**（产品名称）**

**危害分析报告**

**DHF-XXX**

|  |  |  |  |
| --- | --- | --- | --- |
| **职责** | **职能** | **人员** | **签名** |
| **文件编制** |  |  |  |
| **文件审核** |  |  |  |
| **文件审核** |  |  |  |
| **文件审核** |  |  |  |
| **…** |  |  |  |
| **文件批准** |  |  |  |

**版本记录**

| **序号** | **更改日期** | **版本** | **编制人** | **修改说明** |
| --- | --- | --- | --- | --- |
| 01 |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**目录**

[1 概述 4](#_Toc187152723)

[1.1 目的 4](#_Toc187152724)

[1.2 适用范围 4](#_Toc187152725)

[1.3 产品基本信息 4](#_Toc187152726)

[1.3.1 产品预期用途 4](#_Toc187152727)

[1.3.2 产品示意图 4](#_Toc187152728)

[1.3.3 产品功能特性概述 4](#_Toc187152729)

[1.3.4 基本性能 4](#_Toc187152730)

[1.4 术语与缩写 4](#_Toc187152731)

[1.5 危害分析小组和职责 4](#_Toc187152732)

[2 风险要素和风险可接受性准则 5](#_Toc187152733)

[3 风险分析 6](#_Toc187152734)

[3.1 预期用途和可合理预见的误使用 6](#_Toc187152735)

[3.1.1 预期用途，见1.3.1产品基本信息的描述。 6](#_Toc187152736)

[3.1.2 可合理遇见的误使用 6](#_Toc187152737)

[3.2 与安全有关的特征的识别 6](#_Toc187152738)

[3.3 危险和危险情况的识别及风险估计见附录C：危害分析工作表。 6](#_Toc187152739)

[4 风险评价 6](#_Toc187152740)

[5 风险控制 6](#_Toc187152741)

[5.1 风险控制方案的分析、风险控制措施的实施、剩余风险的评价 6](#_Toc187152742)

[5.2 受益-风险分析结果（适用时） 6](#_Toc187152743)

[5.3 由风险控制措施产生的风险 6](#_Toc187152744)

[5.4 风险控制的完整性 6](#_Toc187152745)

[6 综合剩余风险可接受评价结果 6](#_Toc187152746)

[6.1 综合剩余风险评价方法介绍 6](#_Toc187152747)

[6.2 综合剩余风险可接受性评价结果 6](#_Toc187152748)

[7 生产和生产后信息的评价计划和结果 6](#_Toc187152749)

[8 结论 7](#_Toc187152750)

[附录A：严重度、发生概率等级的的评定准则和风险评定准则 7](#_Toc187152751)

[A.1发生概率（O）等级的评定准则 7](#_Toc187152752)

[A.2严重度（S）等级的评定准则 8](#_Toc187152753)

[A.3风险可接受性的评定准则 8](#_Toc187152754)

[附录B：安全性相关特征判定及与医疗器械有关的已知或可预见的危害识别 10](#_Toc187152755)

[附录C：软件安全性等级及软件网络安全等级判定 12](#_Toc187152756)

[C.1软件安全性等级判断依据参考以下两种方式： 13](#_Toc187152757)

[C.2软件项安全性级别判断 14](#_Toc187152758)

[C.3产品网络安全性等级判断 14](#_Toc187152759)

[附录D：危害分析工作表 15](#_Toc187152760)

[附录E：综合剩余风险分析及评价 16](#_Toc187152761)

# 概述

## 目的

运用危害分析方法对产品实施风险分析、风险评价、风险控制、综合剩余风险评价等风险管理活动，形成危害分析报告。

## 适用范围

产品范围：适用于国内注册产品？

产品生命周期阶段：适用于M？前

## 产品基本信息

### 产品预期用途

### 产品示意图

### 产品功能特性概述

### 基本性能

## 术语与缩写

## 危害分析小组人员能力和职责分配

| **姓名** | **职能** | **资质** | **职责描述** |
| --- | --- | --- | --- |
|  | 项目经理 | 学历：  专业：  工作经验：  培训： | 建立危害分析小组，制定风险管理计划，指导和协调风险管理活动，负责危害分析报告的批准。 |
|  | 产品经理 | 学历：  专业：  工作经验：  培训： | 参与风险分析、风险评价、风险控制、综合剩余风险评价等活动，评审危害分析报告。 |
|  | 研发 | 学历：  专业：  工作经验：  培训： | 危害分析的主导者。负责组织编写、评审危害分析报告。 |
|  | 生物学 | 学历：  专业：  工作经验：  培训： | 参与风险分析、风险评价、风险控制、综合剩余风险评价等活动，评审危害分析报告。 |
|  | 动物试验 | 学历：  专业：  工作经验：  培训： | 参与风险分析、风险评价、风险控制、综合剩余风险评价等活动，评审危害分析报告。 |
|  | QV | 学历：  专业：  工作经验：  培训： | 参与风险分析、风险评价、风险控制、综合剩余风险评价等活动，评审危害分析报告。 |
|  | 工艺 | 学历：  专业：  工作经验：  培训： | PFMEA的主导者。参与风险分析、风险评价、风险控制、综合剩余风险评价等活动，评审危害分析报告。 |
|  | 注册 | 学历：  专业：  工作经验：  培训： | 参与风险分析、风险评价、风险控制、综合剩余风险评价等活动，评审危害分析报告。 |
|  | 临床 | 学历：  专业：  工作经验：  培训： | 参与风险分析、风险评价、风险控制、综合剩余风险评价等活动，评审危害分析报告。 |
|  | 采购 | 学历：  专业：  工作经验：  培训： | 参与风险分析、风险评价、风险控制、综合剩余风险评价等活动，评审危害分析报告。 |
|  | QA | 学历：  专业：  工作经验：  培训： | 确保风险管理活动符合风险管理控制要求，并指导风险管理活动实施。参与风险分析、风险评价、风险控制、综合剩余风险评价等活动，评审危害分析报告。 |

# 风险要素和风险可接受性准则

见附录 A：严重度、发生概率、探测度等级的评定准则和风险可接受性评定准则

# 风险分析

## 预期用途和可合理预见的误使用

### 预期用途，见 1.1.3产品基本信息的描述

### 可合理预见的误使用

## 与安全有关的特性的识别

见附录B：用于判定医疗器械与安全有关特征的问题

## 危险和危险情况的识别及风险估计

见附录C：危害分析工作表

# 风险评价

风险评价结果见附录C：危害分析工作表

# 风险控制

## 风险控制方案的分析、风险控制措施的实施、剩余风险的评价

见附录C：危害分析工作表。

## 受益-风险分析结果（适用时）

## 由风险控制措施产生的风险

## 风险控制的完整性

# 综合剩余风险可接受评价结果

## 综合剩余风险评价方法介绍

## 综合剩余风险可接受性评价结果

# 生产和生产后信息的评价计划和结果

生产和生产后信息的收集和评价计划见“生产和生产后风险管理计划”。

生产和生产后信息的评价结果见“年度风险管理评价报告”。

# 结论

从能量（有源）、生物和化学、性能有关的、标识、使用错误等方面进行危害分析，并对不可接受的风险制定风险控制措施计划。

完成了全部的风险控制措施，并对风险控制措施的有效性进行了验证。

进行了剩余风险的评价和综合剩余风险的评价，产品综合剩余风险可接受。

已有方法获得和评审生产和生产后信息。

# 附录A：严重度、发生概率等级的评定准则和风险评定准则（YY/T 1437-2023 附录C）

## A.1发生概率（O）等级的评定准则

示例1（当概率对象的基数较小时，概率的区间不方便分多级可以适当减少级数，但同一系列产品建议使用相同规则，以利于同类产品的数据参考）。

| **等级** | **定性描述** | **概率**  **（10年使用寿命共使用10000次）** |
| --- | --- | --- |
| 1 | 几乎不可能 | ≤0.001% |
| 2 | 很少 | ＞0.001%和≤0.01% |
| 3 | 一般 | ＞0.01%和≤0.1% |
| 4 | 较高 | ＞0.1%和≤1% |
| 5 | 极高 | ＞1%和≤10% |
| 6 | 几乎一定 | ＞10% |

示例2（当概率对象的基数较大时，概率的区间可以分多级，但同一系列产品建议使用相同规则，以利于同类产品的数据参考）。

| **等级** | **定性描述** | **概率**  **（10年使用寿命共使用10000次）** |
| --- | --- | --- |
| 1 | 几乎不可能 | ≤0.001% |
| 2 | 极少 | ＞0.001%和≤0.005% |
| 3 | 很少 | ＞0.005%和≤0.01% |
| 4 | 较少 | ＞0.01%和≤0.05% |
| 5 | 一般 | ＞0.05%和≤0.1% |
| 6 | 中高 | ＞0.1%和≤0.5% |
| 7 | 较高 | ＞0.5%和≤1% |
| 8 | 很高 | ＞1%和≤5% |
| 9 | 极高 | ＞5%和≤10% |
| 10 | 几乎一定 | ＞10% |

## A.2严重度（S）等级的评定准则

| **等级** | **定性描述** | **对制造/组装过程的影响** | **对用户的影响** |
| --- | --- | --- | --- |
| 1 | 无 | 无影响或对操作员造成轻微不便利。 | 使用前器械损坏，不使用已损坏的器械。  不影响器械使用的损坏或功能异常。  对患者无影响。 |
| 2 | 很低 | 无需返工，轻微延长工时，不影响下游过程；  无零部件损坏或报废。 | 设备功能异常轻微影响手术时间。  操作舒适度降低轻微影响手术时间。  患者暂时轻微不适。 |
| 3 | 低 | 当前工序内返工，显著延长工时。  轻微影响下游过程。  次要零部件损坏或报废。 | 不要求专业医疗介入的暂时伤害或损伤，如：  显著延长手术时间。  组织轻微损伤。  血管轻微出血。 |
| 4 | 中等 | 脱线返工，严重影响下游过程。  重要零部件、产品损坏或报废。  设备、工装或夹具的轻微损伤。 | 要求专业医疗介入的暂时伤害或损伤，如：  全身感染、炎症。  使用时器械损坏,从微创伤手术改为传统开腔手术。 |
| 5 | 高 | 大量返工或流水线停止。  设备、机器、工装或夹具损坏。  对操作者有危害。 | 永久性损伤或危机生命的伤害。  不可恢复的伤害。 |
| 6 | 很高 | 对操作者产生严重或致命的危害。 | 由于医疗器械的失效导致的死亡 |

## A.3风险可接受性的评定准则（需要根据产品的实际情况制定，不能直接应用示例）

示例1

| **发生概率（O）** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **严重度（S）** | **1** | **2** | **3** | **4** | **5** | **6** |
| 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  （注意：产品包含欧盟目标市场时，建议只分为可接受风险和不可接受风险两类） | | | | | | |

示例2

| **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，应尽可能将风险降到最低 □：风险可接受，可忽略  （注意：产品包含欧盟目标市场时，建议只分为可接受风险和不可接受风险两类） | | | | | | | | | | |

# 附录B：安全性相关特征判定及与医疗器械有关的已知或可预见的危害识别（YY/T 1437-2023 附录A）

| **序号** | **问题** | **回答** | **相关危险** |
| --- | --- | --- | --- |
| 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,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人点或无线连接)。 |  |  |
| 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 | 在医疗器械中利用什么材料或组分，或者什么材料或组分与医疗器共同使用或者接触？  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？ |  |  |
| A.2.5 | 是否有能量输送给患者或从患者身上获取？  宜考虑的因素包括：  ——传输的能量类型；  ——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 | 是否有物质输送给患者或从患者身上获取？  宜考虑的因素包括：  ——是输送还是获取物质；  ——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灭菌？  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；  ——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。 |  |  |
| 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,以及对算法和数据非授权的操作或更改。 |  |  |
| 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；  ——与交互相关的潜在问题(例如,该医疗器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？  宜考虑的与能量有关的因素包括噪声和振动、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、漏电流、电场或磁场。  宜考虑的与物质有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。  宜考虑的与物质有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,、运输和贮存环境。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：  ——对能源和冷却供应的影响；  ——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；  ——校准品的数值能否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？  宜考虑的因素包括软件预期是由用户还是专家进行安装、验证、修改或更换及软件更新的真实性。 |  |  |
| 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、损、疲劳或重复使用引起的部件失效。也宜考虑备件的可获得性。 |  |  |
| 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,和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物质(例如有毒的化学或生物因子),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和新颖性,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、能力评估、认证或鉴定。 |  |  |
| A.2.29 | 如何提供安全信息？  宜考虑的因素包括：  ——信息是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、实验室负责人或者药剂师)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,说明是否需要对操作者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改变。这可能涉及委托生产、供方和厂商的变化。 |  |  |
| A.2.31 | 医疗器械的成功使用，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。关于可用性的附加信息见IEC62366-1,关于报警的信息见YY 9706.108。 |  |  |
| 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,以及连接过紧和过松。 |  |  |
| 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、映射、反馈模式、失误、疏忽、控制差异、可视性、启动或变换的方向、控制是连续的还是间断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视性、方向性、用户视力、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程度和数量、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？  宜考虑的因素包括：  ——(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IECTR62366-2。 |  |  |
| 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非授权的动作？  宜考虑的因素包括用户接口是否允许用户进人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相关风险；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。YY 9706.108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(是否故意)？  宜考虑的因素有连接器不正确使用、使安全功能或报警失效、忽视制造商推荐的维护、非授权访问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。关于医用电气设备和医用电气系统的基本性能的讨论见GB 9706.1。 |  |  |
| 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。  关于具有一定自动化程度的医疗器械的进一步指南见IEC TR 60601-4-1。 |  |  |
| 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。关于体外诊断医疗器械的指南见附录H。 |  |  |

# 附录C：软件安全性等级及软件网络安全等级判定

软件安全性等级是根据软件系统在最不利情况下可能引发的危险或伤害的情况下，为该软件定义一个安全性等级，以便据此进行必要的软件开发过程的风险控制活动。一般可认为医疗器械网络安全的风险级别与所属医疗器械软件的安全性级别相同。在特殊情况下，网络安全的风险级别可低于软件风险级别。

## C.1软件安全性等级判断依据参考以下两种方式：

1. YY/T0664-2020 软件的安全性级别定义：C级 可能带来死亡或严重伤害； B级 可能带来不可接受风险，但为不严重的伤害；A级 不会带来危险或伤害，或不可接受的风险；
2. 《Guidance for the Content of Premarket submissions for Software Contained in Medical Devices》,具体如下：

注 1：如果对以下任一问题的回答为“是”，软件的安全性级别可能是“C级”。

| **序号** | **问题** | **回答** |
| --- | --- | --- |
| 1 | 软件设备是否适合作为血液建立用电脑软件？  血液建立用电脑软件是指：预期用于生产血液、血液成分的软件，或指预期用于维护机构内部人员判定供体适用性时或判定是否可以发布血液、血液成分用于输注或深加工时所用的数据。 |  |
| 2 | 软件设备是否预期要与某种药品或生物学材料组合使用？ |  |
| 3 | 软件设备是否是具有严重安全性级别医疗设备的一个附件？（例如伤害严重等级可能会有4-6级的伤害） |  |
| 4 | 在降低相关危险前，软件设备的故障是否会导致患者或用户死亡或受重伤？相关示例包括以下： |  |
| 4.a | 软件设备是否控制生命支持/生命维持功能？ |  |
| 4.b | 软件设备是否控制潜在的能导致患者或用户死亡或严重伤害的有害能量的传递？例如：放射治疗系统、除颤器，以及切割发生器？ |  |
| 4.c | 软件设备是否控制当软件发生错误或功能故障时可能导致死亡或严重伤害的治疗措施的进行？ |  |
| 4.d | 软件设备是否提供可直接用于制定治疗决策的信息，如果误用这些信息会导致死亡或严重伤害？ |  |
| 4.e | 软件设备是否具有生命体征监护功能，是否提供在威胁生命安全的情况下需要有医疗介入时会发出警报的功能？ |  |

注 2：如果对以下任一问题的回答为“是”，软件的安全性级别可能是“B级”。

| **序号** | **问题** | **回答** |
| --- | --- | --- |
| 1 | 软件设备是否是具有中等安全性级别医疗设备的一个附件？（例如伤害严重度等级为2、3级） |  |
| 2 | 在降低相关危险前，软件的故障是否会给患者或用户带来较小的伤害？ |  |
| 3 | 是否会因软件故障或软件的设计缺陷而导致错误的诊断，或是使适当的治疗措施延期发生，而这些事件给患者或用户带来较小的伤害？ |  |

注 3：如果对上述两个表的所有问题的回答都是“否”，则软件的安全性级别可能是“A级”。

经过分析，本产品的软件系统的安全性级别定义为：\_\_\_\_\_\_级。

## C.2软件项安全性级别判断

当整个软件系统安全性分级为C级时，对软件系统进行软件项划分，并对高风险部分进行隔离，参考上述原则软件项安全性等级划分如下表。 对使用的未知来源软件，单独进行了安全性等级定义，如下表。（C.2内容可结合软件架构设计细化补充）

| **软件系统（级别）** | **软件一级模块（级别）** | **软件二级模块（级别）** | **所包含未知来源软件（级别）** | **安全隔离说明（C级必须）** |
| --- | --- | --- | --- | --- |
| 系统（C） | 模块1（C） | 模块1-1（C） |  |  |
|  |  | 模块1-2（B） | XXXX软件（B） | 模块1-1与模块1-2采用隔离措施为： |
|  |  |  |  |  |

## C.3产品网络安全性等级判断

网络安全风险级别一般情况下可参照软件安全性级别，考虑因网络安全遇到攻击或威胁，对患者、用户造成身体、财产的伤害。通常认为医疗器械网络安全的风险级别与所属医疗器械软件的安全性级别相同，但也可结合医疗器械的预期用途、不同使用场景的网络环境差异、核心功能进行综合判定。如判断网络安全的风险级别可低于软件风险级别，应详述理由。若产品于其可应用于不同的使用场景（如可同时满足医院使用及家庭使用时），应针对每个使用场景分别判断产品网络安全性等级。

本产品使用场景下的网络环境为：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

本产品本身与网络使用接口包括：\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

经过分析，本产品应用于\_\_\_\_\_\_\_\_\_\_\_\_的使用环境下， 其网络安全的安全性级别定义为：\_\_\_\_\_\_\_级。

# 附录D：危害分析工作表

| **编号** | **危害** | **事件序列** | **危险情况** | **伤害** | **原因** | **前** | | | **风险控制措施** | **后** | | | **参考文件** | **受益风险分析（欧盟市场）** | **是否产生新的风险** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **S** | **O** | **风险** |  | **S** | **O** | **风险** |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

备注 1：可用性相关内容要求：与危害相关的使用场景的识别和描述应该与已识别的危害和危害处境相联系。每个已识别的与危害相关的使用场景的描述，应包括所有危害、事件序列（“危害分析工作表中的事件序列”中必须包含使用错误，并用下划线标注出来）、危害处境以及损害和损害的严重度。识别出的与危险相关的使用场景都应该进行总结性评价。

备注 2：软件相关内容要求：软件有关的危险源其风险程度可能达到C级或B级，在危害分析工作表中的编号上做“C级或B级”标识。

# 附录E：综合剩余风险分析及评价

根据 ISO 14971：2019 中 8 评价综合剩余风险的方法，对本产品已识别的风险及其剩余风险进行综合分析如下：

1. 基于产品的预期用途及基本安全性能与基本性能，产品所有己识别风险的单一剩余风险经评估，均为可接受；再次分析单个风险的风险控制措施之间并无相互冲突，或引发新的风险；评估结果见附录D中采取风险措施后的“风险”栏的结果。
2. 检査产品说明书、操作指导手册、维修保养手册中相关安全信息（包含剩余风险）告知内容，对于重大剩余风险已进行详尽的说明，具体如下。未发现说明或提示信息有冲突或难以执行的现象，文字或图示清晰易懂，未引发新的综合剩余风险。
3. 检査附录 D 风险控制措施中的告警内容，以法规要求及可用性风险分析综合考虑，告警设定已满足法规要求目在可用性方面的剩余风险在可接受范围。综合剩余风险可接受。
4. 来源于不同危害处境而导致的同一种伤害，综合考虑多个危害处境下这种伤害发生的概率及影响，其所造成的的综合剩余风险是可接受的；分析结果以“事件树”的方式列表如下：（摘录附录D中导致相同伤害的不同危害及事件序列，综合考虑这一类伤害可能发生的概率，并评估其是否可接受）

| **编号** | **危害** | **事件序列** | **危险情况** | **伤害** | **单一剩余风险** | | | **综合剩余风险** | | | **理由说明** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **S** | **O** | **风险** | **S** | **O** | **风险** |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |

1. 对于仍处于高风险区域的，或有相互影响的单一剩余风险，综合其危害处境下伤害发生的概率及影响，其所造成的的综合剩余风险也是可接受的；分析结果以“事件树”的方式列表如下：（摘录附录D中严重度为“5、6”级的单一剩余风险，或风险矩阵中处于不可接受范围边界的单一剩余风险.或在制定风险措施时进行过综合受益平衡的单一剩余风险、或多个风险项的风险措施间会有相互影响的单一剩余风险，综合考虑这一类伤害可能发生的概率，并评估其是否可接受）

| **编号** | **危害** | **事件序列** | **危险情况** | **伤害** | **单一剩余风险** | | | **综合剩余风险** | | | **理由说明** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **S** | **O** | **风险** | **S** | **O** | **风险** |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |

1. 所有单一剩余风险的风险评估矩阵分布视图如下，可见到剩余风险都处于可接受区域，并大部分远离风险不可接受的边界线，综合判断，本产品的综合剩余风险为可接受。（摘录附录C中所有采取风险措施后单一剩余风险的风险评估结果于下表对应位置）

| **发生概率（O）** | | | | | | |
| --- | --- | --- | --- | --- | --- | --- |
| **严重度（S）** | **1** | **2** | **3** | **4** | **5** | **6** |
| 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 | | | | | | |

1. 与已上市同类产品或类似产品的安全性比较（必要时）
2. 专家评估结论：

本产品经临床试验、动物实验、可用性用户测试等，使用者及用户专家得出使用结论为：本产品满足预期用途，且安全有效。

参考文件：（文件编号）产品临床试验报告

（文件编号）产品可用性总结性评价报告