



中华人民共和国医药行业标准

YY/T XXXXX—XXXX

有源医疗器械失效模式、影响及危害性分析 (FMECA) 方法

Guidelines for failure mode effects and criticality analysis (FMECA) of active
medical device

(征求意见稿)

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 II

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 概述 2

 4.1 目的 错误！未定义书签。

 4.2 失效模式、影响及危害性分析 错误！未定义书签。

 4.3 FMECA 人员及计划性 2

5 DFMECA 3

 5.1 待分析对象定义 3

 5.2 DFMECA 过程 3

 5.3 DFMECA 后续工作 5

6 PFMECA 5

 6.1 待分析对象定义 5

 6.2 PFMECA 过程 6

 6.3 PFMECA 后续工作 7

附录 A（资料性） 医疗机器人机械臂关节 1 DFMECA 示例 8

附录 B（规范性） FMECA 报告模板 12

附录 C（资料性） 医疗机器人机械臂关节 1 PFMECA 示例 13

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。

本文件由××××提出。

本文件由××××归口。

本文件起草单位：

本文件主要起草人：

有源医疗器械失效模式、影响及危害性分析（FMECA）方法

1 范围

本文件规定了系统性开展有源医疗器械失效模式、影响及危害性分析(FMECA)的程序和方法。
本文件适用于各类有源医疗器械的失效模式、影响及危害性分析过程。

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 16174.1—2024 手术植入物 有源植入式医疗器械 第1部分:安全、标记和制造商所提供信息的通用要求

GB/T 2900.99—2016 电工术语 可信性

GJB/Z 1391—2006 失效模式、影响及危害性分析指南

3 术语和定义

GB 16174.1—2024、GB/T 2900.99—2016、GJB/Z 1391—2006界定的以及下列术语和定义适用于本文件。

3.1

有源医疗器械 active medical device

依靠电能或者其他能量源而非直接人体或重力产生的能量源以发挥其功能的医疗器械。

[来源:GB 16174.1—2024, 3.1]

3.2

产品 item

考虑的对象。

注1:产品可以是单个部件、元件、器件、功能单元、设备、分系统或系统。

注2:产品可以由硬件、软件、人员组成,或其任意组合。

[来源:GB/T 2900.99—2016, 192-01-01]

3.3

失效 failure

执行要求的能力的丧失。

[来源:GB/T 2900.99—2016, 192-03-01]

3.4

失效模式 failure mode

失效发生的种类。

注:失效模式可由功能丧失或发生其他状态的转变来规定。

[来源:GB/T 2900.99—2016, 192-03-17]

3.5

失效影响 failure effect

影响失效产品本身或之外的失效后果。

注:对一些分析,考虑单独的失效模式及其影响是必需的。

[来源:GB/T 2900.99—2016, 192-03-08]

3.6

失效原因 failure cause

导致失效的因素的集合。

注：失效原因可来源于产品的规范、设计、制造、安装、运行或维修。
[来源：GB/T 2900. 99—2016, 192-03-11]

3.7

失效模式及影响分析 failure modes and effects analysis; FMEA
针对子产品中可能的失效模式和失效及其对不同层次影响的研究的定性分析方法。
[来源：GB/T 2900. 99—2016, 192-11-05]

3.8

危害性分析 criticality analysis; CA
对产品中的每个失效模式发生的概率及其危害程度所产生的综合影响进行分析，以全面评价产品各种可能出现的失效模式的影响。
[来源：GJB/Z 1391—2006, 3. 1. 8]

3.9

失效模式、影响与危害性分析 fault modes, effects and criticality analysis; FMECA
针对失效模式和影响分析，并考虑失效模式发生的概率和影响严重性的定量或定性分析方法。
[来源：GB/T 2900. 99—2016, 192-11-06, 有修改]

4 概述

4.1 概述

FMECA 由失效模式及影响分析(FMEA)、危害性分析(CA)两部分组成。 FMEA是对产品进行分析，以识别潜在失效模式、失效原因及其对系统性能影响的系统化程序，CA是FMEA的扩展，目的是对产品中的每个失效模式发生的概率及其危害程度所产生的综合影响进行分析，以全面评价产品各种可能出现的失效模式的影响。只有在进行FMEA基础上，才能进行CA。针对设计对象的分析称 DFMECA, 针对过程对象的分析称 PFMECA。

本文件以严重度(S)、发生概率(O)和可探测度(D)的乘积进行危害性等级排序，和 / 或严重度(S)和发生概率(O)的乘积数值 / 矩阵来做决策。

4.2 分析目的

FMECA（失效模式影响与危害性分析）的目的是通过系统化的分析，在产品设计或制造过程阶段提前识别可能存在的潜在失效模式，评估其影响及危害性程度，并采取对应的改进措施，以提升产品的可靠性。

4.3 分析流程

FMECA分析流程如下图1所示：

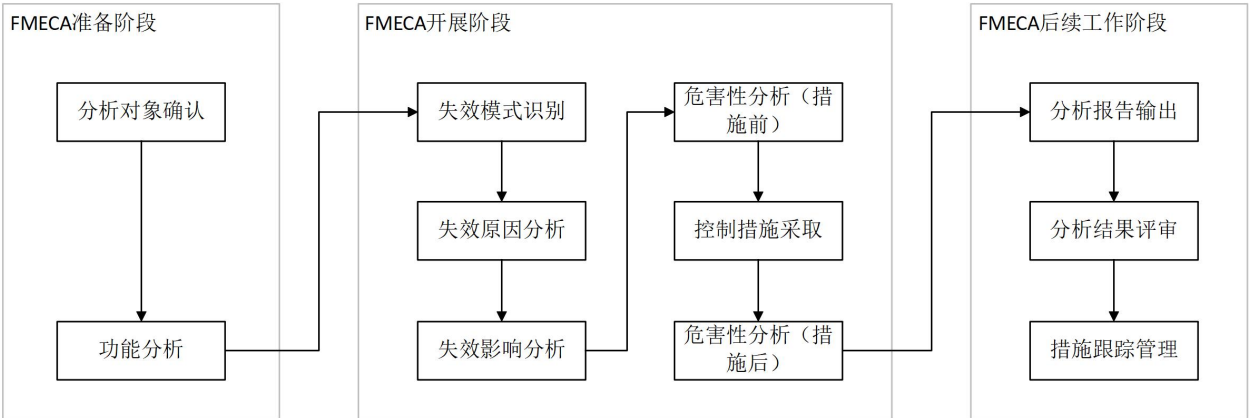


图1 FMECA分析流程

4.4 FMECA 人员及计划性

4.4.1 FMECA 人员

FMECA工作应有具体人员主导完成。可参考以下原则安排其他人员参与FMECA过程：

- a) 应在FMECA管理计划中规定FMECA工作主导人员和参与人员；
- b) 参与FMECA分析的人员尽量由涵盖有源医疗器械相关的多学科专业知识的跨职能部门成员组成，包括掌握专业知识、掌握FMECA方法等人员；
- c) DFMECA建议至少由以下职能人员参与：研发、测试、质量、可靠性等；
- d) PFMECA建议至少由以下职能人员参与：制造 / 工艺、质量、可靠性、研发等；
- e) 根据FMECA开展的需要，可邀请其他职能人员参与分析过程，如风险分析、临床应用等。

4.4.2 FMECA 计划性

FMECA 工作开展计划应注意以下几点：

- a) 应事先制定相应的管理计划来保证 FMECA 工作的开展；
- b) 计划中应至少体现 FMECA 时间节点、参与人员、 FMECA 评审、跟踪管理（例如补偿措施的落实情况）等信息；
- c) FMECA 活动的开展应与项目进度相协调，确保分析及时进行。

5 DFMECA

5.1 待分析对象定义

DFMECA 工作需要团队成员协同完成。分析前，可由系统工程师或 DFMECA 工作负责人完成待分析对象定义，以提升 DFMECA 过程的效率。

待分析对象定义的主要工作：

- a) 明确待分析产品；
- b) 对待分析产品进行功能描述。有源医疗器械示例可参考附录 A 。

5.1.1 明确待分析对象

明确待分析对象首先要明确对哪些元器件、部件、子系统、系统等进行分析。对于导致可靠性水平低或可靠性后果严重的部分，宜从以下几点重点考虑：

- a) 新设计或变更的；
- b) 与影响基本安全和基本性能的高风险问题相关的；
- c) 已有数据表明可靠性水平低的，如历史数据、试验数据等；
- d) 制造商分析出的其他高风险点。

5.1.2 功能分析

功能分析前，如有必要需先进行结构分析。特别是针对结构较为复杂的待分析对象，如有需要可以将产品进一步按照系统、子系统、部件、元器件等层级将已明确的分析对象分解成更基本的要素。分解结果可采用功能方框图、结构树等方式呈现。

功能分析主要是根据结构分析的结果，将待分析对象的功能分配给产品的各组成部分，进而将产品功能或者更低层级的功能跟该产品或更低层级的组成部件相关联。

注1：功能方框图：用框图的形式来表达系统原理，它的作用在于能够清晰地表示系统各组成部分所承担的功能之间的相互关系及功能逻辑顺序。

注2：结构树：根据产品的层次关系，将产品元器件、部件、子系统等按照一定的层级关系组织起来。它可以清晰地描述产品各个元器件、部件、子系统等之间的依赖关系。

5.2 DFMECA 过程

DFMECA 分析主要是对设计进行失效模式识别、失效原因及失效影响分析，并根据分析结果进行危害性评估。DFMECA 过程主要包括以下几个步骤。每个步骤和实际工作的结合可参考附录 A。

5.2.1 失效模式识别

失效是指产品无法满足或提供预期功能，而失效模式是失效的表现形式。失效模式是指依据5.1.2功能分析结果判定的待分析对象部分或全部功能丧失或劣化的表现形式。产品具有多种功能时，应找出该产品每个功能的全部可能的失效模式。功能失效的描述可以从以下几方面考虑，但不限于：

- a) 功能丧失（即无法工作）；
- b) 功能不足（即性能损失）；
- c) 超出功能（即操作超过可接受的阈值）；
- d) 功能退化（即随着时间的推移性能下降）；
- e) 功能异常（即非预期功能）；
- f) 功能延迟（即在非预期的时间间隔后操作）等。

5.2.2 失效原因分析

失效原因指导致失效模式出现的原因。一种失效模式可能有一种以上的失效原因，需分别展开。失效原因尽可能详述，详细的失效原因描述有利于精确的制定检测方法和补偿措施。常见的失效原因可从如下几个方面进行分析，但不局限于：

- a) 材料、结构、公差等设计问题；
- b) 软件问题（如：未定义的状态、不完整的数据、算法不正确、网络安全漏洞、软件兼容性等）；
- c) 系统交互问题（如：接口、反馈等）；
- d) 随时间变化问题（如：疲劳、磨损、腐蚀、设计寿命不足等）；
- e) 外部环境（如：温度、湿度、气压、盐雾、振动、设备串扰等）；
- f) 误操作。

5.2.3 失效影响分析

失效影响是失效模式的后果，一个失效模式可以有多个失效影响，失效影响可从局部影响和最终影响两方面考虑。

局部影响是指失效模式对被分析产品或同一层级产品局部的使用、功能等的影响。局部影响的描述为确定检测方法、补偿措施提供了依据。局部影响可能是失效模式本身。

最终影响主要用于描述失效模式对有源医疗器械使用、功能等的影响，及对用户和适用的法律法规等的影响。

5.2.4 危害性分析

危害性分析的目的是通过评估失效模式的严重度(S)、发生概率(O)、可探测度(D)来评估其危害性排序，并得到采取行动的优先级。有源医疗器械范围广，涉及种类繁多，各制造商可根据自身产品特点定义严重度、发生概率和可探测度等级。

严重度(S)是评价失效模式导致的最严重影响的度量。针对有源医疗器械，可以从待分析对象发生某种失效模式后造成的临床影响来划分严重度等级。

发生概率(O)描述了在用户使用中发生失效的可能性。发生概率的来源可参考历史数据、相似产品的信息、设计分析、试验、专业知识等方面的信息。公司内如有经验数据，应优先采用。

可探测度(D)表示了现有设计控制方法对失效原因或失效模式探测有效性的度量，探测等级依据最有效的探测措施进行评估。可探测度越高，分值越低。

失效模式危害性评价时，以危害性评价指数 $RPN = S \times O \times D$ 表征其危害性的相对大小。一般当 RPN 值高于一定数值，则为不可接受的风险，该失效应采取处理措施。还可将 RPN 值结合 $S \times O$ 分值/矩阵来决定需处理的潜在失效项。对于低于规定 RPN 值的风险项，虽然属于可接受风险，但若条件允许，尽可能采取措施降低其风险等级。

5.2.5 采取措施

可采取的措施一般有失效检测和补偿两种。

失效检测措施主要是指用检测的方式来识别出是否有失效发生。检测措施的完善一般可以提升可探测度。失效检测一般有目视检查、机内测试、状态监测、自动传感检测等方法。大部分的失效检测属于事后检测，但是也可以通过对潜在失效模式的分析，在设计中采用事前检测方法。

补偿措施既包括预防、纠正措施，也包括冗余设计、维护保养等补偿方法。预防、纠正措施指针对失效原因，在考虑或确定设计方案时应重点从设计、工艺、元器件或材料选择、试验及质量控制等方面采取的技术、控制措施。而常用的补偿方法有：冗余设计、安全装置（报警、监控等）、替换的工作方式（备用设备等）、维修维护等。

5.2.6 采取措施后的危害性评价

评分目的是为了判断采取措施后，该失效的危害性是否可以降低到可接受标准之下。具体可参照 5.2.4 有关内容。

5.2.7 参考文件

体现了补偿措施的过程、方法、结果等文件。可用于改进措施落实情况的追踪及落实结果的评价。

5.3 DFMECA 后续工作

DFMECA 分析工作完成后，需输出报告。报告格式可参考附录 B。还需开展以下工作：

- DFMECA 结果评审，该过程可结合技术评审、节点评审等进行，也可单独进行；
- 将 DFMECA 措施的落实分配给具体人员，并纳入项目管理的范畴；
- 定期跟踪检测 / 补偿措施的落实情况；
- 评估措施的落实效果；
- DFMECA 输出内容应持续更新。

6 PFMECA

6.1 待分析对象定义

PFMECA 工作同样需要团队成员协同完成。分析前，可由 PFMECA 工作负责人完成待分析对象定义，以提升 PFMECA 过程的效率。

定义待分析对象的主要工作：

- 确定待分析过程对象；
- 对待分析过程对象进行功能描述。

有源医疗器械示例可参考附录 C。

6.1.1 明确待分析对象

制造过程会影响产品的质量。确定待分析过程对象的目的是明确识别哪些过程或过程的哪个环节需要进行分析。一般可以考虑将以下过程纳入待分析范围：新开发的过程、变更的过程、可能导致高风险的过程、根据经验需要重点考虑的其他过程等。

6.1.2 功能分析

首先，将待分析过程分解为过程工序、工步等。针对复杂的过程，可利用过程流程图或结构树来描述过程、工序、工步间的关系，并将过程可视化。

其次，将过程功能按照分解结果分配到各工序、工步，并进行描述。过程功能分析主要有以下 3 种：

- 过程本身功能：其功能可以从以下几点考虑：内部功能、外部功能、客户相关功能和 / 或最终用户功能。
- 工序功能：可以以图纸、工艺路线或其他相关资料中的要求来做功能描述。
- 工步功能：可用工步结果的组装规格或其他生产文件要求来做功能描述。

注1：过程流程图是利用一定的符号将实际的工艺过程以图形方式表现出来，以便于确定可能的变量形式。它有助于对要改进的过程有一个全面的、统一的了解，帮助项目团队确定过程中的一切可控与不可控的变量以及可能出现的问题。

注2：结构树是按照层次排列系统元素，并通过结构连接说明关联关系。这个形象化的结构考虑了程序方法和过程

工作要素（设备、人力等）之间的关系。

6.2 PFMECA 过程

PFMECA 的主要工作是对过程进行分析，以识别失效模式、分析失效原因及失效影响，并根据失效模式的严重度(S)、发生概率(O)、可探测度(D) 进行危害性评估。PFMECA 过程包括以下几个步骤。每个步骤跟实际工作的结合可参考附录 C。

6.2.1 失效模式识别

PFMECA 的失效模式是指待分析过程对象不能满足制造过程要求或导致产品不能满足设计要求的表现形式。

过程功能失效的描述可以从以下几方面考虑，但不限于：

- a) 功能丧失；
- b) 功能不足；
- c) 过功能；
- d) 功能退化；
- e) 间歇性功能；
- f) 意外的功能；
- g) 功能延迟等。

各项解释可参考5.2.1相关内容。

6.2.2 失效原因分析

失效原因是引起失效模式发生的原因，它揭示了失效模式为何发生。典型的失效原因可以从人、机、料、法、环、测等几个方面考量。其中：

“人”主要指过程执行者的原因造成了失效，例如拿错零件；

“机”主要指过程中生产设备的原因造成了失效，例如生产设备软件异常；“料”主要指过程中材料的原因造成了失效，例如材料质量问题；

“法”主要指过程中方法（工艺指导书等）的原因造成了失效，例如螺栓扭紧力过大；

“环”主要指过程中环境因素造成了失效，例如温度不达标造成失效；

“测”主要指过程中由于测量偏差引起的误判。

6.2.3 失效影响分析

失效影响是失效模式的后果，失效影响可从局部影响和最终影响两方面考虑。

局部影响主要指失效对本过程、工序、工步的影响、对下游过程、工序、工步的影响等。最终影响主要描述失效对有源医疗器械的功能、性能、生产成本和效率、用户使用等的影响。

6.2.4 危害性分析

过程危害性分析的目的是通过综合考虑失效模式的严重度(S)、发生概率(O)和可探测度(D)来评估其危害性，并根据危害性分析结果确定采取改进措施的优先顺序。

严重度(S)是对过程所有可能的失效模式导致的最严重影响的度量。其等级分类可以从影响生产人员健康、产品废弃、部分废弃、返工、部分返工、对过程造成轻微不便、无明显影响等方面考虑，从高到低划分。

发生概率(O)描述过程中失效模式的发生频度，例如装配过程中的不良率。可参考类似过程的现场经验、类似过程的历史记录、生产过程是否有变更、生产过程中的失效发生情况等方面考虑。

可探测度(D)表示了现有过程控制方法对失效原因或失效模式探测有效性的度量，探测等级依据最有效的探测措施进行评估。可探测度越高，分值越低。

危害性评价指数 $RPN = S \times O \times D$ 。一般当 RPN 值高于一定数值，则为不可接受的风险，该失效应采取处理措施。还可将 RPN值结合 $S \times O$ 分值 / 矩阵结果来决定需处理的失效项。

6.2.5 可采取的措施

可采取的措施一般分两种，即失效检测和补偿。

失效检测措施主要指过程中的检测行为，在失效造成影响之前检测到失效，并报警或停机，从而降低失效的影响。例如：可视化检验等。

补偿措施一般指在过程开始前通过一系列手段减少失效的产生。例如：详细的操作指导书、人员培训、过程监管等。

6.2.6 采取措施后的危害性评价

评分目的是为了判断采取措施后，该失效的危害性是否可以降低到可接受标准之下。具体可参照 5.2.4 相关内容。

6.2.7 参考文件

参考文件是指体现了补偿措施的过程、方法、结果等文件。可用于补偿措施落实情况的追踪及落实结果的评价。

6.3 PFMECA 后续工作

PFMECA 分析工作完成后，需输出报告，报告格式可参考附录 B。还需开展以下工作：

- a) PFMECA 分析后还需要通过改进流程来降低过程风险，并评估这些改进措施的有效性；
- b) 将 PFMECA 措施的落实分配给具体人员，并纳入项目管理的范畴；
- c) 定期追踪检测 / 预防措施的落实情况；
- d) 评估措施的落实效果；
- e) PFMECA 输出内容应持续更新。

附录 A
(资料性)
医疗机器人机械臂关节 1 DFMECA 示例

A.1 概述

以医疗机器人为例，针对某机械臂关节 1 的 DFMECA 过程如下。

A.2 待分析对象定义

医疗机器人为全自主新研产品，因为直接作用于手术过程，失效后危害性较高。据此特点，医疗机器人的所有设计均需进行 DFMECA 分析。文件仅体现某机械臂关节 1 的部分 DFMECA 过程，以作示例。

A.3 功能分析

- 机械臂关节 1 的功能可描述如下：
- a) 安装在调整臂末端（固定连接）；
 - b) 提供工具臂 × 方向运动、定位、锁紧和调整（手动）；
 - c) 锁紧力不小于××N ；
 -

A.4 失效模式识别

所识别的失效模式及该失效所属失效类别见表 A.1 。

表 A.1 机械臂关节 1 失效模式

功能	失效模式	功能失效类别
安装在调整臂末端（固定连接）	掉落	功能丧失
提供工具臂 × 方向运动、定位、锁紧和调整（手动）	不能手动调整	功能丧失
锁紧力不小于××N	多次操作后，锁紧后晃动	功能退化
.....		

A.5 失效原因分析

根据上文失效模式，识别到的失效原因见表 A.2 。

一个失效往往对应多个失效原因，本文仅为示例，针对每种失效，仅列出一个失效原因。

表 A.2 机械臂关节 1 失效原因

失效模式	失效原因	失效原因类别
掉落	关节 1 与调整臂连接组件强度不足，受过载或冲击而 断裂	材料强度问题
不能手动调整	模组动力输入轴安装紧固件脱落，卡死 关节	公差问题
多次操作后，锁紧后晃动	转动抱闸齿轮与关节输出齿轮磨损	设计寿命不足
.....		

A.6 失效影响分析

根据所识别的失效模式，分析所得失效影响见表 A.3。

表 A.3 机械臂关节 1 失效影响

失效模式	局部影响	最终影响	失效影响类别
掉落	机械臂掉落	手术中掉落造成死亡	对最终用户影响
不能手动调整	机械臂无法调整	显著延长手术时间	对最终用户影响
多次操作后，锁紧后晃动	机械臂无法锁紧	显著延长手术时间	对最终用户影响
……			

A.7 危害性分析

医疗机器人的严重度(S)、发生概率(O)、可探测度(D)等级参见表 A.4~A.6。

表 A.4 医疗机器人严重度等级

等级	定性描述	对患者的影响
1	无	对患者基线状态或手术结果无影响。 包括：使用前器械损坏，不使用已损坏的器械； 不影响产品使用的损坏或功能异常
2	很低	对患者基线状态或手术结果有轻微影响。 包括： 设备功能异常轻微影响手术时间； 器械使用不当轻微影响手术时间； 器械损坏，更换器械
3	低	对患者基线状态有显著影响。包括： 显著延长手术时间； 组织损伤； 血管出血； 局部感染； 局部毒性反应
4	中等	对患者基线状态有严重影响。 包括： 过敏反应； 全身感染； 全身毒性反应； 从微创手术改为传统开腔手术
5	高	对患者基线状态有重大改变。 包括： 紧急抢救； 不可恢复的伤害。 例如，器官摘除、截肢等
6	很高	器械相关的死亡
注：企业根据自身情况可进行等级分值的调整，比如调整为1~10分。		

表 A.5 医疗机器人发生概率等级

等级	定性描述	概率（该失效模式在产品寿命周期内发生的概率）
1	几乎不可能	≤0.001%
2	极少	≤0.005%
3	很少	≤0.01%
4	较少	≤0.05%
5	一般	≤0.1%
6	中高	≤0.5%
7	较高	≤1%
8	很高	≤5%
9	极高	≤10%
10	几乎一定	>10%

表 A.6 医疗机器人可探测度等级

等级	定性描述	
1	几乎肯定	能否在原型机之前发现：以前的产品历史，相关的研究阶段测试
2	很高	能否在设计发布前检测到：设计验证，动物学研究结果和 / 或方案要求 的测试
3	高	
4	中上	
5	中等	能否在量产前被检测到：过程和产品确认
6	小	能否在出厂前被检测到：在线检测、出厂放行测试
7	很小	
8	微小	能否在发货后，但在最终用户前检测到
9	很微小	能否在失效发生前检测到：使用说明、标签
10	几乎不可能	直到在用户现场发现失效才能被检测到

根据所识别到的失效模式及分析所得失效原因和失效影响，可以获得机械臂关节 1 的危害性分析见表 A.7。医疗机器人的危害性接受准则为：当 S/O 矩阵中标记为“×”或者 RPN 值 ≥120 时，风险不可接受；否则，风险可接受。S/O 矩阵可见表 A.8。

根据 RPN 值及 S/O 矩阵可知，3 项失效模式中，有 2 项可接受，1 项不可接受。本着尽量降低危害性的原则，针对此 3 项潜在失效，实际工作中均采取了增加检测及补偿措施。

表 A.7 机械臂关节 1 危害性分析

失效模式	失效原因	局部影响	最终影响	严重度 (S)	发生概率 (O)	可探测度 (D)	RPN
掉落	关节 1 与调整臂连接组件强度不足，受过载或冲击而断裂	机械臂掉落	手术中掉落造成死亡	6	1	3	18
不能手动调整	模组动力输入轴安装紧固件脱落，卡死关节	机械臂无法调整	显著延长手术时间	4	3	3	36
多次操作后，锁紧后晃动	转动抱闸齿轮与关节输出齿轮磨损	机械臂无法锁紧	显著延长手术时间	4	5	3	60

医疗机器人的危害性接受准则为：当 S/O 矩阵中标记为“×”或者 RPN 值 ≥ 120 时，风险不可接受；否则，风险可接受。S/O 矩阵可见表 A.8。

根据 RPN 值及 S/O 矩阵可知，3 项失效模式中，有 2 项可接受，1 项不可接受。本着尽量降低危害性的原则，针对此 3 项潜在失效，实际工作中均采取了增加检测及补偿措施。

表 A.8 S / O 矩阵

发生概率(O) 严重度(S)	1	2	3	4	5	6	7	8	9	10
1	▽	▽	▽	▽	▽	▽	▽	▽	▽	×
2	▽	▽	▽	▽	▽	▽	▽	×	×	×
3	▽	▽	▽	▽	▽	×	×	×	×	×
4	▽	▽	▽	▽	×	×	×	×	×	×
5	▽	▽	×	×	×	×	×	×	×	×
6	▽	×	×	×	×	×	×	×	×	×
×：风险不可接受；▽：风险可接受										

A.8 报告输出

依次完成“可采取的措施”、“采取措施后的危害性评价”等工作，即可完成机械臂关节 1 的 DFMECA 报表。

附 录 B
(规范性)
FMECA 报告模板

FMECA 报告常用模板见表 B.1 。

表 B.1 FMECA 报告模板

项目名称：_____																				分析日期：_____	
产品型号：_____																				FMECA 版本：_____	
分析对象：_____																				分析人员：_____	
序号	分析对象	功能描述	失效模式	失效原因	失效影响		措施前					措施		措施后				参考文件			
					局部影响	最终影响	现有预防措施	现有探测措施	严重度(S)	发生概率(O)	可探测度(D)	风险评价指数(RPN)	失效探测措施	补偿措施	严重度(S)	发生概率(O)	可探测度(D)		风险评价指数(RPN)		
1																					
2																					
3																					
4																					
5																					
6																					

附录 C
(资料性)
医疗机器人机械臂关节 1 PFMECA 示例

C.1 概述

以医疗机器人为例，针对某机械臂关节 1 装配过程 PFMECA 过程如下。

C.2 待分析对象定义

医疗机器人为全自主新研产品，因为直接作用于手术过程，失效后危害性较高。其制造过程亦为新建，所以整个制造过程均需进行 PFMECA 分析。本文仅展示某机械臂关节 1 的部分 PFMECA 过程，以作示例。

C.3 功能分析

该机械臂关节 1 装配过程所要实现的功能如下：

- a) 关节转动摩擦力不大于××Nm；
- b) 关节运动空间：××°±**°；
- c) 关节连接可靠，锁紧后无晃动；
- d) 关节转动无明显卡顿感；
-

C.4 失效模式识别

所识别的失效模式及该失效所属失效类别见表 C.1。

表 C.1 机械臂关节 1 装配过程失效模式

功能	失效模式	功能失效类别
关节转动摩擦力不大于××Nm	关节转动摩擦力过大	过功能
关节运动空间：××°±**°	关节工作空间不对称	功能不足
关节连接可靠，锁紧后无晃动	关节晃动	功能丧失
关节转动无明显卡顿感	关节运动明显卡顿	间歇性功能
.....		

C.5 失效原因分析

根据上文失效模式，识别到的失效原因见表 C.2。
一个失效往往对应多个失效原因，本文仅为示例，针对每种失效，仅列出一个失效原因。

表 C.2 机械臂关节 1 装配过程失效原因

失效模式	失效原因	失效原因类别
关节转动摩擦力过大	CIMRS添加过多	料
关节工作空间不对称	零位孔安装偏移	人
关节晃动	轴承压盖螺钉拧紧扭矩不足	法
关节运动明显顿挫	有异物进入传动结构	环
.....		
注：CIMRS为一种垫片型号。		

C.6 失效影响分析

根据所识别的失效模式，分析所得失效影响见表 C.3。

表 C.3 机械臂关节 1 装配过程失效影响

失效模式	局部影响	最终影响
关节转动摩擦力过大	当前工序内返工，显著延长工时	生产成本增加
关节工作空间不对称	当前工序内返工，显著延长工时	生产成本增加
关节晃动	当前工序内返工，显著延长工时	生产成本增加
关节运动明显顿挫	工序内返工，显著延长工时	生产成本增加
.....		

C.7 危害性分析

医疗机器人的严重度(S)、发生概率(O)、可探测度(D)等级参见表 C.4～表 C.6。

表 C.4 医疗机器人制造过程严重度

等级	定性描述	对制造 / 组装过程的影响
1	无	无影响或对操作员造成轻微不便利
2	很低	无需返工，轻微延长工时，不影响下游过程；无零部件损坏或废弃
3	低	当前工序内返工，显著延长工时，轻微影响下游过程；次要零部件损坏或废弃
4	中等	脱线返工，严重影响下游过程；重要零部件、产品损坏或废弃；设备、工装或夹具的轻微损伤
5	高	大量返工或流水线停止；设备、机器、工装或夹具损坏。对操作或操作员有危害
6	很高	器械相关的死亡（操作人员）

注：企业根据自身情况可进行等级分值的调整，比如调整为1~10分。

表 C.5 医疗机器人制造过程发生概率

等级	定性描述	概率
1	几乎不可能	≤0.001%
2	极少	≤0.005%
3	很少	≤0.01%
4	较少	≤0.05%
5	一般	≤0.1%
6	中高	≤0.5%
7	较高	≤1%
8	很高	≤5%
9	极高	≤10%
10	几乎一定	>10%

表 C.6 医疗机器人制造过程可探测度分值的定义

探测等级	描述	分值
1	连续使用监测	10.0
6	100% 自动检测	5.0
7	100%人工客观检验	4.0
7	有效样本统计测试	4.0
7	计量型统计过程控制, $cpk \geq 1.33$	4.0
9	100%人工主观检验	3.0
9	计量型统计过程控制, $cpk = 1.00 \sim 1.32$	2.0
9	计数型统计过程控制	2.0
10	末件检验	1.0
10	首件检验	1.0
10	检验员证明	1.0
10	计量型统计过程控制, $cpk \leq 0.99$	1.0
10	抽样检验, 不完全统计	1.0
10	未进行分类的其他检测	1.0

注: CPK为过程能力指数, 是衡量制程稳定性的核心指标, 用于评估生产过程在满足产品规格(上下限)时的能力。

根据所识别到的失效模式及分析所得失效原因和失效影响, 可以获得机械臂关节 1 的危害性分析见表 C.7。医疗机器人的危害性接受准则为: 当 RPN 值 ≥ 120 或 S/O 矩阵中标记为“×”时, 风险不可接受, 否则风险可接受。S/O 矩阵可见表 C.8。

根据 RPN 值及 S/O 矩阵可知, 4 项失效模式均可接受。但本着尽量降低危害性的原则, 针对此 4 项潜在失效, 工作中均采取了增加检测及补偿措施。

表 C.7 机械臂关节 1 装配过程危害性分析

失效模式	失效原因	局部影响	最终影响	严重度(S)	发生概率(O)	可探测度(D)	RPN
关节转动摩擦力过大	CIMRS添加过多	当前工序内返工, 显著延长工时	生产成本增加	3	4	7	84
关节工作空间不对称	零位孔安装偏移	当前工序内返工, 显著延长工时	生产成本增加	3	4	7	84
关节晃动	轴承压盖螺钉拧紧扭矩不足	当前工序内返工, 显著延长工时	生产成本增加	3	4	7	84
关节运动明显顿挫	有异物进入传动结构	工序内返工, 显著延长工时	生产成本增加	3	4	7	84

注: CIMRS为一种垫片型号。

表 C.8 S / O 矩阵

严重度 (S) \ 发生概率 (O)	1	2	3	4	5	6	7	8	9	10
1	▽	▽	▽	▽	▽	▽	▽	▽	×	×
2	▽	▽	▽	▽	▽	▽	×	×	×	×
3	▽	▽	▽	▽	×	×	×	×	×	×
4	▽	▽	▽	×	×	×	×	×	×	×
5	▽	×	×	×	×	×	×	×	×	×
6	×	×	×	×	×	×	×	×	×	×
×：风险不可接受；▽：风险可接受，应尽可能将风险降到最低；√：风险可接受，可忽略的风险。										

C.8 报告输出

依次完成“可采取的措施”、“采取措施后的危害性评价”等工作，即可完成对机械臂关节 1 的 PFMECA 报表。