医疗或生理状况会多大程度促成(或降低)伤害的可能性? —对患者以外的人员是否有影响,例如: <ul style="list-style-type: none"> —传播性病原体传染他人的可能性? —胚胎或胎儿暴露于致畸剂或辐射? 	

- | |
|---|
| <ul style="list-style-type: none"> —由于不必要的暴露而产生抗菌素耐药性？ —错误拒绝移植器官？ —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

由于临床诊断人员的决定和措施大多超出制造商的合理的风险控制措施,因此风险控制活动需要关注在制造商控制下降低事件的概率。这包括提供安全信息和对实验室中使用者的安全信息的有效性的验证。如果制造商使用 $R \times B$ 方法,这将意味着风险控制措施可以直接降低 R 的概率。

H.3.2 设计和制造的固有安全

患者风险通常可以通过降低报告错误结果或发生临床显著延误的概率(例如,通过确保性能特征满足医疗要求)来减少。对于血糖、电解质、酶和治疗药物等分析物的定量检测,限制偏差的幅度可以减少不适当的医疗决定的频率。

控制检查结果准确度和可靠性的设计特征的示例包括:

- 校准品值的正确性(例如,溯源至公认的标准参考物质);
- 测量不确定度(例如,测量系统的精密度);
- 体外诊断试剂(例如,优化组分)的分析特异性;
- 检测限或定量限(例如,改进检测技术);
- 仪器的可靠性(例如,减少硬件或软件故障);
- 区分阳性和阴性样本(例如,强健的分割值);
- 消除容易出错的程序步骤(例如,自动化、防错);
- 部件版本可追溯性和阳性样本识别(例如,条码);
- 软件功能化(例如,最新的编码标准);
- 系统易用性(例如,可用性工程);
- 数据网络和互联网连接(例如,安全);
- 减少试剂或校准品的变异(例如,批次规格、供应商管理);
- 防止虚假结果(例如,间歇性的元件故障);
- 试剂、校准品或质控品的稳定性(例如,微生物控制品)。

H.3.3 医疗器械或制造过程中的防护措施

体外诊断器械或试剂盒用于预防可能导致错误或延误结果的情况的检测特征示例包括:

- 确保足够样本量的液位感应器(例如,检测“吸取量不足”);
- 故障检测系统(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);
- 检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;
- 核实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;
- 对供应组分的进货检验;

过程中的接受测试和最终产品的接受测试。

注：对由用户实施的检测方法的建议，如质控测试、确认检查或危急值提示，都被视为安全信息，而非防护措施。

H.3.4 安全信息

使体外诊断医疗器械使用者能够预防危险或危险情况发生的信息可成为有效风险控制措施，如果（1）这些信息指导使用者采取或避免什么活动以预防危险情况，（2）预期使用者有能力执行指令，（3）如果需要，按理他们可以按预期执行。忽视这些信息的不良后果必须是明确的。

医学实验室或其他预期使用者的风险管理过程需要安全信息。使用者所需的控制对患者风险的安全信息的示例包括：

- 禁忌症或临床应用；
- 样品收集、储存和准备的特殊要求；
- 禁止使用不适当的样本类型的警告；
- 使用者可检测到的干扰物质（例如，可见溶血）；
- 关于危险的警告，包括可能的使用错误；
- 不兼容的系统部件和附件；
- 共用设施和设施规格（例如，使用环境）；
- 试剂储存要求和有效期；
- 安装、维修和废弃处置信息；
- 质控建议；
- 经确认的测量间隔和样品稀释的说明；
- 生物参考区间和医学决定水平；
- 经确认的重复使用物品的清洁方法；
- 预防性维修要求和程序；
- 接口和连接性规范；
- 系统故障时的备份和恢复建议。

注：体外诊断医疗器械标签的安全信息在可以参考法规或国际标准，如 ISO 18113 系列^[26]。

H.3.5 标准和分析性能准则的作用

为数不多的国际产品标准规定了体外诊断医疗器械的最新技术水平。例如 ISO 15197^[26]（血糖自我监测设备）和 ISO 17593^[26]（口服抗凝治疗自测用体外监测设备）。然而，一些体外诊断医疗器械的国际标准涉及固有安全的某些方面，这些标准可以提供证据，表明来自特定危险情况的风险已经降低到最新技术水平。

例如，ISO 17511^[26]定义了一种过程，用于建立体外诊断校准品的值到更高计量学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。医学实验室溯源联合委员会（JCTLM）在 <http://www.bipm.org/jctlm/> 网站上维护体外诊断参考测量系统数据库。使用 JCTLM 认可的参考测量系统符合 ISO 17511^[26]，可以提供制造商已将与检查结果准确性相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体外诊断标准示例包括 ISO 17822-1^[26]（核酸检测系统）、ISO 20776^[26]（抗菌药物）、ISO 20916^[26]（临床性能研究）、ISO 23640^[26]（体外诊断试剂稳定性）、IEC 61010-2-101^[11]（体外诊断器械安全性）、IEC 61326-2-6^[13]（体外诊断器械电磁兼容性），以及 IEC/ISO 80001 系列^[19]（联网医疗器械）。

广泛认可的某些分析物性能标准可以在世界卫生组织（WHO）、国际和国家公共卫生机构、标准组织、专业医学会和主管当局的出版物中找到。

制造商有责任证明这些标准和性能标准适用于其特定体外诊断医疗器械及其预期用途的程度，且证实已按照 ISO 14971 的要求考虑所有相关的危险情况。

H.3.6 用户教育培训

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

例如，口服抗凝监测系统的产品标准（ISO 17593^[34]）要求制造商为临床医生提供确认过的培训计划并为患者和这些器械的其他用户提供教育计划。制定国际标准的专家认为，这些风险控制措施必须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，请考虑：

- 器械使用者的使用环境、资质和能力可能差异很大；
- 世界各地的质量控制和质量保证实践不统一；
- 向体外诊断医疗器械使用者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测的临床医生那里。

H.4 受益-风险分析

第 7.4 条款为进行受益-风险分析提供了指导。

如果不太可能直接描述体外诊断医疗器械的受益，可以建立监测哨点。示例包括体外诊断医疗器械识别特定疾病的能力，在疾病的不同阶段提供诊断、预测未来的疾病发作、和/或识别患者对给定治疗可能反应的能力。

H.5 剩余风险披露

H.5.1 总则

附录 D 说明了公示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体外诊断医疗器械的风险与其受益，并就风险可接受性做出知情决策。制造商需要考虑医学实验室和临床医生所需要的信息，以评估固有的剩余风险，并确定进一步降低风险措施的必要性。

体外诊断医疗器械剩余风险的公示可以采取不同的形式，包括随附文件中提供的关于性能规格（“宣称”）、体外诊断医疗器械或检查程序的局限性，和/或制造商无法消除的潜在危险和危险情况的信息。剩余风险的公示是在向用户提供安全信息的风控措施之外进行的。

注：体外诊断医疗器械随附文件中剩余风险的公示也可由国家法规或国际标准规定，如 ISO 18113 系列标准^[35]。

H.5.2 性能规范

描述相关的分析性能特征和临床性能研究结果（见 ISO 20916^[36]），允许医学实验室主任和临床医生来评价体外诊断医疗器械在其预期医疗应用中的效用。

性能特征的描述需足够详细，以便实验室或其他用户可以验证体外诊断医疗器械能否按制造商的预期执行，能够确定与检查结果相关的测量不确定度，并且能够知道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 给出了潜在相关性能特征的示例。

H.5.3 体外诊断医疗器械的局限性

ISO 18113-1^[36]要求随附文件公开体外诊断医疗器械的分析和临床局限性。这些局限性描述了体外诊断医疗器械可能无法按预期执行的情况，因此可以作为一种公示剩余风险的方法，例如：

- 干扰物质无法被用户察觉（例如，药物、生物代谢物）；
- 性能特征可能不适用特定的患者人群；
- 被测值超出范围（测量范围外的性能特征未得到确认）；
- 参考范围或医学决定水平可能不适用于患者群体；
- 预期用途的主要样本类型未被确认；
- 可能影响检查结果的情况和因素尚未被研究。

H.5.4 公认的使用局限性

一些可能导致危险情况的事件或环境被认为是医学实验室的常识。这些风险是通过医疗标准或实验室实践来控制的，通常不会在使用说明书中描述以避免用户陷入不必要的细节。制造商应考虑是否需要额外的信息以确保用户了解与这些事件或环境相关的风险，记住，传递如此多风险的危险在于，可能使用户难以理解哪些需要重点控制。例如：

- 警告、指示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指令被认为是误用（见 H.2.3.5）。
- 预期机电设备偶尔会出现故障并需要维修，或使用超过有效期的生物材料可能变得不稳定和失效。
- 预期实验室将实施应变计划（例如备份系统或替代的实验室）以确保在这些情况下基本服务可用（见 ISO 15189^[36]）。

H.6 生产及生产后活动

H.6.1 总则

建立有效的体系来监测生产后信息（投诉、不良事件和不合格品）对制造商来说是个挑战，特别是预期在医学实验室中使用的器械，因为监测危险情况和伤害实际概率的可靠数据很难获取。监测危险的发生及其原因更加直接，因为这些反馈可以由经历这些事件的器械用户直接提供。应收集和分析器械故障、使用错误和医疗事故的报告，并将观察到的频率与预期频率进行比较（允许繁忙实验室漏报的可能性）。

在建立生产后信息收集体系时，制造商可利用产品风险分析对预期的伤害、危险情况、危险及其原因制定分类和编码方案，便于确定基于风险的调查优先级。事件可以根据潜在伤害的严重度估计以及不正确或延误的结果将导致伤害的概率进行分类。该工具可用于处理投诉、上市后监测和不良事件报告以及产品故障调查。

H.6.2 监测分析性能

有效的体外诊断医疗器械上市后监测体系需要主动监测来自内部和外部可用的性能分析数据。

性能数据的内部来源可以包括例行地收集在产品放行测试、赋值活动、稳定性监测过程和产品故障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自愿参加外部质量控制和能力验证计划、用户性能评估以及仪器安装和服务活动所定期获得的数据。

H.6.3 监测临床表现

医学实验室通常无法知道报告的结果是不正确的，并可能导致不适当的医疗决策、介入或伤害，除非接收到临床医生的投诉。因此，任何报告的伤害严重度及概率应作为上市后监管的一部分仔细监测。

除了由主管当局监测客户反馈的临床事件，不良事件和召回数据库，来自公共安全机构、国家医学实验室协会和医学文献的报道都可搜索获取到类似产品新的和突然出现的危险或危险情况。

H.7 体外诊断医疗器械风险场景示例

H.7.1 总则

以下通用示例展示了常见类型的体外诊断医疗器械造成的危险情况的不同风险分析方法。这些示例并不预期代表唯一推荐的方法，也可能不适用于所有的器械或预期用途。体外诊断医疗器械制造商有责任决定适合其设备使用的风险分析方法。风险管理计划应记录整个生命周期中使用的方法，以及选择它的理由。

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，患者正在被一个向中央医学实验室申请了体外诊断检查的临床医生评估。如果体外诊断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) 初始原因发生（如器械故障或使用错误）；
- b) 体外诊断医疗器械产生临床上不正确的检查结果（即危险）；
- c) 器械使用者未能察觉到不正确的结果（或原因）；
- d) 器械使用者向临床医生报告不正确的结果；
- 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) 临床医生不当介入/不介入；
- h) 患者因医生的介入/不介入而受伤（即经受了伤害）。

在上述的场景中，来自于不正确结果的危险的事件序列经医学实验室扩展到临床医生，临床医生的决策和行动在很大程度上超出制造商合理的风险控制措施。出于风险分析的目的，当临床医生接收到不正确的结果，患者可以被认为处于危险情况下，因为这个事件后，患者暴露于来自不正确结果带来的临床决定和行动的受伤可能性中。

危险情况的这一定义允许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单独分析和记录，这些团队可以专注于与他们的专业知识相关的事件。这两部分分析的结果可以结合起来得到伤害的总概率。

这种方法有效地利用了技术和医学专家。它还允许为风险管理文档创建临床风险分析报告，以便在设计更改时用以支持风险分析的更新，以及确定在上市后监管期间遇到的源于任何危险情况的伤害的严重度和概率。

H.7.3 个人（自测）器械：血糖状态分类错误

在此场景中，被诊断患有2型糖尿病的患者定期监测他们的血糖浓度并在结果显示高血糖时自行施用抗血糖药物。虽然患者实际上是低血糖，但器械不正确地给出了一个升高的结果，抗血糖药物导致患者进一步低血糖。导致伤害可能发生的事件序列如下：

- a) 初始原因发生（如器械故障或使用错误）；
- b) 个人体外诊断医疗器械产生临床上错误血糖结果（即危险）；

- c) 患者未识别结果不正确;
- d) 不正确的结果误导患者作出不适当的治疗决策;
- e) 患者进行抗血糖治疗;
- f) 患者出现明显的低血糖 (即经受到伤害)。

在上述的场景中,由于不正确升高的血糖测量引起的对患者血糖状态的不正确分类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由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(如胰岛素自行给药)则患者被认为处于危险情况中。

在这种情况下,分离事件序列没有任何优势。整体风险分析可以由适当的技术和医学专家组成的单一跨职能团队有效地执行。

H.7.4 用于床旁的便携式体外诊断医疗器械: 危急结果延误

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,该机构进行体外诊断检查以评估潜在的器官损伤。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,器械显示错误信息且检查结果无法获取。导致伤害可能发生的事件序列如下:

- a) 初始原因发生(例如,器械故障或使用错误);
- b) 体外诊断医疗器械无法输出临床上必要的检查结果(即,危险);
- c) 器械使用者无法在规定时间内重复检查;
- d) 临床医生无法获得支持介入决策的结果;
- e) 临床医生在未受益于检查结果的情况下作出关键决策/行动;
- f) 医生的决策/活动不适合患者的病情;
- g) 患者因临床医生的活动/未采取行动而受伤(即,经受到伤害)。

在上述的场景中,事件顺序导致临床医生在没有评估内部器官损伤的情况下执行紧急程序。出于风险分析的目的,患者可被认为处在危险情况下,当执行紧急程序治疗时,这可能直接导致伤害(如,器官进一步损伤),或者当没有在需要的时间内收到预期的结果时,在此之后患者暴露于未受益于检查结果下的临床决定和行动中。

制造商可以考虑将整个事件顺序作为一个整体来分析,或根据更适合于客观风险分析的方法而将其划分为多个部分。