ICS 11.040.01;35.240.80
C 30

YY

中华人民共和国医药行业标准

YY/T 0664—2020
代替 YY/T 0664—2008

医疗器械软件　软件生存周期过程

Medical device software—Software life cycle processes

(IEC 62304:2015,MOD)

2020-09-27 发布　　2021-09-01 实施

国家药品监督管理局　　发布

目　　次

前言 …… Ⅲ
引言 …… Ⅴ
1　范围 …… 1
1.1　*目的 …… 1
1.2　*应用范围 …… 1
1.3　与其他标准的关系 …… 1
1.4　符合性 …… 1
2　*规范性引用文件 …… 1
3　*术语和定义 …… 2
4　*总要求 …… 6
4.1　*质量管理体系 …… 6
4.2　*风险管理 …… 6
4.3　*软件安全分级 …… 6
4.4　*遗留软件 …… 8
5　软件开发过程 …… 9
5.1　*软件开发策划 …… 9
5.2　*软件需求分析 …… 11
5.3　*软件体系结构设计 …… 13
5.4　*软件详细设计 …… 13
5.5　*软件单元的实现 …… 14
5.6　*软件集成和集成测试 …… 15
5.7　*软件系统测试 …… 16
5.8　*软件在系统级别应用的发布 …… 17
6　软件维护过程 …… 18
6.1　*建立软件维护计划 …… 18
6.2　*问题和修改分析 …… 18
6.3　*修改的实施 …… 19
7　*软件风险管理过程 …… 19
7.1　*促成危险情况的软件分析 …… 19
7.2　风险控制措施 …… 20
7.3　风险控制措施的验证 …… 20
7.4　软件变更的风险管理 …… 20
8　*软件配置管理过程 …… 21
8.1　*配置标识 …… 21
8.2　*变更控制 …… 21
8.3　*配置状态报告 …… 22

9 * 软件问题解决过程 …… 22
9.1 编写问题报告 …… 22
9.2 调查问题 …… 22
9.3 通知相关方 …… 22
9.4 使用变更控制过程 …… 22
9.5 保持记录 …… 22
9.6 分析问题的趋势 …… 23
9.7 验证软件问题的解决 …… 23
9.8 测试文档的内容 …… 23
附录 A（资料性附录） 本标准要求的理由说明 …… 24
附录 B（资料性附录） 关于本标准条款的指南 …… 26
附录 C（资料性附录） 与其他标准的关系 …… 39
附录 D（资料性附录） 实施 …… 55
参考文献 …… 57

图 1 软件开发过程和活动图示 …… Ⅴ
图 2 软件维护过程和活动图示 …… Ⅵ
图 3 赋予软件安全级别 …… 7
图 B.1 危险（源）、事件序列、危险情况和伤害关系的图示（源于 YY/T 0316—2016 的附录 E） …… 29
图 B.2 软件项划分示例 …… 30
图 B.3 法规视角——现成软件与未知来源软件、遗留软件之间的关系 …… 32
图 C.1 重要医疗器械标准与本标准的关系 …… 39
图 C.2 软件作为 V 模型的一部分 …… 42
图 C.3 YY/T 0664 与 IEC 61010-1 联合应用 …… 48

表 A.1 按软件安全级别的要求汇总 …… 25
表 B.1 ISO/IEC 12207 中规定的开发（模型）策略 …… 26
表 C.1 与 YY/T 0287—2017 的关系 …… 40
表 C.2 与 YY/T 0316—2016 的关系 …… 41
表 C.3 与 IEC 60601-1 的关系 …… 43
表 C.4 与 ISO/IEC 12207:2008 的关系 …… 49
表 D.1 用于未经质量管理体系认证的小型制造商的检查表 …… 55

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准代替 YY/T 0664—2008《医疗器械软件　软件生存周期过程》，与 YY/T 0664—2008 相比，除编辑性修改外主要技术变化如下：

——纳入国际标准 IEC 62304:2006/AMD1:2015 的修正内容，这些修正内容涉及的章条已通过在其外侧页边空白位置的垂直双线(||)进行了标示。主要修订内容包括：

- 删除了术语“软件产品”(2008 年版的 3.26)，用“医疗器械软件”(见 3.11)代替“软件产品”；
- 增加了“危险情况”(见 3.33)、“遗留软件”(见 3.34)、“发布”(见 3.35)、“剩余风险”(见 3.36)、“风险估计”(见 3.37)、“风险评价”(见 3.38)的术语和定义；
- 修改了“软件安全分级”的要求(见 4.3，2008 年版的 4.3)；
- 增加了“图 3 赋予软件安全级别”(见 4.3)；
- 增加了“遗留软件”的要求(见 4.4)；
- 增加了“识别和避免常见软件缺陷”的要求(见 5.1.12)；
- 修改了“验证软件集成”的要求(见 5.6.2，2008 年版的 5.6.2)；
- 修改了条款适用的软件安全级别(见 5.7.1、5.7.2、5.7.3、5.8.1、5.8.2、5.8.7、5.8.8，2008 年版的 5.7.1、5.7.2、5.7.3、5.8.1、5.8.2、5.8.7、5.8.8)；
- 修改了“评价软件系统测试”的要求(见 5.7.4，2008 年版的 5.7.4)；
- 修改了“软件系统测试记录的内容”(见 5.7.5，2008 年版的 5.7.5)；
- 删除了“将事件序列形成文档”的要求(2008 年版的 7.1.5)；
- 删除了“将任何新事件序列形成文档”的要求(2008 年版的 7.3.2)；
- 修改了“编写问题报告”的要求(见 9.1，2008 年版的 9.1)；
- 修改了“软件安全分级”的指南(见附录 B.4.3，2008 年版附录 B.4.3)；
- 增加了“遗留软件”的指南(见附录 B.4.4)。

——修改了术语“异常”为“反常”(见 3.2，2008 年版的 3.2)。

——修改了术语“危害”为“危险(源)”(见 3.9，2008 年版的 3.9)。

——修改了术语“安全性”为“安全”(见 3.20，2008 年版的 3.21)，全文用“安全”代替“安全性”。

——修改了术语“严重伤害”为“严重损伤”(见 3.22，2008 年版的 3.23)。

——由于翻译对部分内容进行的修改。

本标准使用重新起草法修改采用 IEC 62304:2015《医疗器械软件　软件生存周期过程》。

本标准与 IEC 62304:2015 相比较存在技术性差异，这些差异涉及的条款已通过在其外侧页边空白位置的垂直单线(|)进行了标示。主要技术性差异及原因如下：

——关于规范性引用文件，本标准做了具有技术性差异的调整，以适应我国的技术条件，调整的情况集中反映在第 2 章“规范性引用文件”中，具体调整如下：

- 用等同采用国际标准的 YY/T 0316 代替 ISO 14971。

——针对删除了的术语、条款或列项中涉及“不使用”的内容，相应序号(包括表序号)顺延，以符合 GB/T 1.1 的规定，确保技术内容的确定和文本结构的协调统一；

——修改了术语“制造商(见 3.10)”的定义，以便与 YY/T 0287—2017 标准保持一致；

——删除了术语“医疗器械”，因医疗器械法规和 YY/T 0287—2017 中均对“医疗器械”有定义，本标准不再重复；

——修改了术语“过程(见 3.13)”“验证(见 3.31)”的定义,以便与 GB/T 19000—2016 保持一致;

——修改了术语“回归测试”(见 3.14)的定义,以便与 ISO/IEC/IEEE 90003:2018 保持一致;

——修改了术语“损害”(见 2008 年版的 3.8)为“伤害”(见 3.8),并修改了定义,以便与 YY/T 0316—2016 保持一致;

——修改了术语“保密安全”(见 2008 年版的 3.22)为“信息安全”(见 3.21),并修改了定义,以便与 ISO/IEC/IEEE 12207:2017 保持一致;

——将“软件以外的风险控制措施”“软件系统以外的风险控制措施”“不在软件系统内(以外)实施的风险控制措施”“(软件系统)以外的风险控制措施”统一修改为“外部风险控制措施”(见 4.3 和图 3),以便与法规保持一致;

——修改了 8.2.2 注/8.2.3 注中“5.1.1 e)”为“5.1.1 d)”,基于标准上下文,纠正编辑性错误;

——增加了附录 B.4.5 法规视角,以便理解标准和法规要求;

——删除了图 3 中 IEC 标注,图中内容与 IEC 62304:2015 存在技术性变化;

——修改了附录 C 中表 C.1 和表 C.2,以便分别与 YY/T 0287—2017 和 YY/T 0316—2016 保持一致;

——删除了附录 C.4.7,因 IEC 60601-1-4 已废止;

——删除了第 3 章中定义的术语索引,不使用。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由国家药品监督管理局提出。

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

本标准起草单位:北京国医械华光认证有限公司、中国食品药品检定研究院、国家药品监督管理局医疗器械技术审评中心、北京怡和嘉业医疗科技股份有限公司、东软医疗系统股份有限公司、上海微创医疗器械(集团)有限公司、深圳迈瑞生物医疗电子股份有限公司、上海西门子医疗器械有限公司、康泰医学系统(秦皇岛)股份有限公司、北京推想科技有限公司。

本标准主要起草人:刘荣敏、吕建英、郑佳、彭亮、陈兴文、王志强、李勇、殷骏、高云琼、李学勇、陈宽、李朝晖、王美英、许慧雯、陈蓓、严佳玲、杨智明、王少康、邵玉波、韦晓洁。

本标准所代替标准的历次版本发布情况为:

——YY/T 0664—2008。

引　言

软件通常是医疗器械技术的一个组成部分。建立包含软件的医疗器械的安全和有效性，要求有软件预期用途的知识，并要证实软件的使用在没有引起任何不可接受的风险的情况下实现预期目的。

本标准为医疗器械软件的安全设计和维护提供了一个生存周期过程框架，包括必要的活动和任务。本标准为每个生存周期过程规定了要求。每个生存周期过程由一组活动组成，多数活动又由一组任务组成。

作为主要的基础，这里设定医疗器械软件是在质量管理体系（见 4.1）和风险管理体系（见 4.2）之内开发和维护的。风险管理过程已在 YY/T 0316 中得到很好地阐述。因此本标准通过直接对 YY/T 0316的规范性引用，利用了该有利条件。对软件来说少量附加的风险管理要求是必要的，特别是在识别与危险（源）有关的软件影响因素方面。将这些要求加以汇总并纳入第七章作为软件风险管理过程。

在风险管理过程的危险（源）识别活动中确定软件是否为危险情况的促成因素。在确定软件是否是促成因素时，需要考虑可能由软件间接造成的危险情况（例如：通过提供可能导致给予不适当治疗的误导性信息）。在风险管理过程的风险控制活动中做出使用软件来控制风险的决定。本标准要求的软件风险管理过程必须包含在按照 YY/T 0316 建立的医疗器械风险管理过程之中。

软件开发过程由若干活动组成。这些活动如图 1 所示，并在第 5 章中描述。因为现场的许多事件与医疗器械系统的服务或维护有关，包括不适当的软件更新和升级，软件维护过程被视为与软件开发过程一样重要。软件维护过程和软件开发过程很相似，如图 2 所示和第 6 章的描述。

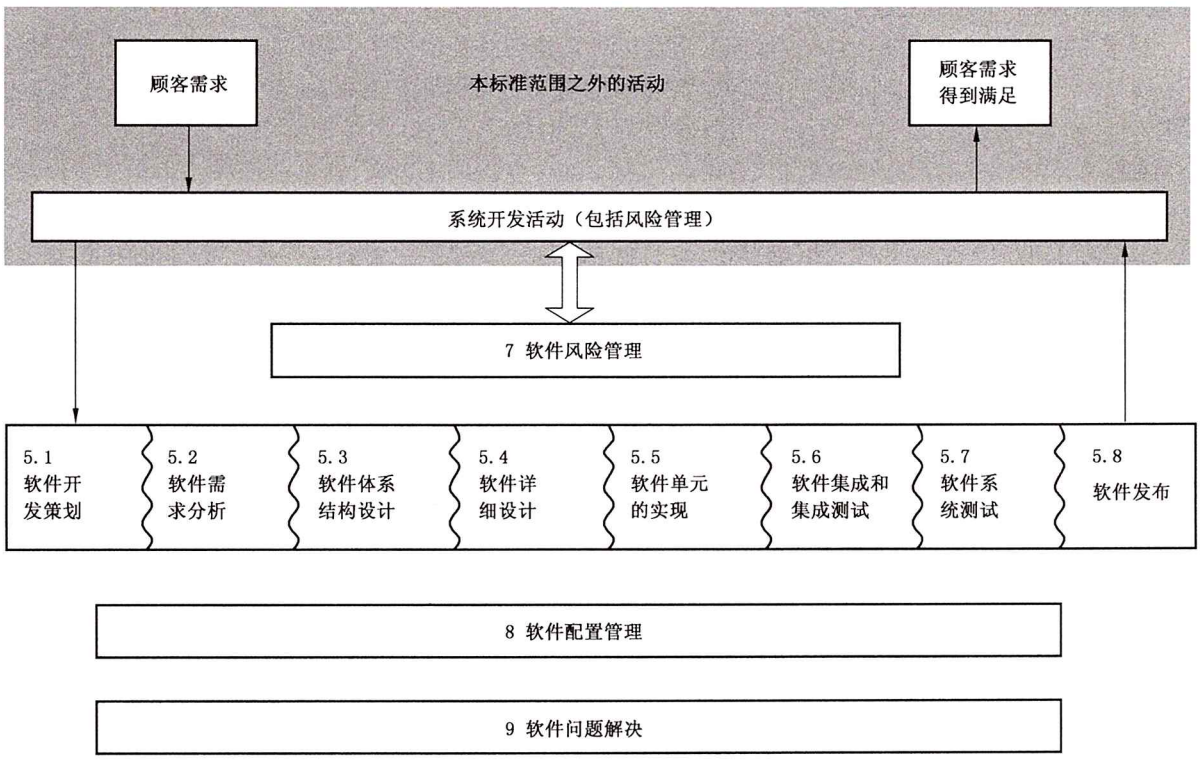


图 1　软件开发过程和活动图示

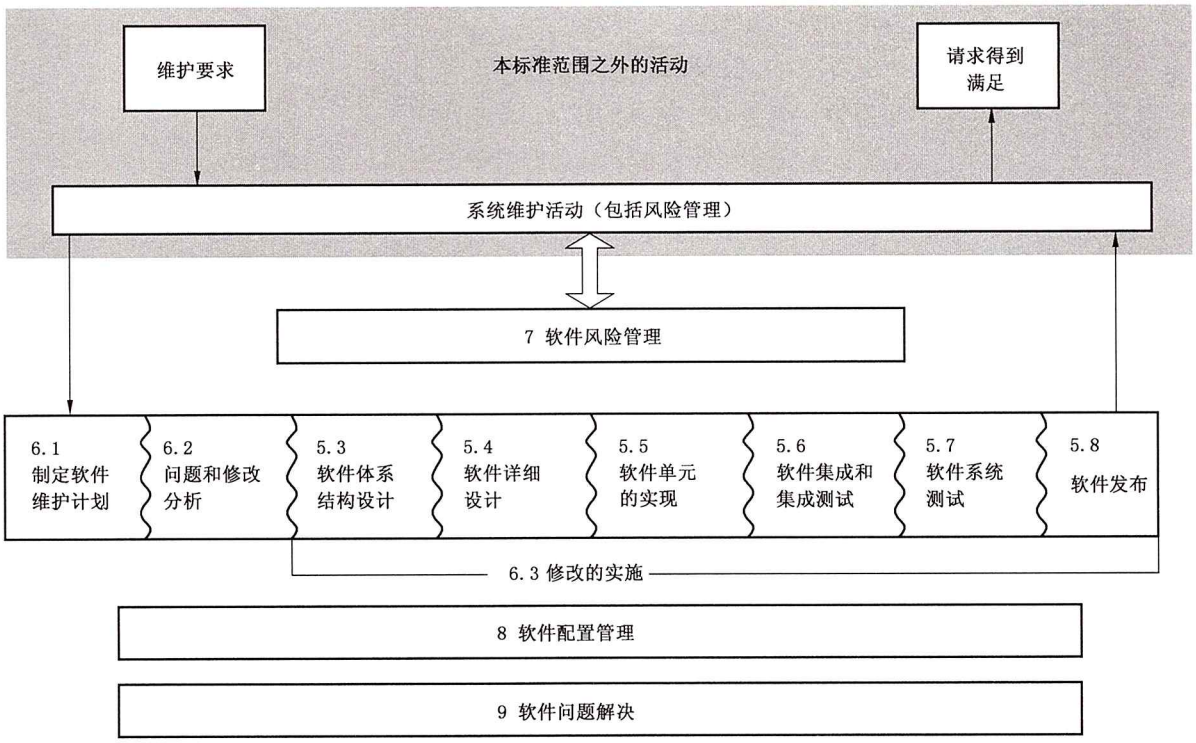


图 2　软件维护过程和活动图示

本标准为开发安全的医疗器械软件规定了两个必不可少的附加过程，即软件配置管理过程（见第 8 章）和软件问题解决过程（见第 9 章）。

对于本标准发布前的软件设计，本标准增加了处理遗留软件的要求，以帮助制造商符合标准进而满足法规要求。软件安全级别的变更包括对要求的说明和对软件安全级别的更新，以纳入基于风险的方法。

本标准不为制造商规定组织结构，或组织的哪一部分完成哪个过程、活动或任务。本标准只要求完成过程、活动或任务以建立对本标准的符合性。

本标准不指定要形成文档的名称、格式或明确的内容。本标准要求编制任务文档，但如何组合编排这些文档的决定留给标准的使用者。

本标准不指定特定的生存周期模型。本标准的使用者负责为软件项目选择生存周期模型，并将本标准中的过程、活动和任务映射在该模型上。

附录 A 为本标准各章提供理由说明。附录 B 为本标准各条款提供指南。

对于本标准：

- “应（shall）”意指为符合本标准，符合一项要求是强制性的。
- “宜（should）”意指为符合本标准，符合一项要求是推荐性的但不是强制性的。
- “可（may）”用于描述符合一项要求的一种允许的方式。
- “建立（establish）”意指规定、形成文件并实施。

本标准中术语“适当时（as appropriate）”与要求的过程、活动、任务或输出一起使用时，意指制造商应使用该过程、活动、任务或输出，除非制造商能以文件形式说明不这样做的合理理由。

本标准中带星号（*）的条款表示在附录 B 中有关于该条款的指南。

医疗器械软件　软件生存周期过程

1　范围

1.1　*目的

本标准为医疗器械软件规定了生存周期要求。本标准中描述的一组过程、活动和任务，为医疗器械软件生存周期过程建立了共同的框架。

1.2　*应用范围

本标准适用于医疗器械软件的开发和维护。医疗器械软件包括本身是医疗器械的软件或是最终医疗器械的嵌入部分或组成部分的软件。

注 1：本标准可用于本身是医疗器械的软件的开发和维护。然而，在该类型软件能够投入使用之前，还需要在系统级上进行附加的开发活动。本标准不覆盖这些系统级活动，相关要求可参见 IEC 82304-1[1]。

本标准描述了预期应用于软件的过程，该类软件可在处理器上执行或通过在处理器上运行的其他软件（例如解释器）执行。

无论使用何种持久存储设备存储软件（例如：硬盘、光盘、永久内存或闪存），本标准均适用。

无论使用何种交付方法交付软件［例如：通过网络或电子邮件传输，或光盘、闪存或带电可擦除编程只读存储器（EEPROM）等物理移送］，本标准均适用。软件交付方法本身不视为医疗器械软件。

本标准不覆盖医疗器械的确认和最终发布，即使该医疗器械完全由软件组成。

注 2：如果医疗器械包含拟在处理器上执行的嵌入式软件，则本标准的要求适用于该软件，包括有关未知来源软件的要求（见 8.1.2）。

注 3：在软件和医疗器械能够投入使用之前，需要在系统级上进行确认和其他开发活动。本标准不覆盖这些系统级活动，可参见相关产品标准（如 IEC 60601-1[4]，IEC 82304-1[1]等）。

1.3　与其他标准的关系

在开发医疗器械时，本医疗器械软件生存周期标准和其他适用的标准共同使用。本标准与其他相关标准之间的关系参见附录 C。

1.4　符合性

符合本标准意指按照软件安全级别，实施在本标准中确定的所有过程、活动和任务。

注 1：为每项要求赋予的软件安全级别在正文中标注在该项要求之后。

通过对本标准所要求的所有文档（包括风险管理文档）的检查和对软件安全级别所要求的过程、活动和任务的评定来确定符合性。

注 2：此种评定可通过内部或外部的审核来进行。

注 3：尽管要完成特定的过程、活动和任务，但实施这些过程和执行这些活动和任务的方法具有灵活性。

注 4：若任何包含“适当时（as appropriate）”的要求未实施，为说明理由而形成的文档对于本评定是必要的。

注 5：本标准中用术语“符合性（compliance）”之处，在 ISO/IEC 12207 中用术语“符合性（conformance）”。

注 6：有关遗留软件的符合性，见 4.4。

2　*规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文

件。凡是不注日期的引用文件，其最新版本(包括所有修改单)适用于本文件。

YY/T 0316 医疗器械 风险管理对医疗器械的应用(YY/T 0316—2016，ISO 14971:2007 更正版，IDT)

3 术语和定义

下列术语和定义适用于本文件。

3.1

活动 activity

一组单个或多个相互关联或相互作用的任务。

3.2

反常 anomaly

与基于需求规范、设计文件和标准等的预期，或人的认知或经验相偏离的任何情况。反常可能但不限于在医疗器械软件或适用文档的评审、测试、分析、编译/编辑或使用过程中发现。

注：改写 IEEE 1044:1993，定义 3.1。

3.3

体系结构 architecture

系统或组件的组织结构。

[IEEE 610.12:1990]

3.4

变更请求 change request

拟对医疗器械软件所做变更的形成文件的说明。

3.5

配置项 configuration item

在给定参考点上能够唯一标识的实体。

注：改写 ISO/IEC 12207:2008，定义 4.7。

3.6

交付物 deliverable

对一项活动或任务所要求的结果或输出(包括文档)。

3.7

评价 evaluation

对一个实体满足其规定准则的程度的系统性确定。

[ISO/IEC 12207:2008，定义 4.12]

3.8

伤害 harm

对人体的损伤或对人体健康的损害，或对财产或环境的损害。

[YY/T 0316—2016，定义 2.2]

3.9

危险(源) hazard

可能导致伤害的潜在根源。

[YY/T 0316—2016，定义 2.3]

3.10

制造商 manufacturer

以其名义制造预期可用的医疗器械并负有医疗器械设计和/或制造责任的自然人或法人，无论此医

疗器械的设计和/或制造是由该自然人或法人进行或由另外的一个或多个自然人或法人代表其进行。

注1：此“自然人或法人”对确保符合医疗器械预期可用或销售的国家或管辖区的所有适用的法规要求负有最终法律责任，除非该管辖区的监管机构(RA)明确将该责任强加于另一自然人或法人。

注2：在其他GHTF指南文件中说明了制造商的责任。这些责任包括满足上市前要求和上市后要求，比如不良事件报告和纠正措施通知。

注3：上述定义中所指的“设计和/或制造”可包括医疗器械的规范制定、生产、制造、组装、加工、包装、重新包装、标记、重新标记、灭菌、安装或再制造；或为了医疗目的而将多个器械(可能包括其他产品)组合在一起。

注4：假如组装或修改不改变医疗器械的预期用途，该医疗器械已经由另一自然人或法人按照使用说明书提供给个体患者，组装或修改医疗器械的任何自然人或法人不是制造商。

注5：不是以原制造商的名义更改医疗器械的预期用途或改进医疗器械的任何自然人或法人，使器械以其名义提供使用，宜认为是改进后的医疗器械的制造商。

注6：不覆盖或改变现有标记，只将自己的地址和联系方式加在医疗器械上或包装上的授权代表、经销商或进口商，不被认为是制造商。

注7：纳入医疗器械法规要求的附件，负责设计和/或制造该附件的自然人或法人被认为是制造商。

[YY/T 0287—2017，定义3.10]

3.11

医疗器械软件　medical device software

旨在集成到正在开发的医疗器械中的已开发的软件系统，或者预期作为医疗器械使用的软件系统。

3.12

问题报告　problem report

使用者或其他利益相关人员认为对预期使用不安全、不适当或违反规范的医疗器械软件实际或潜在特性的记录。

注1：本标准不要求每个问题报告都引起对医疗器械软件的变更。制造商可拒绝误导性的、误判的或无关紧要事件的问题报告。

注2：问题报告可能与已发布的医疗器械软件或仍在开发中的医疗器械软件有关。

注3：本标准要求制造商对涉及已发布产品的问题报告实施额外的决策步骤(见第6章)，以确保监管措施的识别和实施。

3.13

过程　process

利用输入实现预期结果的相互关联或相互作用的一组活动。

注1：过程的“预期结果”称为输出，还是称为产品或服务，随相关语境而定。

注2：一个过程的输入通常是其他过程的输出；而一个过程的输出又通常是其他过程的输入。

注3：两个或两个以上相互关联和相互作用的连续过程也可作为一个过程。

注4：组织通常对过程进行策划，并使其在受控条件下运行，以增加价值。

注5：不易或不能经济地确认其输出是否合格的过程，通常称之为“特殊过程”。

注6：这是ISO/IEC 导则 第1部分 ISO补充规定的附件SL中给出的ISO管理体系标准中通用术语及核心定义之一，最初的定义已经被改写，以避免过程和输出之间循环解释，并增加注1～注5。

[GB/T 19000—2016，定义3.4.1]

3.14

回归测试　regression testing

在对测试项或其运行环境修改后进行的测试，以确定是否出现回归失效。

注：回归测试用例集的充分性取决于所测试的测试项，以及对该测试项或其运行环境的修改。

[ISO/IEC/IEEE 90003:2018，定义3.6]

3.15

风险　risk

伤害发生的概率和该伤害严重度的组合。

[YY/T 0316—2016,定义 2.16]

3.16

风险分析　risk analysis

系统地运用现有信息确定危险(源)和估计风险的过程。

[YY/T 0316—2016,定义 2.17]

3.17

风险控制　risk control

作出决策并实施措施,以便降低风险或把风险维持在规定水平的过程。

[YY/T 0316—2016,定义 2.19]

3.18

风险管理　risk management

用于风险分析、评价、控制工作的管理方针、程序及其实践的系统运用。

注:改写 YY/T 0316—2016,定义 2.22,删除了"和监视"。

3.19

风险管理文档　risk management file

由风险管理产生的一组记录和其他文件。

[YY/T 0316—2016,定义 2.23]

3.20

安全　safety

免除了不可接受的风险的状态。

[YY/T 0316—2016,定义 2.24]

3.21

信息安全　security

防止蓄意破坏或强制失效,保密性、完整性、可得性和可核查性四个属性的组合,及第五个属性可用性,所有这些属性均有保证性的问题。

注:改写 ISO/IEC/IEEE 12207:2017,定义 3.1.49。

3.22

严重损伤　serious injury

导致下列结果的损伤或疾病:

a)　危及生命;

b)　造成人体功能的永久性损害或人体结构的永久性损坏;

c)　需要内科或外科介入以防止人体功能的永久性损害或人体结构的永久性损坏。

注:永久性损害意味着人体结构或功能不可逆的损害或损坏,微不足道的损害或损坏除外。

3.23

软件开发生存周期模型　software development life cycle model

贯穿从需求定义到发布的软件生存周期的概念结构,其:

——识别医疗器械软件开发中包含的过程、活动和任务;

——描述活动和任务之间的顺序和依赖关系;

——识别特定交付物完整性验证时机的里程碑。

注:改写 ISO/IEC 12207:1995,定义 3.11。

3.24

软件项　software item

计算机程序中任何可识别的部分,例如:源代码、目标代码、控制代码、控制数据或这些项的集合。

注 1：三个术语描述软件分解。顶层是软件系统。最底层不能进一步分解的是软件单元。该结构的所有层级，包括顶层和底层，都可以称为软件项。软件系统则由一个或多个软件项组成，而每个软件项由一个或多个软件单元或可分解的软件项组成。提供软件项和软件单元的粒度是制造商的责任。

注 2：改写 GB/T 19003—2008，定义 3.14 和 ISO/IEC 12207:2008，定义 4.41。

3.25

软件系统　software system

有组织的、经集成的软件项组合，以完成某个特定功能或一组功能。

3.26

软件单元　software unit

不可再分的软件项。

注：软件单元的粒度由制造商定义（参见 B.3）。

3.27

未知来源软件　software of unknown provenance；SOUP

已经开发且通常可得到，并且不是为包含到医疗器械内而开发的软件项（也称为“成品软件”）；或以前开发的、不能得到其开发过程足够记录的软件项。

注：医疗器械软件系统本身不能声称是未知来源软件。

3.28

系统　system

由一个或多个过程、硬件、软件、设施和人员组成的集合体，提供满足规定需求或目标的能力。

注：改写 ISO/IEC 12207:2008，定义 4.48。

3.29

任务　task

需要完成的单项工作。

3.30

可追溯性　traceability

开发过程的两个或多个交付物间能够建立关联的程度。

[IEEE 610.12:1990]

注：开发过程交付物的示例包括：需求、体系结构、风险控制措施等。

3.31

验证　verification

通过提供客观证据对规定要求已得到满足的认定。

注 1：验证所需的客观证据可以是检验结果或其他形式的确定结果，如：变换方法进行计算或文件评审。

注 2：为验证所进行的活动有时被称为鉴定过程。

注 3：“已验证”一词用于表明相应的状态。

[GB/T 19000—2016，定义 3.8.12]

注 4：在设计和开发中，验证涉及检查给定活动的结果的过程以确定该项活动与规定要求的符合性。

3.32

版本　version

一个配置项已标识的实例。

注 1：对医疗器械软件的某版本进行修改会产生一个新版本，需要对修改实施配置管理措施。

注 2：改写 ISO/IEC 12207:2008，定义 4.56。

3.33

危险情况　hazardous situation

人员、财产或环境暴露于一个或多个危险（源）中的情形。

[YY/T 0316—2016,定义 2.4]

3.34

遗留软件 legacy software

合法地投放市场且至今仍在销售的医疗器械软件,但其开发符合本标准现行版本的客观证据不充分。

3.35

发布 release

为特定目的提供一个配置项的特定版本。

注:改写 ISO/IEC 12207:2008,定义 4.35。

3.36

剩余风险 residual risk

实施风险控制措施后还存在的风险。

注 1:改写 GB/T 20000.4:2003,定义 3.9。

注 2:GB/T 20000.4:2003,定义 3.9 使用术语"防护措施"而不使用"风险控制措施"。然而,在 YY/T 0316—2016 中,"防护措施"只是 6.2 所描述的风险控制方案之一。

[YY/T 0316—2016, 定义 2.15]

3.37

风险估计 risk estimation

用于对伤害发生概率和该伤害严重度赋值的过程。

[YY/T 0316—2016,定义 2.20]

3.38

风险评价 risk evaluation

将估计的风险与给定的风险准则进行比较,以决定风险可接受性的过程。

[YY/T 0316—2016,定义 2.21]

4 *总要求

4.1 *质量管理体系

医疗器械软件制造商应证实其有能力提供持续满足顾客要求和适用法规要求的医疗器械软件。

注 1:可通过应用符合下列要求的质量管理体系,证实此能力:

——YY/T 0287[5];

——国家质量管理体系标准;或

——国家法规要求的质量管理体系。

注 2:将质量管理体系要求应用于软件的指南参见 ISO/IEC 90003[17]。

4.2 *风险管理

制造商应应用符合 YY/T 0316 的风险管理过程。

4.3 *软件安全分级

软件安全分级应满足如下准则和要求:

a) 制造商应根据软件系统在最不利情况下(如图 3 所示)促成的危险情况引发的对患者、操作者或其他人员伤害的风险,赋予每个软件系统一个软件安全级别(A、B 或 C)。

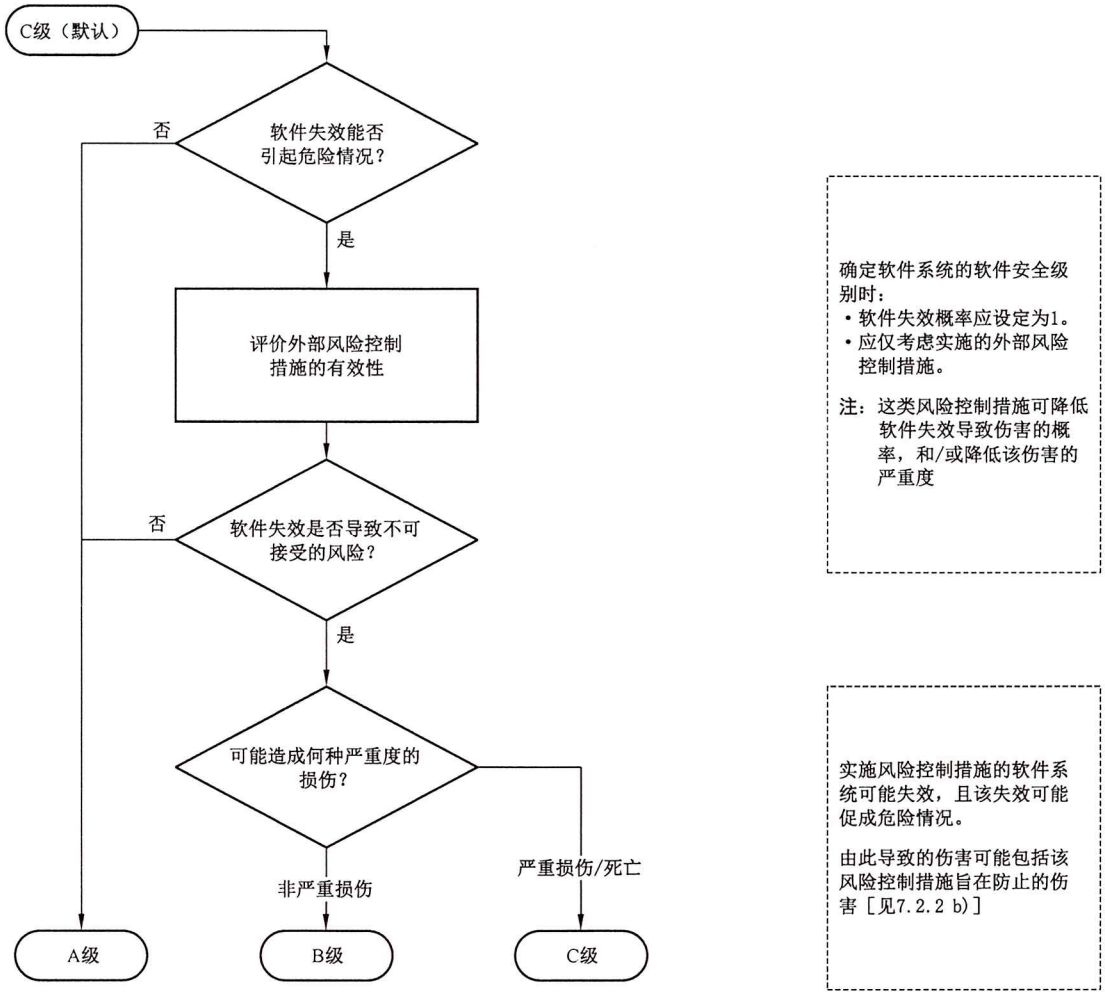


图 3　赋予软件安全级别

下列情况下软件系统的软件安全级别为 A：

——软件系统不可能促成危险情况；或

——在考虑外部风险控制措施后，软件系统可能促成不导致不可接受风险的危险情况。

下列情况下软件系统的软件安全级别为 B：

——在考虑外部风险控制措施后，软件系统可能促成导致不可接受风险的危险情况，且导致的可能伤害是非严重损伤。

下列情况下软件系统的软件安全级别为 C：

——在考虑外部风险控制措施后，软件系统可能促成导致不可接受风险的危险情况，且导致的可能伤害是死亡或严重损伤。

对于最初分类为软件安全级别 B 或 C 的软件系统，制造商可以实施软件系统外部附加风险控制措施（包括修改含有软件系统的系统体系结构），并在随后为软件系统赋予新的软件安全级别。

注 1：外部风险控制措施是指软件系统以外的风险控制措施，可以是硬件、单独的软件系统、医疗程序或其他方法，以最大程度地降低软件促成的危险情况。

注 2：关于风险可接受性的定义，见 YY/T 0316—2016 的 3.2。

b）　制造商应在风险管理文档中将赋予每个软件系统的软件安全级别形成文件。

c）　当一个软件系统分解为多个软件项，及当一个软件项又进一步分解为多个软件项时，此类软

件项应继承原软件项(或软件系统)的软件安全级别,除非制造商以文件形式说明分类为不同软件安全级别的理由[根据 4.3 a)用"软件项"替换"软件系统"赋予的软件安全级别]。此类理由说明应解释新的软件项如何被隔离,以便可对其单独分级。

d) 如果以分解方式产生的软件项的安全级别与其原软件项不同,制造商应将每个此类软件项的软件安全级别形成文件。

e) 为符合本标准,当本标准应用于一组软件项时,制造商应使用此组中级别最高的软件项所要求的诸过程和任务,除非制造商在风险管理文档中将使用较低级别的理由说明形成文件。

f) 对每个软件系统,在赋予软件安全级别以前,均应应用 C 级要求。

注:在随后的章条中,对每一特定要求所适用的软件安全级别,以[…级]的形式标注于该要求之后。

4.4 * 遗留软件

4.4.1 概述

针对遗留软件,作为应用第 5 章~第 9 章的替代方案,可按照 4.4.2~4.4.5 所述证实遗留软件的符合性。

4.4.2 风险管理活动

根据 4.2 的要求,制造商应:

a) 评定来自该组织内部和/或用户的有关遗留软件事件和/或险肇事件的任何反馈,包括生产后信息;

b) 实施与继续使用遗留软件相关的风险管理活动,并考虑以下方面:

——在整个医疗器械体系结构中遗留软件的集成;

——作为遗留软件一部分实施的风险控制措施是否持续有效;

——与遗留软件继续使用相关的危险情况的识别;

——遗留软件促成危险情况的潜在原因的识别;

——针对遗留软件促成危险情况的每个潜在原因,确定风险控制措施。

4.4.3 差距分析

基于遗留软件的软件安全级别(见 4.3),制造商应根据 5.2、5.3、5.7 和第 7 章的要求对可获得的交付物进行以下差距分析:

a) 制造商应评定可获得的交付物是否持续有效;

b) 识别到差距之处,制造商应针对缺失的交付物和相关活动,评价弥补措施对风险的潜在降低;

c) 基于此评价,制造商应确定拟创建的交付物和拟执行的相关活动。交付物至少应为软件系统测试记录(见 5.7.5)。

注:该差距分析宜确保对遗留软件所实施的风险控制措施包含在软件需求中。

4.4.4 差距关闭活动

差距关闭活动涉及如下内容:

a) 制造商应建立并执行生成所识别的交付物的计划。若可获得,可使用客观证据生成所需的交付物,而不执行 5.2、5.3、5.7 和第 7 章所要求的活动;

注:关于如何处理已识别差距的计划可包含在软件维护计划中(见 6.1)。

b) 该计划应阐述问题解决过程的使用要求,以便按照第 9 章处置在遗留软件和交付物中发现的问题;

c) 对遗留软件的变更应按照第 6 章进行。

4.4.5 使用遗留软件的理由

制造商应基于4.4的输出将遗留软件的版本连同继续使用遗留软件的理由形成文件。

注：根据本标准，满足4.4的要求即可使用遗留软件。

5 软件开发过程

5.1 * 软件开发策划

5.1.1 软件开发计划

制造商应建立一项(或多项)软件开发计划，以便实施适合于拟开发软件系统的范围、规模和软件安全级别的软件开发过程相关活动。在计划中应完整地定义或引用软件开发生存周期模型。计划应说明下列各项：

a) 用于软件系统开发的过程(见注4)；

b) 各项活动和任务的交付物(包括文档)；

c) 系统需求、软件需求、软件系统测试以及在软件中实施的风险控制措施之间的可追溯性；

d) 软件配置和变更管理，包括未知来源软件的配置项和用于支持开发的软件；

e) 软件问题解决方案，以处理在生存周期各阶段的医疗器械软件、交付物和活动中所发现的问题。

[A、B、C级]

注1：软件开发生存周期模型可根据软件系统的每个软件项的软件安全级别为不同的软件项识别不同的要素(过程、活动、任务和交付物)。

注2：这些活动和任务可以重叠或相互作用，可迭代或循环地完成。其意图并非暗示宜使用特定的生存周期模型。

注3：在本标准中将其他过程与开发过程分开描述。这并非暗示其他过程必须作为单独的活动和任务来实施。可将其活动和任务整合到开发过程中。

注4：软件开发计划可以引用现有的过程或定义新过程。

注5：可将软件开发计划整合到整个系统的开发计划中。

5.1.2 保持对软件开发计划的更新

适当时，制造商应随着开发的进行更新计划。[A、B、C级]

5.1.3 引用系统设计和开发的软件开发计划

在软件开发计划中，制造商应：

a) 引用系统需求，作为软件开发的输入；

b) 包括或引用用于协调软件开发和系统开发所必需的规程以满足4.1的要求(例如系统的集成、验证和确认)。

[A、B、C级]

注：如果软件系统是一个独立的系统(纯软件器械)，在软件系统需求和系统需求之间可能没有区别。

5.1.4 软件开发标准、方法和工具的策划

制造商应在软件开发计划中包括或引用与C级软件项开发有关的：

a) 标准；

b) 方法；

c) 工具。

[C 级]

5.1.5 软件集成和集成测试的策划

制造商应在软件开发计划中包括或引用一项计划，以集成软件项（包括未知来源软件）并在集成过程中完成测试。[B、C 级]

注 1：将集成测试和软件系统测试合并到一项单一的计划和一组活动中是可接受的。

注 2：见 5.6。

5.1.6 软件验证策划

制造商应在软件开发计划中包括或引用下列验证信息：

a） 要求验证的交付物；

b） 每个生存周期活动所要求的验证任务；

c） 对交付物进行验证的里程碑；

d） 验证交付物的验收准则。

[A、B、C 级]

5.1.7 软件风险管理策划

制造商应在软件开发计划中包括或引用一项计划，以实施软件风险管理过程的活动和任务，包括与未知来源软件有关的风险的管理。[A、B、C 级]

注：见第 7 章。

5.1.8 文档的策划

制造商应在软件开发计划中包括或引用有关在软件开发生存周期中要生成的文件的信息。对每个已识别的文件或文件类型，应包括或引用如下信息：

a） 标题、名称或命名约定；

b） 目的；

c） 开发、评审、批准和修改的规程和职责。

[A、B、C 级]

注：文档配置管理考虑的因素见第 8 章。

5.1.9 软件配置管理策划

制造商应在软件开发计划中包括或引用软件配置管理信息。软件配置管理信息应包括或引用：

a） 拟受控项的级别、型式、类别或清单；

b） 软件配置管理活动和任务；

c） 负责实施软件配置管理活动的一个或多个组织；

d） 这些组织和其他诸如软件开发或维护组织的关系；

e） 何时将这些项目置于配置控制之下；

f） 何时使用问题解决过程。

[A、B、C 级]

注：见第 8 章。

5.1.10 拟受控的支持项

拟受控项应包括用于医疗器械软件开发并对医疗器械软件可能有影响的工具、项目或设置。[B、C

级]

注 1：此类项目的示例包括编译器/汇编器的版本、生成文件、批处理文件和特定的环境设置。

注 2：见第 8 章。

5.1.11 验证前软件配置项的控制

制造商应进行策划以将软件配置项在验证之前置于配置管理控制之下。[B、C 级]

5.1.12 识别和避免常见软件缺陷

制造商应在软件开发计划中包括或引用以下规程：

a) 基于所选的与其软件系统相关的编程技术，识别可能引入的缺陷类别；

b) 证实这些缺陷不会促成不可接受风险的形成文件的证据。

注：有关促成危险情况的缺陷或原因类别的示例参见 YY/T 1406.1—2016 的附录 B。

[B,C 级]

5.2 * 软件需求分析

5.2.1 定义来自系统需求的软件需求并将其形成文件

对医疗器械的每个软件系统，制造商应定义来自系统级需求的软件系统需求并形成文件。[A、B、C 级]

注：如果软件系统是一个独立的系统(纯软件器械)，在软件系统需求和系统需求之间可能没有区别。

5.2.2 软件需求的内容

若适用于医疗器械软件，制造商应在软件需求中包括：

a) 功能和性能需求；

注 1：示例包括：

——性能(如软件的目的、时序要求)；

——物理特性(如编码语言、平台、操作系统)；

——软件运行的计算环境(如硬件、存储容量、处理单元、时区、网络基础设施)；

——与升级或多种未知来源软件或其他器械版本的兼容性需求。

b) 软件系统的输入和输出；

注 2：示例包括：

——数据特性(如数字的、字母数字的、格式)；

——范围；

——约束；

——默认值。

c) 软件系统和其他系统之间的接口；

d) 软件驱动的报警、警告和操作者信息；

e) 信息安全需求；

注 3：示例包括：

——与敏感信息泄露有关的需求；

——身份验证；

——授权；

——审核跟踪；

——通信的完整性；

——系统信息安全/恶意软件防护。

f) 由软件实现的用户界面需求；

注 4：示例包括与以下内容有关的需求：

——对人工操作的支持；

——人机交互；

——对人员的约束；

——需要人员集中注意力的区域。

注 5：有关可用性工程需求的信息参见 IEC 62366-1[10]和其他标准(如 IEC 60601-1-6[8])。

g) 数据定义和数据库需求；

注 6：示例包括：

——表单；

——匹配；

——功能。

h) 已交付医疗器械软件在一个或多个操作和维护现场的安装和验收需求；

i) 与操作和维护方法有关的需求；

j) 与 IT-网络方面有关的需求：

注 7：示例包括以下相关内容：

——已联网的报警、警告和操作者信息；

——网络协议；

——网络服务不可用时的处置。

k) 用户维护需求；

l) 法规要求。

注 8：a)～l)中的需求可重叠。

[A、B、C 级]

注 9：所有这些需求在软件开发之初可能无法得到。

注 10：在其他标准中，ISO/IEC 25010[11]提供可能对定义软件需求有用的质量特性信息。

5.2.3 将风险控制措施纳入软件需求

制造商应将在软件中实施的风险控制措施包含在适当的医疗器械软件需求中。[B、C 级]

注：这些需求在软件开发之初可能无法得到，且可能随着软件的设计和风险控制措施的进一步确定而变化。

5.2.4 医疗器械风险分析的再评价

制造商应在建立了软件需求后对医疗器械风险分析进行再评价，并在适当时予以更新。[A、B、C 级]

5.2.5 更新需求

作为软件需求分析活动的结果，制造商应确保现有需求(包括系统需求)得到再评价，并在适当时予以更新。[A、B、C 级]

5.2.6 验证软件需求

制造商应对软件需求进行以下验证并形成文件：

a) 实现了系统需求，包括那些与风险控制有关的需求；

b) 彼此不互相矛盾；

c) 避免使用含糊不清的术语表述；

d) 以允许建立测试准则和实施测试的术语描述；

e) 可被唯一识别；

f) 可追溯至系统需求或其他来源。

[A、B、C 级]

注：本标准不要求使用正式规范的语言。

5.3 * 软件体系结构设计

5.3.1 将软件需求转换为体系结构

制造商应将对医疗器械软件的需求转换为形成文件的体系结构，该体系结构描述软件的结构并识别所有软件项。[B、C 级]

5.3.2 为软件项接口开发体系结构

制造商应为软件项与软件项的外部组件(软件和硬件)之间，以及软件项之间的接口开发一个体系结构并将其形成文件。[B、C 级]

5.3.3 规定未知来源软件项的功能和性能需求

如果软件项被识别为未知来源软件，制造商应规定未知来源软件项预期用途所必需的功能和性能需求。[B、C 级]

5.3.4 规定未知来源软件项所要求的系统硬件和软件

如果软件项被识别为未知来源软件，制造商应规定为支持未知来源软件项正常运行所必需的系统硬件和软件。[B、C 级]

注：示例包括处理器类型和速度、存储器类型和大小、系统软件类型、通信和显示软件需求。

5.3.5 确定风险控制所必需的隔离

制造商应确定风险控制所必需的软件项之间的任何隔离，并说明如何确保隔离有效。[C 级]

注：一个隔离的示例是将软件项在不同的处理器上运行。隔离的有效性可通过处理器间不共享资源来保证。当软件体系结构设计可确保有效性时，也可应用其他隔离手段(参见 B.4.3)。

5.3.6 验证软件体系结构

制造商应验证下列各项并形成文件：

a) 软件体系结构实现系统和软件需求，包括与风险控制有关的需求；

b) 软件体系结构能够支持软件项之间、软件项与硬件之间的接口；

c) 医疗器械体系结构支持任何未知来源软件项的正常运行。

[B、C 级]

注：可使用体系结构至软件需求的可追溯性分析来满足要求 a)。

5.4 * 软件详细设计

5.4.1 将软件细分为软件单元

制造商应将软件细分直至其呈现为软件单元。[B、C 级]

注：某些软件系统未进一步细分。

5.4.2 为每个软件单元开发详细设计

制造商应形成具有足够细节的设计文件，以正确实现每个软件单元。[C 级]

5.4.3 为接口开发详细设计

制造商应为软件单元与外部组件(硬件或软件)之间的任何接口,以及软件单元之间的任何接口形成具有足够细节的设计文件,以正确实现每个软件单元及其接口。[C 级]

5.4.4 验证详细设计

制造商应验证软件详细设计的下列各项并形成文件:

a) 是否实现软件体系结构;

b) 是否与软件体系结构不相矛盾。

[C 级]

注:使用体系结构至软件详细设计的可追溯分析来满足要求 a)是可接受的。

5.5 * 软件单元的实现

5.5.1 实现每个软件单元

制造商应实现每个软件单元。[A、B、C 级]

5.5.2 建立软件单元的验证过程

制造商应为验证软件单元建立策略、方法和规程。在通过测试进行验证时,应评价测试规程的充分性。[B、C 级]

注:将单元测试和软件系统测试合并到一项单一的计划和一组活动中是可接受的。

5.5.3 软件单元的验收准则

适当时,在集成为更大的软件项之前,制造商应为软件单元建立验收准则,并确保软件单元符合验收准则。[B、C 级]

注:验收准则的示例:

——软件编码是否实现了包括风险控制措施在内的需求?

——软件编码是否和软件单元的接口设计不相矛盾?

——软件编码是否符合编程规程或编码标准?

5.5.4 附加的软件单元验收准则

当下列各项在设计中出现,适当时,制造商应包括附加的验收准则:

a) 适当的事件序列;

b) 数据和控制流;

c) 所计划的资源分配;

d) 故障处理(错误界定、隔离和恢复);

e) 变量的初始化;

f) 自我诊断;

g) 存储管理和存储溢出;

h) 边界条件。

[C 级]

5.5.5 软件单元的验证

制造商应实施软件单元验证并将结果形成文件。[B、C 级]

5.6 *软件集成和集成测试

5.6.1 集成软件单元

制造商应按照集成计划(见 5.1.5)集成软件单元。[B、C 级]

5.6.2 验证软件集成

制造商应验证软件单元已经按照集成计划(见 5.1.5)集成到软件项和/或软件系统中,并保留此验证证据的记录。[B、C 级]

注:此验证仅验证已按照计划进行了集成。验证很可能通过某种形式的检查来实施。

5.6.3 软件集成测试

制造商应按照集成计划(见 5.1.5)测试集成后的软件项并将结果形成文件。[B、C 级]

5.6.4 软件集成测试的内容

对于软件集成测试,制造商应阐明集成的软件项是否按预期运行。[B、C 级]

注 1:要考虑的示例:

——所要求的软件的功能性;

——风险控制措施的实施;

——特定的时序和其他性能;

——内部和外部接口特定的功能;

——非正常条件下(包括可预见的误使用)的测试。

注 2:将集成测试和软件系统测试合并到一项单一计划和一组活动中是可接受的。

5.6.5 评价软件集成测试规程

制造商应评价集成测试规程的充分性。[B、C 级]

5.6.6 进行回归测试

在软件项集成之后,制造商应进行适当的回归测试,以证实未将风险不可接受的缺陷引入到先前集成的软件中。[B、C 级]

5.6.7 集成测试记录的内容

制造商应:

a) 将测试结果(通过/未通过和反常清单)形成文件;

b) 保留充分的记录,以使测试可重复;

c) 标明测试者的身份。

[B、C 级]

注:要求 b)可以通过保留如下内容来实现,例如:

——表明所要求操作和预期结果的测试用例规范;

——设备的记录;

——用于测试的测试环境(包括软件工具)记录。

5.6.8 使用软件问题解决过程

制造商应将软件集成和集成测试期间所发现的反常输入到软件问题解决过程。[B、C 级]

注：见第 9 章。

5.7 * 软件系统测试

5.7.1 为软件需求建立测试项

制造商应：

a) 为软件系统测试建立并实施一组测试，表达为输入触发、预期输出、通过/未通过准则和规程，并覆盖全部软件需求。[A、B、C 级]

注 1：将集成测试和软件系统测试合并为一项单一的计划和一组活动中是可接受的。在较早阶段测试软件需求也是可接受的。

注 2：不仅可对每个需求进行单独测试，也可对多个需求进行联合测试，特别是多个需求之间存在依赖关系时。

b) 评价验证策略和测试规程的充分性。

5.7.2 使用软件问题解决过程

制造商应将软件系统测试期间所发现的反常输入到软件问题解决过程。[A、B、C 级]

5.7.3 变更后再测试

当在软件系统测试期间做出变更时，制造商应：

a) 适当时，重复测试、实施经修改的测试或附加的测试，以验证纠正问题时所做变更的有效性；

b) 进行适当的测试，以证实没有引入非预期的副作用；

c) 实施 7.4 中规定的有关风险管理活动。

[A、B、C 级]

5.7.4 评价软件系统测试

制造商应评价验证策略和测试规程的适宜性。

制造商应验证：

a) 所有的软件需求均经测试或以其他方式验证；

b) 软件需求与测试或其他验证之间的可追溯性均已记录；

c) 测试结果满足所要求的通过/未通过准则。

[A、B、C 级]

5.7.5 软件系统测试记录的内容

为支持测试的可重复性，制造商应将以下内容形成文件：

a) 引用的测试用例规程，该规程体现所要求的行动和预期结果；

b) 测试结果(通过/未通过和反常清单)；

c) 被测试软件的版本；

d) 相关硬件和软件测试配置；

e) 相关测试工具；

f) 测试日期；

g) 负责执行测试和记录测试结果的人员的身份。

[A、B、C 级]

5.8 * 软件在系统级别应用的发布

5.8.1 确保软件验证的完成

制造商应确保在软件发布之前已完成所有软件验证活动且已对其结果进行评价。[A、B、C 级]

5.8.2 将已知的剩余反常形成文件

制造商应将所有已知的剩余反常形成文件。[A、B、C 级]

5.8.3 评价已知的剩余反常

制造商应确保所有已知的剩余反常均得到评价，以确保其不会促成不可接受的风险。[B、C 级]

5.8.4 将所发布的版本形成文件

制造商应将要发布的医疗器械软件版本形成文件。[A、B、C 级]

5.8.5 将所发布软件的创建过程形成文件

制造商应将用于创建所发布软件的规程和环境形成文件。[B、C 级]

5.8.6 确保活动和任务的完成

制造商应确保所有软件开发计划(或维护计划)中的活动和任务以及相关文档均完整齐全。[B、C 级]

注：见 5.1.3 b)。

5.8.7 将软件归档

制造商应将下列内容归档：

a) 医疗器械软件和配置项；

b) 文档。

存档时间至少为制造商规定的医疗器械软件寿命期或有关法规要求规定的时间中较长者。[A、B、C 级]

5.8.8 确保所发布软件的可靠交付

制造商应建立规程，以确保所发布的医疗器械软件能够可靠地交付到使用地点，而无损毁或未授权的变更。这些规程应说明包含医疗器械软件的媒介的生产和处置情况，适当时，包括：

——复制；

——媒介标记；

——包装；

——防护；

——存储；

——交付。

[A、B、C 级]

6 软件维护过程

6.1 *建立软件维护计划

制造商应为进行维护过程的活动和任务建立一项或多项软件维护计划。计划应说明以下内容：

a) 对医疗器械软件发布后发生的反馈，进行如下处理的规程：
   ——接收；
   ——形成文件；
   ——评价；
   ——解决；
   ——跟踪。
b) 确定是否将反馈视为问题的准则。
c) 使用软件风险管理过程。
d) 使用软件问题解决过程，分析和解决在医疗器械软件发布后出现的问题。
e) 使用软件配置管理过程（见第 8 章）管理对现有软件系统的修改。
f) 评价并实施未知来源软件如下事项的规程：
   ——升级；
   ——缺陷修复；
   ——打补丁；
   ——废弃。

[A、B、C 级]

6.2 *问题和修改分析

6.2.1 形成文件并评价反馈

6.2.1.1 监视反馈

制造商应监视与已发布的用于预期用途的医疗器械软件有关的反馈。[A、B、C 级]

6.2.1.2 形成文件并评价反馈

反馈应形成文件并予以评价，以确定已发布的医疗器械软件是否存在问题。任何此类问题应以问题报告的形式予以记录（见第 9 章）。问题报告应包括实际的或潜在的不良事件及对规范的偏离。[A、B、C 级]

6.2.1.3 评价问题报告对安全的影响

应对每个问题报告进行评价，以确定其对已发布的用于预期用途的医疗器械软件的安全有何影响（见 9.2），是否有必要对该软件进行变更以解决问题。[A、B、C 级]

6.2.2 使用软件问题解决过程

制造商应使用软件问题解决过程（见第 9 章）处理问题报告。[A、B、C 级]

注：某个问题可能表明某软件系统或软件项尚未被赋予正确的软件安全级别。该问题的解决过程可能引起软件安全级别的变更。当该过程完成时，软件系统或其软件项安全级别的任何变更，宜予以公布并形成文件。

6.2.3 分析变更请求

除第9章所要求的分析之外，制造商还应就每个变更请求对组织、对已发布的用于预期用途的医疗器械软件及对与其有接口的系统的影响进行分析。[A、B、C级]

6.2.4 批准变更请求

制造商应评价并批准修改已发布医疗器械软件的变更请求。[A、B、C级]

6.2.5 与用户和监管机构沟通

制造商应识别经批准的影响已发布医疗器械软件的变更请求。

按照当地法规要求，制造商应告知用户和监管机构如下信息：

a) 已发布医疗器械软件中的任何问题和不变更继续使用的后果；

b) 已发布医疗器械软件任何可获得的变更的性质，以及如何获得并安装这些变更。

[A、B、C级]

6.3 *修改的实施

6.3.1 使用已建立的过程实施修改

制造商应识别并实施因修改而需要重复的第5章的任何活动。

[A、B、C级]

注：有关软件变更的风险管理要求见7.4。

6.3.2 修改后软件系统的再发布

制造商应按照5.8的要求发布修改。[A、B、C级]

注：修改可以作为软件系统完整再发布的一部分发布，或作为对现有软件系统的修改以修改包形式发布，该修改包包含经变更的软件项及用于安装这些变更所需的工具。

7 *软件风险管理过程

7.1 *促成危险情况的软件分析

7.1.1 识别可能促成危险情况的软件项

制造商应识别可能促成危险情况的软件项，危险情况在YY/T 0316的医疗器械风险分析活动(见4.2)中已识别。[B、C级]

注：危险情况可能是软件失效的直接结果，或在软件中实施的风险控制措施失效的结果。

7.1.2 识别促成危险情况的潜在原因

制造商应识别上文所识别软件项促成危险情况的潜在原因。

适当时，制造商应考虑的潜在原因包括：

a) 不正确的或不完整的功能性规范；

b) 所识别的软件项功能性方面的软件缺陷；

c) 来自未知来源软件的失效或非预期结果；

d) 可能导致不可预知的软件运行的硬件失效或其他软件缺陷；

e) 可合理预见的误使用。

[B、C 级]

7.1.3 评价已公开的未知来源软件反常清单

如果源于未知来源软件的失效或非预期结果是软件项促成危险情况的潜在原因，制造商至少应评价由供应商公开的、与在医疗器械中使用版本的未知来源软件项有关的任何反常清单，以确定是否有任何已知的反常导致了可能促成危险情况的事件序列。[B、C 级]

7.1.4 将潜在原因形成文件

制造商应在风险管理文档中将软件项促成危险情况的潜在原因形成文件(见 YY/T 0316)。
[B、C 级]

7.2 风险控制措施

7.2.1 确定风险控制措施

对在风险管理文档中形成文件的软件项可能促成危险情况的每一种情况，制造商应按照 YY/T 0316规定风险控制措施并形成文件。[B、C 级]

注：风险控制措施可以在硬件、软件、工作环境或用户说明书中实施。

7.2.2 在软件中实施的风险控制措施

如果风险控制措施作为软件项功能的一部分来实施，制造商应：

a) 在软件需求中包括风险控制措施；

b) 基于风险控制措施所控制的风险[见 4.3 a)]，为有助于风险控制措施实施的每个软件项赋予软件安全级别；

c) 按照第 5 章开发软件项。

[B、C 级]

注：本要求为 YY/T 0316 的风险控制要求提供附加的详细资料。

7.3 风险控制措施的验证

7.3.1 验证风险控制措施

应对在 7.2 中形成文件的每个风险控制措施的实施进行验证并形成文件。制造商应评审风险控制措施，并确定其是否可能导致新的危险情况。[B、C 级]

7.3.2 将可追溯性形成文件

制造商应将软件危险(源)的可追溯性形成文件，适当时包括：

a) 从危险情况到软件项；

b) 从软件项到特定的软件原因；

c) 从软件原因到风险控制措施；

d) 从风险控制措施到风险控制措施的验证。

[B、C 级]

注：见 YY/T 0316 风险管理报告。

7.4 软件变更的风险管理

7.4.1 分析与医疗器械软件安全相关的变更

制造商应分析对医疗器械软件(包括未知来源软件)的变更以确定是否：

a) 引入了促成危险情况另外的潜在原因；

b) 需要附加的软件风险控制措施。

[A、B、C 级]

7.4.2 分析软件变更对现有风险控制措施的影响

制造商应分析对软件的变更，包括对未知来源软件的变更，以确定软件修改是否可能干扰现有的风险控制措施。[B、C 级]

7.4.3 基于分析实施风险管理活动

制造商应在这些分析的基础上实施 7.1、7.2 和 7.3 中所确定的相关风险管理活动。[B、C 级]

8 * 软件配置管理过程

8.1 * 配置标识

8.1.1 建立标识配置项的方法

制造商应根据 5.1 规定的开发和配置策划为拟受控的配置项及其版本的唯一性标识建立一个方案。[A、B、C 级]

8.1.2 标识未知来源软件

对于拟使用的每个未知来源软件配置项，包括标准库，制造商应将以下各项形成文件：

a) 标题；

b) 制造商；

c) 未知来源软件的唯一标识符。

[A、B、C 级]

注：未知来源软件的唯一标识符可以是，例如版本、发布日期、补丁编号或升级名称。

8.1.3 标识系统配置文档

制造商应将组成软件系统配置的一组配置项及其版本形成文件。[A、B、C 级]

8.2 * 变更控制

8.2.1 批准变更请求

制造商应仅在对经批准的变更请求作出响应时才对按照 8.1 标识的需受控的配置项进行变更。[A、B、C 级]

注 1：批准变更请求的决定可以整合到变更控制过程或作为其他过程的一部分。本条仅要求变更的批准先于其实施。

注 2：可在生存周期不同阶段的各验收过程提出变更请求，如计划所述，见 5.1.1 d)和 6.1 e)。

8.2.2 实施变更

制造商应按变更请求中的规定实施变更。制造商应识别并实施因变更而需要重复的任何活动，包括对软件系统和软件项的软件安全级别的变更。[A、B、C 级]

注：本条说明了宜如何实施变更以达到充分的变更控制。这并不意味着实施是变更控制过程的组成部分。实施宜使用所策划的过程，见 5.1.1 d)和 6.1 e)。

8.2.3 验证变更

制造商应验证变更，包括重复因变更而失效的任何验证，并考虑 5.7.3 和 9.7。[A、B、C 级]

注：本条只要求变更经过验证。这并不意味着验证是变更控制过程的组成部分。验证宜使用所策划的过程，见 5.1.1 d)和 6.1 e)。

8.2.4 为变更的可追溯性规定方法

制造商应保持以下各项之间关系和依赖性的记录：

a) 变更请求；

b) 有关的问题报告；

c) 变更请求的批准。

[A、B、C 级]

8.3 * 配置状态报告

制造商应保留包括系统配置在内的受控配置项历史的可检索记录。[A、B、C 级]

9 * 软件问题解决过程

9.1 编写问题报告

制造商应为医疗器械软件中发现的每个问题编写问题报告。问题报告应包括严重程度的说明(例如，对性能、安全或信息安全的影响)以及可能有助于解决问题的其他信息(例如，受影响的器械和受影响的支持性附件)。[A、B、C 级]

注：问题可在软件发布之前或之后、在制造商的组织内部或外部发现。

9.2 调查问题

制造商应：

a) 调查问题并在可能时识别问题的原因；

b) 利用软件风险管理过程评价问题与安全的相关性(见第 7 章)；

c) 将调查和评价的结果形成文件；

d) 为纠正问题所需的措施创建一个或多个变更请求，或将不采取措施的理由形成文件。

[A、B、C 级]

注：如果问题与安全无关，制造商不必为符合软件问题解决过程而对问题进行纠正。

9.3 通知相关方

适当时，制造商应将存在的问题通知相关方。[A、B、C 级]

注：问题可在发布之前或之后，在制造商的组织内部或外部发现。制造商根据此情况确定相关方。

9.4 使用变更控制过程

制造商应按照变更控制过程的要求(见 8.2)批准并实施所有变更请求。[A、B、C 级]

9.5 保持记录

制造商应保持问题报告及其解决情况的记录，包括对其验证的记录。

适当时，制造商应更新风险管理文档。[A、B、C 级]

9.6 分析问题的趋势

制造商应对问题报告进行分析以从中发现问题的趋势。[A、B、C 级]

9.7 验证软件问题的解决

制造商应验证问题的解决以确定是否：

a) 问题已得到解决，问题报告已关闭；

b) 不良趋势已得到扭转；

c) 变更请求已在适当的医疗器械软件和活动中实施；

d) 引入了其他问题。

[A、B、C 级]

9.8 测试文档的内容

当在一项变更之后测试、再测试或回归测试软件项和系统时，制造商应在测试文档中包括：

a) 测试结果；

b) 发现的反常；

c) 所测试软件的版本；

d) 相关硬件和软件的测试配置；

e) 相关的测试工具；

f) 测试日期；

g) 测试者的身份。

[A、B、C 级]

附 录 A
（资料性附录）
本标准要求的理由说明

A.1 理由说明

本标准的基本要求是在医疗器械软件的开发和维护过程中遵循一组过程，且过程的选择与对患者和其他人员的风险相适应。这源于确信软件测试不足以确定其在运行中是安全的。

本标准要求的过程分为两类：

——为确定软件中每一软件项运行产生的风险所要求的过程；

——基于已确定的风险选定的，为使每一个软件项达到适当低的软件失效概率所要求的过程。

本标准要求对所有的医疗器械软件实施第一类过程，而第二类过程仅对选定的软件项实施。

因此，声称符合本标准宜包括一项形成文件的风险分析，该风险分析识别包含软件且可能导致危险情况的可预见的事件序列（见 YY/T 0316）。可由软件间接引起的危险情况（例如，通过提供可能导致给予不适当治疗的误导性信息）宜包括在此风险分析中。

作为第一类过程的组成部分所要求的所有活动在标准正文中标注为“[A、B、C 级]”，表明对这些活动均有要求且与其适用的软件分级无关。

基于下列理由，这些活动是对 A、B、C 所有级别的要求：

——活动产生有关风险管理或软件安全分级的计划；

——活动产生一个输出，此输出是风险管理或软件安全分级的输入；

——活动是风险管理或软件安全分级的一部分；

——活动建立一个管理系统，即文档或记录保持系统，以支持风险管理或软件安全分级；

——活动通常发生在相关软件的分级未知时；

——活动可能引起变更，从而可能使相关软件的现有软件安全分级失效。这包括发布后安全有关问题的发现和分析。

另一类过程只是对软件安全级别为 B 或 C 的软件系统或软件项的要求。作为这些过程的组成部分所要求的活动，在标准正文中标注为“[B、C 级]”或“[C 级]”，表明这些活动是基于其适用的软件分级的选择性要求。

基于下列理由，相关活动是对 B 级和 C 级软件的选择性要求：

——活动通过在设计、测试或其他验证时要求更详细或更严格提高软件可靠性；

——活动是一项支持 B 级或 C 级所要求的另一项活动的管理活动；

——活动支持安全相关问题的纠正；

——活动生成安全相关软件设计、实施、验证和发布的记录。

基于下列理由，相关活动是对 C 级软件的选择性要求：

——活动通过在设计、测试或其他验证时要求更详细、更严格或关注特定问题进一步提高软件可靠性。

注意本标准中定义的所有过程和活动，在保证高质量软件的开发和维护中被认为是有价值的。作为对 A 级软件的要求，对许多这些过程和活动的省略并不意味着这些过程和活动是无价值的或不推荐的。省略的意图是要承认不可能引起危险（源）的软件的安全和有效性可主要通过在医疗器械设计期间的全部确认活动（本标准范围以外），及通过一些简单的软件生存周期控制活动得到保证。

A.2 按级别的要求汇总

表 A.1 总结了将每个要求赋予哪个软件安全级别。本表是资料性的，仅为方便而提供。标准的正文部分为每项要求识别了相应的软件安全级别。

表 A.1 按软件安全级别的要求汇总

章条号		A 级	B 级	C 级
第 4 章	全部要求	×	×	×
5.1	5.1.1、5.1.2、5.1.3、5.1.6、5.1.7、5.1.8、5.1.9	×	×	×
	5.1.5、5.1.10、5.1.11 、5.1.12		×	×
	5.1.4			×
5.2	5.2.1、5.2.2、5.2.4、5.2.5、5.2.6	×	×	×
	5.2.3		×	×
5.3	5.3.1、5.3.2、5.3.3、5.3.4、5.3.6		×	×
	5.3.5			×
5.4	5.4.1		×	×
	5.4.2、5.4.3、5.4.4			×
5.5	5.5.1	×	×	×
	5.5.2、5.5.3、5.5.5		×	×
	5.5.4			×
5.6	全部要求		×	×
5.7	全部要求	×	×	×
5.8	5.8.1、5.8.2、5.8.4、5.8.7、5.8.8	×	×	×
	5.8.3、5.8.5、5.8.6		×	×
第 6 章	全部要求	×	×	×
7.1	全部要求		×	×
7.2	全部要求		×	×
7.3	全部要求		×	×
7.4	7.4.1	×	×	×
	7.4.2、7.4.3		×	×
第 8 章	全部要求	×	×	×
第 9 章	全部要求	×	×	×

附 录 B
（资料性附录）
关于本标准条款的指南

B.1 范围

B.1.1 目的

本标准的目的是提供一个持续产出高质量、安全的医疗器械软件的开发过程。为达到此目的，本标准识别需要完成的最低限度的活动和任务，以提供以下信任：软件是以可能产出高度可靠和安全的医疗器械软件的方式开发的。

本附录为本标准要求的应用提供指南。其不增加或改变本标准的要求。本附录可帮助更好的理解本标准的要求。

注意在本标准中的活动是过程中引出的条款，而任务是在活动中定义的。例如，为软件开发过程定义的活动包括：软件开发策划、软件需求分析、软件体系结构设计、软件详细设计、软件单元的实现、软件集成和集成测试、软件系统测试和软件发布。这些活动中的任务都是单独的要求。

本标准不要求一个特定的软件开发生存周期模型。然而，符合本标准确实意味着过程之间的依赖性，因为一个过程的输入产生于另一个过程。例如，软件系统的软件安全分级，宜在风险分析过程已确定了软件系统失效可能引起何种伤害之后完成。

因为过程之间这种逻辑依赖性，在本标准中以一个序列，意指“瀑布”或“单程”生存周期模型，描述本标准中的过程是最容易的。然而也可以使用其他模型。如 ISO/IEC 12207[12] 中所定义的一些开发（模型）策略（参见表 B.1），包括：

——瀑布：“单程”策略，也称为“瀑布”，由一次性实施的开发过程组成。简而言之，确定顾客需求、定义需求、系统设计、系统实施、测试、修复和交付。

——增量式开发模型：“增量式开发模型”策略首先确定顾客需求并定义系统需求，然后在一个软件构建序列中进行其余的开发。第一个构建包含策划能力的一部分，下一个构建增加更多能力，如此这般，直到系统完整为止。

——渐进：“渐进”策略也在构建中开发系统，但是与增量式开发模型策略不同的是其承认不充分理解用户需求，事先不能定义所有需求。在这个策略中，事先定义部分顾客需求和系统需求，然后将其在每个后续的构建中细化。

表 B.1 ISO/IEC 12207 中规定的开发（模型）策略

开发策略	首先定义全部需求？	多重的开发周期？	提供中间版本软件？
瀑布 （单程）	是	否	否
增量式开发模型 （预先策划的产品改进）	是	是	不确定
渐进	否	是	是

无论选择哪一种生存周期，都有必要保持诸如规范、设计文件和软件等过程输出之间的逻辑依赖性。瀑布型生存周期模型通过延迟过程的开始时间，直至该过程的多个输入都完整并经批准之后来达

到此目的。

其他生存周期，尤其是渐进生存周期，允许在过程的所有输入都可获得之前产生过程输出。例如，一个新的软件项可能在整个软件体系结构最终确定之前被规定、分级、实现和验证。此类生存周期带有风险：对一个过程输出的变更或开发将使另一个过程输出无效。因此，所有的生存周期都使用一个综合的配置管理系统来确保所有的过程输出达到一致的状态，并保持依赖性。

不管使用何种软件开发生存周期，下列各项原则都是重要的：

——所有的过程输出宜保持一致的状态；无论何时，只要任一过程输出被创建或变更，宜迅速更新所有相关过程的输出以保持它们彼此的一致性，并保持本标准明示或隐含要求的所有依赖性；

——当需要作为对软件进一步工作的输入时，所有的过程输出宜是可获得的；

——在发布任何医疗器械软件之前，所有的过程输出宜是相互一致的，并且宜遵守本标准明示或隐含要求的过程输出之间的所有依赖性。

B.1.2 应用领域

本标准适用于医疗器械软件的开发和维护，以及包含未知来源软件的医疗器械的开发和维护。

使用本标准要求制造商实施符合 YY/T 0316 的医疗器械风险管理过程。因此，当医疗器械体系结构包含一个新获得的组件（这可以是购买的组件或未知来源的组件）时，诸如包含未知来源软件的打印机/绘图机，制造商要对所获得的组件负责，应将其包括在医疗器械的风险管理中。这里假定通过医疗器械风险管理的适当实施，制造商会理解该组件并认识到其包括未知来源软件。使用本标准的制造商将启动软件风险管理过程，作为整个医疗器械风险管理过程的一部分。

发布后医疗器械软件的维护涉及医疗器械软件的生产后经验。软件维护包括联合所有技术和管理手段，包括监督措施，对问题报告采取措施以将医疗器械软件保持在或恢复到可实现所要求功能的状态，并处理与已发布医疗器械软件有关的修改请求。例如，这包括问题纠正、向监管机构报告、再确认和预防措施，参见 GB/T 20157[3]。

B.2 规范性引用文件

ISO/IEC 90003[17]为将质量管理体系应用于软件开发提供指南。本标准不要求但强烈推荐使用该指南。

B.3 术语和定义

可能时，用国家标准、行业标准或国际标准中的定义规定了术语。

本标准选用三个术语描述软件系统（顶层）的分解。软件系统可以是医疗器械的子系统（参见 IEC 60601-1-4[7]）或医疗器械本身，后者即为独立软件。不再为了测试或软件配置管理的目的而进一步分解的最底层是软件单元。该结构的所有层级，包括顶层和底层，可称为软件项。这样，一个软件系统由一个或多个软件项组成，每个软件项由一个或多个软件单元或可分解的软件项组成。提供软件项和软件单元的粒度是制造商的责任。使这些术语模糊化，可使用户将其应用于许多不同的开发方法和医疗器械中采用的不同软件类型。

B.4 通用要求

没有已知的方法可保证任何种类软件 100％的安全。

提高医疗器械软件安全的三个主要原则：

——风险管理；

——质量管理；

——软件工程。

为开发和维护安全的医疗器械软件，有必要建立风险管理过程并将其作为质量管理体系的组成部分，而后者则作为应用适当软件工程方法和技术的总体框架。这三个概念的结合允许医疗器械制造商遵循一个结构清晰并持续可重复的决策过程，以提高医疗器械软件的安全。

B.4.1 质量管理体系

一组严谨且有效的软件过程包括诸如管理、基础设施、改进和培训等组织过程。为避免重复并将重点集中在软件工程上，本标准省略了这些过程。这些过程由质量管理体系所覆盖。YY/T 0287[5]是一个预期专门将质量管理概念应用于医疗器械的行业标准。符合 YY/T 0287 质量管理体系要求并不自动构成对国家或地区法规要求的符合性。识别并建立与相关法规要求的符合性是制造商的责任。

B.4.2 风险管理

软件开发人员充分参与风险管理活动，以确保所有可合理预见的医疗器械软件相关风险得到考虑。

本软件工程标准并不试图规定一个适当的风险管理过程，而是要求制造商应用一个符合 YY/T 0316的风险管理过程。YY/T 0316 是医疗器械风险管理的专用标准。涉及软件作为促成因素的危险情况引发的特定软件风险管理活动在第 7 章描述的支持过程中予以识别。

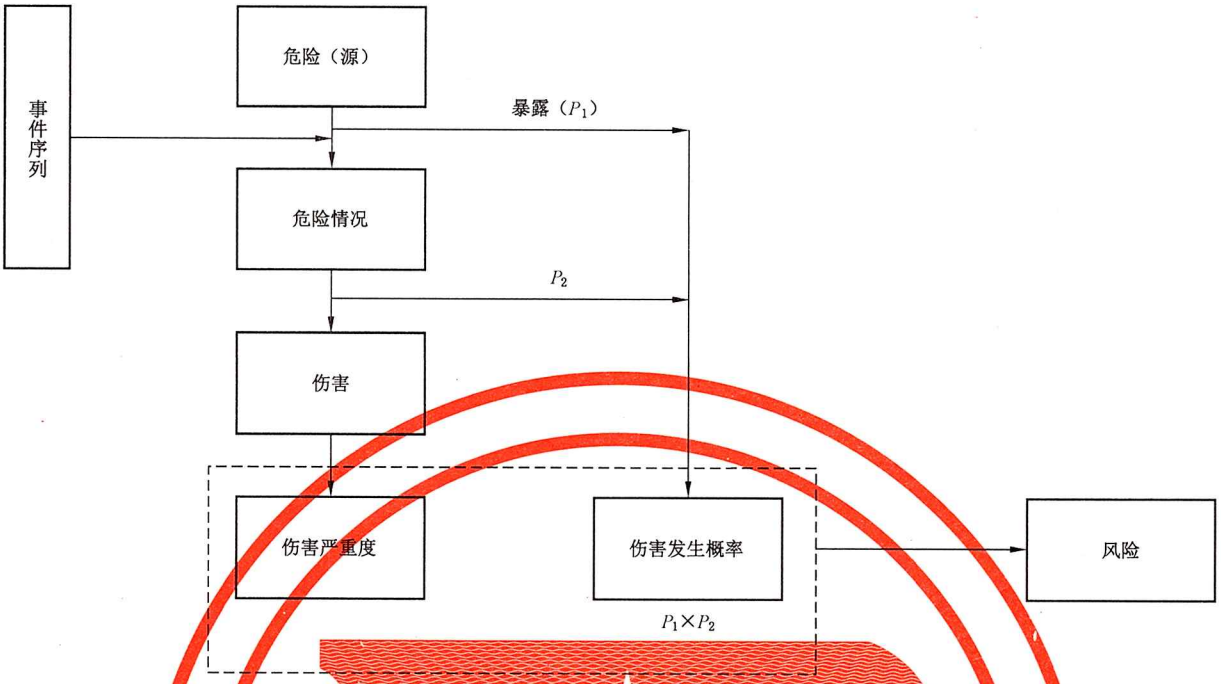
B.4.3 软件安全分级

当软件作为医疗器械的一部分，作为医疗器械的一个附件，或作为医疗器械本身时，与之有关的风险被用作软件安全分级方案的输入，从而确定在软件开发和维护期间所使用的过程。

风险是伤害的严重度及其发生概率的组合。然而，对于定量估计软件失效发生概率的方法不存在共识。当软件在导致危险情况的一个事件序列或事件组合中出现时，估计危险情况的风险不能考虑软件失效发生的概率。在这种情况下，考虑最坏情况的概率是适当的，且软件失效发生的概率宜设定为 1。当有可能估计事件序列中其余事件的概率时（若其不是软件），则该概率可用作危险情况发生的概率（图 B.1 中的 P_1）。

然而，在许多情况下，可能无法估计事件序列中其余事件的概率，宜仅根据伤害的性质来评估风险（危险情况发生的概率宜设定为 1）。在这些情况下，风险估计宜关注危险情况所造成伤害的严重度。还可以根据临床知识对概率进行主观排序，以区分临床医生可能发现的失效与不会被发现且更可能造成伤害的失效。

对危险情况导致伤害的概率的估计（图 B.1 中的 P_2），通常需要临床知识来区分临床实践可能预防伤害的危险情况与更有可能造成伤害的危险情况。



说明：

P_1——危险情况发生的概率；

P_2——危险情况导致伤害的概率。

图 B.1　危险（源）、事件序列、危险情况和伤害关系的图示（源于 YY/T 0316—2016 的附录 E）

如果将软件系统分解成软件项，那么每个软件项可以有自己的软件安全级别。

仅在下列情况下，确定与软件项失效有关的风险才是可能的：

——系统的体系结构和软件的体系结构根据软件项的用途和其与其他软件项和硬件项的接口定义软件项的作用；

——对系统的变更是受控的；

——在完成对体系结构和规定的风险控制措施的风险分析之后。

本标准要求以最少量的活动使所有级别的软件达到以上条件。

当全组的软件项已被定义，且风险管理活动已确定了软件项如何与安全有关时，软件体系结构活动的终点即为开发的起点。因此这是根据软件项在安全方面的作用可对其进行准确分级的起点。

该点对应于 YY/T 0316 中风险控制的开始点。

在该点之前，风险管理过程确定体系结构的风险控制措施，如增加保护性子系统，或降低软件失效引起伤害的概率。在该点之后，风险管理过程使用旨在降低软件项失效概率的过程。换句话说，软件项的分级规定了适用于该软件项基于过程的风险控制措施。

预期制造商会发现在这一点之前对软件分级是有用的，例如，将关注点集中在所研究的领域，但这样的分级宜视为初步的分级，不宜用于说明过程省略的合理性。

软件安全分级方案不期望与 YY/T 0316 的风险分级相一致。YY/T 0316 方案根据风险的严重度和可能性对其进行分级，而软件安全分级方案依据在软件系统和软件项开发和维护时应用的过程对其分级。

随着设计的进展，新的风险可能变得明显。因此，风险管理宜作为开发过程的组成部分予以应用。这使得体系结构设计成为可能，该设计确定全组的软件项，包括那些需要正确起作用以确保安全运行的软件项和防止故障引起伤害的软件项。

软件体系结构宜促进安全运行所要求的软件项的隔离，并宜描述用以确保这些软件项有效隔离的方法。隔离不限于物理分离(处理器或内存分区)，而且包括防止一个软件项对另一个软件项产生负面影响的任何机制。基于所涉及的风险和隔离的理由说明确定隔离的充分性并形成文件。

如 B.3 所述，本标准选用三个术语描述软件系统(顶层)的分解。

图 B.2 以图形说明在软件系统内对软件项的可能划分，以及在分解中软件安全级别如何应用于成组的软件项。

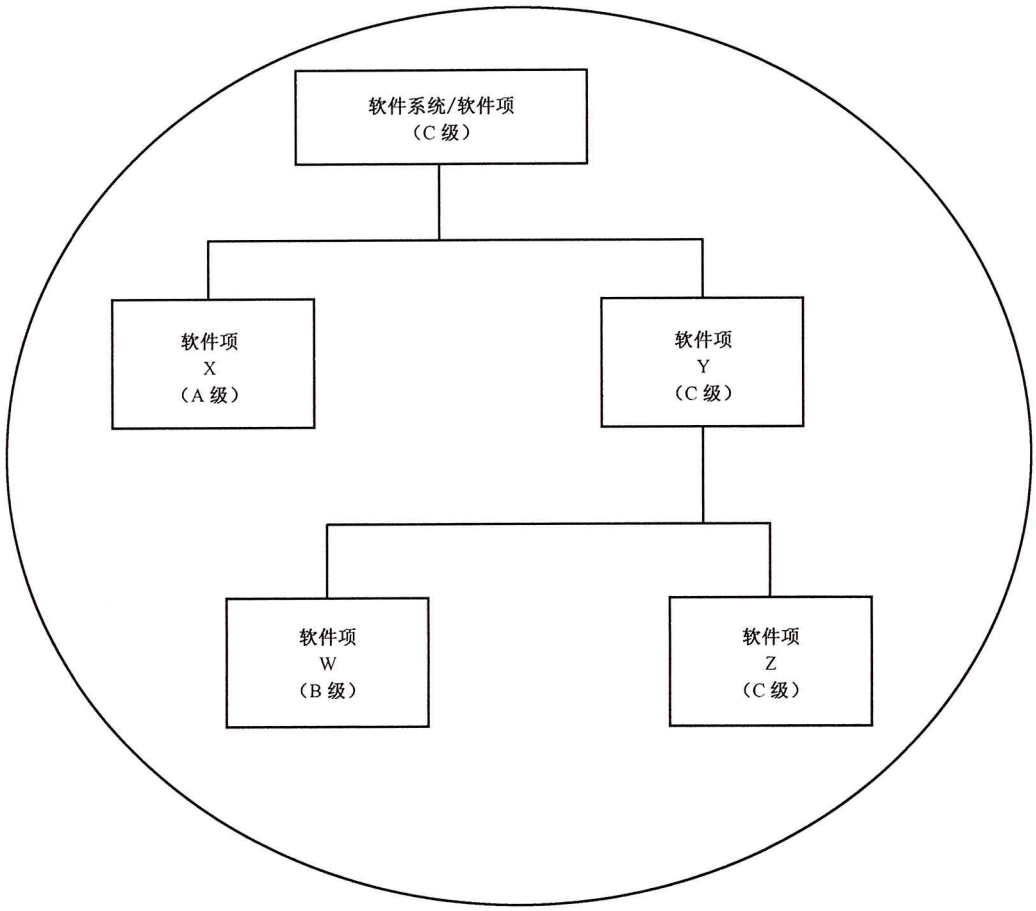


图 B.2　软件项划分示例

对本示例，由于正在开发的医疗器械软件的类型，制造商知道软件系统初步的软件安全级别是软件安全 C 级。在软件体系结构设计期间制造商已决定用三个软件项——X、W 和 Z 划分系统，如 B.2 所示。制造商能够将促成可导致死亡或严重损伤的危险情况的所有软件系统隔离到软件项 Z，并将剩余的促成可导致不严重损伤的危险情况的软件系统隔离到软件项 W。软件项 W 分级为软件安全 B 级，软件项 Z 分级为软件安全 C 级。因此，按 4.3 c)软件项 Y 应分级为 C 级。按此要求，软件系统也是软件安全 C 级。软件项 X 已分级为软件安全 A 级。这样制造商能够将软件项 X 和 Y 之间，以及软件项 W 和 Z 之间隔离的理由说明形成文件，以确保隔离的完整性。如果不可能隔离软件项 X 和 Y，则软件项 X 应分级为软件安全 C 级。

B.4.4　遗留软件

4.4 建立了将本标准应用于遗留软件的过程。某些国家和地区可能要求制造商证明符合本标准，以获得医疗器械软件的监管许可，即使该软件是在本标准当前版本实施之前设计的(遗留软件)。在这

种情况下，4.4 中的要求为制造商证明遗留软件符合本标准提供了一种方法。

制造商也许认为，作为孤立活动进行的、一个已完成的开发生存周期的回顾性文档的编制不会导致与产品使用有关风险的降低。但该过程使得本标准定义的部分活动得以确定，而这确实可使风险降低。该过程中隐含的一些附加的目标是：

——所需的活动和产生的文档宜依托并尽可能利用现有文档；

——制造商宜尽可能有效地利用资源，以达到降低风险的效果。

除了产生用来识别需要执行的部分活动的计划之外，该过程还会产生支持继续安全地使用遗留软件的客观证据，及对此结论简要的理由说明。与计划继续使用遗留软件相关的风险取决于在何种环境下用遗留软件创建软件系统。制造商要将所有已识别的与遗留软件相关的医疗器械危险（源）形成文件。

4.4 要求对遗留软件在生产和使用期间获得的、可用的生产后现场数据进行全面评定。生产后数据的典型来源包括：

——由器械导致的不良事件；

——从器械的用户收到的反馈；

——制造商发现的反常。

虽然对前瞻性地定量估计软件失效发生概率的方法尚无共识，对遗留软件来说，基于其使用和生产后数据的评价相关信息可能是可获得的。如果在这种情况下有可能定量地估计序列中事件的概率，则可以使用一个定量值来表示整个事件序列发生的概率。如果不可能进行这样的定量估计，则考虑最坏情况的概率是适当的，并且软件失效发生的概率宜设定为 1。

制造商关于在整个医疗器械系统体系结构中如何使用遗留软件的决定是风险评定的输入。要考虑的风险因具体情况而异：

——当遗留软件一直安全可靠地使用且制造商希望继续使用该遗留软件时，继续使用的理由主要基于对生产后记录所做的风险评定。

——当创建新的软件系统复用遗留软件时，该遗留软件的预期用途可能与其原始预期用途不同。在这种情况下，风险评定应考虑到由于遗留软件失效而可能出现改变了的一组危险情况。

——复用的遗留软件可用于类似的预期用途，也可集成到新的软件系统中。在这种情况下，风险评定宜考虑根据 5.3 修改体系结构风险控制措施。

当要对遗留软件进行变更并在新的软件系统中使用时，制造商宜考虑现有安全和可靠运行的记录可能因变更而失效的情况。

对遗留软件的变更宜根据第 4～9 章进行，包括根据 7.4 评定对风险控制措施的影响。对于遗留软件，现有的风险控制措施可能没有完全形成文件，宜特别关注利用可获得的形成文件的设计记录以及具有系统知识的专业人士，以评价变更的潜在影响。

根据 4.4，制造商进行差距分析以确定可用的文档，包括在遗留软件开发期间完成的已执行任务的客观证据以及与 5.2、5.3、5.7 和第 7 章进行比较的客观证据。完成此差距分析的典型步骤包括：

a) 标识遗留软件，包括清晰标识所需的版本、修订以及任何其他方法；

b) 对照 5.2、5.3、5.7 和第 7 章对交付物的要求评价现有交付物；

c) 评价可获得的客观证据，将以前使用的软件开发生存周期模型形成文件（适当时）；

d) 评价现有风险管理文档的充分性，并考虑 YY/T 0316。

考虑完成的差距分析，制造商要评价由于生成缺失的交付物和相关活动而导致的潜在风险的降低，并创建执行活动和生成交付物的计划以关闭这些差距。

降低风险宜权衡依照第 5 章应用软件开发过程的受益和在不完全了解其开发历史的情况下修改遗留软件可能引入增大风险的新缺陷的可能性。第 5 章的某些要素在事后完成时可能会被评定为几乎没有降低风险。例如，详细设计和单元验证主要在开发新软件或重构现有软件的过程中降低风险。如果

没有策划这些目标，孤立地执行这些活动虽然可创建文档，但不会导致风险降低。

差距关闭计划至少要处理软件系统测试记录的缺失。如果这些记录不存在或不适于支持继续使用遗留软件的理由，则差距关闭计划宜包括根据5.2在功能级创建软件系统需求并根据5.7对其进行测试的内容。

继续使用遗留软件的理由是建立在可获得的客观证据和分析的基础上的，并宜形成文件。而后者是在评定风险的过程和创建适于遗留软件复用环境的差距关闭计划的过程中获得的。

考虑到遗留软件可获得的生产后记录和受填补过程差距所影响的风险控制措施，该理由说明为遗留软件在所策划的复用环境中安全可靠运行提供了正面的实例。

在根据4.4复用遗留软件后，交付物中留有差距的遗留软件的那些部分仍然是遗留软件，可根据4.4考虑再次进一步复用。当通过变更遗留软件关闭交付物中的差距时，变更宜根据第4～9章实施。

B.4.5 法规视角——现成软件与未知来源软件、遗留软件之间的关系

各个国家和地区的医疗器械监管机构对于现成软件的定义、类型和监管要求存在差异。

在中国医疗器械软件监管法规视角下，现成软件是指生产企业未进行完整生存周期控制的软件，包括“遗留软件”“成品软件”和“外包软件”。其中，“遗留软件”是指生产企业以前开发但现在不能得到足够开发记录的软件，包括医疗器械软件和非医疗器械软件；“成品软件”是指已开发且通常可得到的，但生产企业未进行完整生存周期控制的软件，即采购的或免费获得的第三方软件，包括医疗器械软件和非医疗器械软件；“外包软件”是指生产企业委托第三方开发的软件，通常为医疗器械软件。

本标准所定义的未知来源软件主要是非医疗器械软件，成品软件作为未知来源软件的子集不含医疗器械软件，故为法规视角“成品软件”的子集。本标准所定义的遗留软件是指在售的但不满足本标准要求的医疗器械软件，不含未上市的和已退市的医疗器械软件，也不含非医疗器械软件，故为法规视角“遗留软件”的子集。因此，本标准所定义的未知来源软件和遗留软件的合集仅是法规视角现成软件的子集。

在法规视角下，现成软件与未知来源软件、遗留软件之间的关系如图B.3所示。

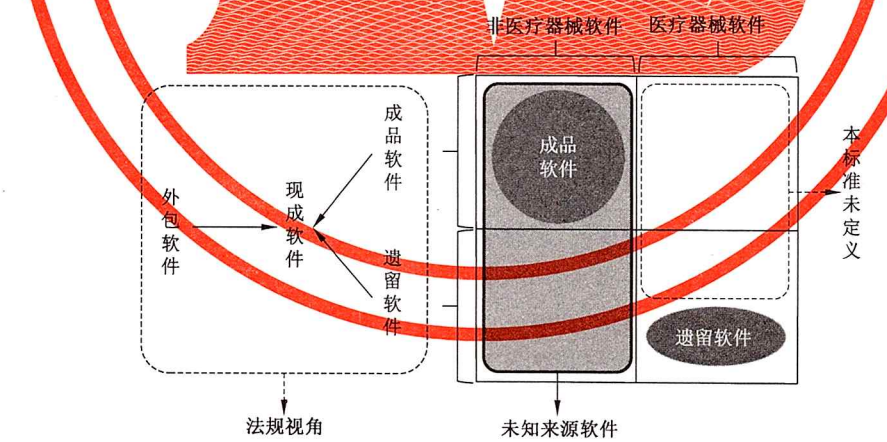


图 B.3 法规视角——现成软件与未知来源软件、遗留软件之间的关系

B.5 软件开发过程

B.5.1 软件开发策划

此项活动的目的是对软件开发任务进行策划以降低软件引起的风险，与开发组成员沟通规程和目标，并确保满足医疗器械软件的系统质量要求。

软件开发策划活动可以在一个单一或多项计划中将任务形成文件。有些制造商可能已建立适用于其所有医疗器械软件开发的方针和规程。在这种情况下，计划可简单地引用现有方针和规程。有些制造商可能为每个医疗器械软件的开发准备一个或一组专门的计划，详细清楚地说明特定的活动并引用通用规程。另一种可能性是为每个医疗器械软件的开发量身定制一个或一组计划。策划宜在开发过程所必需的详细程度上做出说明，并宜与风险水平相适应。例如，较高风险的系统或项目宜遵循较严格的开发过程，并宜对任务做更详细地说明。

策划是迭代性的活动，宜随开发的进展予以再检查和更新。当对系统及开发系统所需投入程度的理解得更多时，计划可以逐步完善以包含更多更适宜的信息。例如，作为执行风险管理过程和开发软件体系结构的结果，系统的初始软件安全级别可能改变。或者，可能决定将某未知来源软件包含到系统中。更新计划以反映当前对系统的认知与对系统或系统中项目所需严格程度的认知是很重要的，以便能对开发过程进行适当控制。

B.5.2 软件需求分析

此项活动要求制造商为医疗器械软件建立并验证软件需求。建立可验证的需求对于确定要构建什么，确定医疗器械软件要展现出的可接受的特性，证实完成的医疗器械软件完备可用是十分必要的。为证实需求已如设想的那样实施，每个需求宜以这种方式表述：即能建立客观准则以确定其是否已得到正确实施。如果器械的风险管理过程将需求置于软件以控制所识别的风险，这些需求在软件需求中宜以这种方式标识：使得追溯风险控制措施到软件需求成为可能。所有的软件需求宜以这种方式标识：使得证实需求与软件系统测试之间的可追溯性成为可能。如果一些国家的法规许可要求符合特定的法规或国际标准，此符合性要求宜在软件需求中形成文件。因为软件需求确立在软件中要实现什么，在完成需求分析活动之前，要求对该需求进行一次评价。

顾客需求、设计输入、软件需求、软件功能规范和软件设计规范之间的差别是一个经常混淆的领域。设计输入是把顾客需求诠释为正式形成文件的医疗器械需求。软件需求是软件如何满足顾客需求和设计输入的正式形成文件的规范。软件功能规范通常包括在软件需求中，并详细定义软件如何满足其需求，尽管许多不同的替代方案也可满足需求。软件设计规范定义如何对软件进行设计和分解，以实现其需求和功能规范。

按照惯例，已将软件需求、功能规范和设计规范编写成成套的一个或多个文件。现在可将此资料视为通用数据库中的数据项。每个数据项可有一个或多个属性，详细说明其目的和与数据库中其他项的联系。该方法允许显示和打印最适合每组预期用户（例如：营销人员、制造商、测试者和审核者）的信息的不同视域，并支持可追溯性以证实需求的充分实现以及测试用例对需求的测试程度。支持此方法的工具可以像利用超文本链接的超文本文件（HTML）一样简单，或者像计算机辅助软件工程（CASE）工具和需求分析工具一样复杂和有能力。

系统需求过程超出本标准的范围。然而，用软件实现医疗器械功能性的决定通常在系统设计期间做出，将一些或所有系统需求分配到软件中实现。软件需求分析活动由两部分组成，分析系统需求过程分配给软件的需求，和由所分配的需求派生出一组完整的软件需求。

为确保系统的完整性，制造商宜规定对系统需求进行变更和澄清的协商机制，以纠正母系统需求或软件需求中不切实际、不一致或模糊之处。

系统和软件需求的获取和分析过程可以是迭代性的。本标准并不要求将过程严格地划分成两层。但在实践中，通常将系统体系结构和软件体系结构同时概述，随后将系统和软件需求以分层的形式形成文件。

B.5.3 软件体系结构设计

此项活动要求制造商定义软件的主要结构组件并确定其关键任务，其外部可见特性，以及组件之间

的关系。如果一个组件的特性会影响其他组件，则在软件体系结构中宜对该特性进行描述。对于可能影响软件之外医疗器械组件的特性，这种描述尤其重要（见 5.3.5 和 B.4.3）。有关体系结构的决定对于实施风险控制措施极其重要。不理解（及不形成文件）可能影响其他组件的组件特性，几乎不可能证明系统是安全的。软件体系结构是确保软件需求的正确实现所必需的。除非所有的软件需求能由所确定的软件项来实现，否则软件体系结构是不完整的。由于软件的设计和实现依赖于体系结构，所以为完成该活动，要对体系结构进行验证。体系结构的验证一般通过技术评价进行。

在软件体系结构活动期间对软件项的软件安全分级为随后的软件过程选择打下了基础。分级的记录作为风险管理文档的一部分置于变更控制之下。

许多后续的事件可能使分级无效。包括如下示例：

——系统规范、软件规范或体系结构的变更；

——在风险分析中发现的错误，尤其是不可预见的危险（源）；

——发现某需求不可行，尤其是风险控制措施。

因此，在软件体系结构设计之后的所有活动期间，宜对软件系统和软件项的分级进行再评价，而且可能需要对其进行修正。作为将分级升级到更高级别的结果，这有可能引发返工以对软件项应用附加过程。使用软件配置管理过程（见第 8 章）确保所有必要的返工的识别和完成。

B.5.4 软件详细设计

此项活动要求制造商细化在体系结构中定义的软件项和接口，以创建软件单元及其接口。虽然软件单元常常被认为是单一的功能或模块，但该观点并不总是适当的。本标准已将软件单元定义为不再细分为更小项目的软件项。软件单元可单独进行测试。制造商宜定义软件单元的详细程度。详细设计规定算法、数据表示法、不同软件单元之间的接口和软件单元与数据结构之间的接口。详细设计也必然要涉及医疗器械软件的封装。足够详细地定义软件单元和接口的设计是必要的，以便客观地验证其安全和有效性，在这种情况下，能够使用其他需求或设计文档来确保这一点。详细设计宜足够完整，而不需要程序员做出临时的设计决定。详细设计还应考虑医疗器械软件的体系结构。

软件项可以被分解，以便只有少数几个新软件项实现原软件项安全有关的要求。其余软件项不实现安全有关的功能，并且可被重新分级到较低的软件安全级别。然而，做出这一决定本身就是风险管理过程的一部分，宜在风险管理文档中形成文件。

因为实现依赖详细设计，所以有必要在完成活动之前验证详细设计。详细设计的验证通常通过技术评价进行。5.4.4 要求制造商验证详细设计活动的输出。设计规定如何实现需求。设计验证确保设计实现软件体系结构，且与软件体系结构不相矛盾。

如果设计含有缺陷，编码就不会正确地实现需求。

当在设计中出现制造商认为对安全重要的设计特性时，制造商宜对其进行验证。这些特性的示例包括：

——预期事件的实现，CPU 的输入、输出、接口、逻辑流和分配，存储资源配置，错误和例外的定义，错误和例外的隔离，以及错误的纠正；

——缺省状态的定义，在该状态下对所有可导致危险情况的故障与事件和转移一起进行处理；

——变量的初始化，存储管理；

——冷复位和热复位、待机和其他可能影响风险控制措施的状态变化。

B.5.5 软件单元的实现

此项活动要求制造商编写并验证软件单元代码。详细设计被转化为源代码。编码代表规范分解的终点，和可执行软件编写的开始。为了持续达到期望的编码特性，宜使用编码标准规定优先选择的编码风格。编码标准示例包括对可理解性、语言使用规则或限制以及复杂性管理的要求。对每个单元的编

码进行验证，以确保其按详细设计所规定的那样起作用，并符合所规定的编码标准。

5.5.5 要求制造商验证编码。如果编码未正确实现设计，医疗器械软件将不按预期运行。

B.5.6 软件集成和集成测试

此项活动要求制造商策划并将软件单元集成为软件项集合，以及将软件项集成为较高集成度的软件项集合，并验证所形成的软件项按照预期运行。

集成的方法可包括从非递增的集成到任何形式的递增集成。被集成的软件项的性质决定所选择的集成方法。

软件集成测试重点关注数据的传输和软件项内部和外部接口间的控制。外部接口是那些与包括操作系统软件在内的其他软件以及医疗器械硬件间的接口。

集成测试的严格程度以及与集成测试有关文档的详细程度宜与以下各项相匹配：与器械有关的风险、器械具有潜在危害的功能对软件的依赖性及特定软件项在较高风险的器械功能方面的作用。例如，尽管所有软件项都宜进行测试，但对安全有影响的软件项宜经受更直接、彻底和详细的测试。

适用时，集成测试证实程序在其输入和输出域边界的性能，并确认程序对无效的、非预期的和特殊输入的响应。当给定输入组合或非预期的输入顺序，或当违反规定的时序要求时，程序的动作就显示出来。适当时，计划中的测试需求宜包括作为集成测试一部分来执行的白盒测试。

白盒测试，也就是通常所说的透明盒、结构的、净盒和开盒测试，是一种测试技术，它利用被测试软件项内部活动的显性知识来选取测试数据。白盒测试利用对软件项的特定了解来检测输出。只有当测试者知道软件项的预期动作时，测试才是准确的。然后测试者就可以明白软件项是否偏离其预期目标。白盒测试不能保证全部规范已被实现，因其专注于对软件项实现的测试。黑盒测试，也通称为性能的、功能的、不透明盒和闭盒测试，专注于对功能规范的测试，它不能保证实现的所有部分都得到测试。因而黑盒测试是针对规范的测试，会发现遗漏有关的错误，表明部分规范未得到满足。白盒测试是针对实现的测试，将发现运转状态方面的错误，表明部分实现有缺陷。为全面测试医疗器械软件，黑盒测试和白盒测试可能都是需要的。

在 5.6 和 5.7 中确定的计划和测试文档可能是限于特定开发阶段或进化型原型独有的文件。它们也可以组合，使单一文件或成套文件覆盖多个子部分的需求。文件的全部或部分可以合并到较高层级的项目文件中，诸如一个软件或项目的质量保证计划，或一个阐明硬件和软件测试各方面的综合测试计划。在这些情况下，宜建立交叉索引来识别不同的项目文件与每个软件集成任务之间的关系。

软件集成测试可在模拟环境中、在实际的目标硬件上或在整个医疗器械上进行。

5.6.2 要求制造商验证软件集成活动的输出。软件集成活动的输出是集成后的软件项。为使整个医疗器械软件正确安全地运行，这些集成的软件项应正常运行。

B.5.7 软件系统测试

此项活动要求制造商通过验证软件需求的成功实现验证软件的功能。

软件系统测试证实软件具有规定的功能。这项测试验证根据软件需求所建立的程序的功能和性能。

软件系统测试专注于功能（黑盒）测试，虽然可能希望使用白盒测试（见以前部分）的方法更有效地完成某些测试，如启动压力条件或缺陷，以及增加合格性测试的代码覆盖率。按测试类型和测试阶段测试的组织是灵活的，但对需求、风险控制、可用性以及测试类型（如缺陷测试、安装测试、压力测试）的覆盖率宜得到证实并形成文件。

软件系统测试是对集成后软件的测试，可在模拟环境中、在实际的目标硬件上或在整个医疗器械上进行。

当对软件系统做出变更（即使是小的变更）时，宜确定回归测试的程度（不仅仅是对单个变更的测

试)以确保没有引入非预期的副作用。宜对此项回归测试(以及不完全重复软件系统测试的理由说明)进行策划并形成文件(参见 B.6.3)。

软件系统测试的职责可以分散开,发生在不同的位置并由不同的组织进行。然而,不管任务分配、合同关系、组件来源或开发环境如何,器械制造商对确保软件按其预期用途正确运行保留最终责任。

如果在测试期间发现的反常可重复,但是已做出不修复它们的决定,那么就需要对这些反常与风险分析相联系进行评价,以验证其不影响器械的安全。宜了解反常的根本原因和征兆,并把不修复它们的理由说明形成文件。

5.7.4 要求对软件系统测试的结果进行评价,以确保获得了预期结果。

B.5.8 软件在系统级别应用的发布

此项活动要求制造商将要发布的医疗器械软件的版本形成文件,说明该版本的软件是如何创建的,并遵循软件发布的适当规程。

制造商宜能够表明所发布的软件是按开发过程开发的。如果将来需要的话,制造商也宜能够回溯该软件以及用于软件生成的工具,并以将受损或误用减到最低的方式存储、包装和交付软件。宜建立确定的规程以确保适当地完成这些任务,并有一致的结果。

B.6 软件维护过程

B.6.1 建立软件维护计划

软件维护过程不同于软件开发过程,在于以下两方面:

——允许制造商用比完整的软件开发过程更简捷的过程实现快速的变更,以对紧急问题做出响应;

——响应与已发布产品有关的软件问题报告时,制造商不仅要处理问题,也要符合当地法规(一般通过运行一个主动的警戒方案来实现,从现场收集问题数据并就问题与用户和监管机构沟通)。

6.1 要求在维护计划中建立这些过程。

此项活动要求制造商创建或识别实施维护活动和任务的规程。为了实施纠正措施,控制维护期间的变更和管理修订后软件的发布,制造商宜形成文件并解决已报告的问题和来自用户的请求,同时管理对医疗器械软件的修改。当由于问题或由于改进或调整的需要,对医疗器械软件进行代码和有关文档的修改时,此过程被激活。其目标是修改已发布的医疗器械软件并保持其完整性。此过程包括将医疗器械软件移植到不是其最初发布时的环境或平台。本章规定的活动对于维护过程是特有的;然而,维护过程也有可能使用本标准中的其他过程。

制造商需要对如何进行维护过程相关的活动和任务做出策划。

B.6.2 问题和修改分析

此项活动要求制造商分析反馈的影响,验证所报告的问题,考虑、选择修改选项并获得对其实施的批准。问题和其他变更请求可能影响医疗器械的性能、安全或法规许可。有必要通过分析确定一份问题报告是否存在任何影响,或为纠正一个问题或实现一项请求所做的修改是否将产生任何影响。通过追踪或回归分析对以下内容进行验证特别重要,即作为软件维护活动的组成部分,正实施的软件变更未对内置在医疗器械内的风险控制措施产生不利的变更或修改。在对先前未引起危险情况或没有降低风险的软件进行修改时,验证其在修改后也不引起危险情况或没有降低风险也很重要。如果当前的软件修改可能导致危险(源)或降低风险,则软件项的软件安全级别有可能已改变。

区分软件维护(见第 6 章)和软件问题解决(见第 9 章)是很重要的。

软件维护过程关注的是对医疗器械软件发布后出现的反馈充分响应。作为医疗器械的组成部分,

软件维护过程需要确保：

——有关安全的问题报告得到处理并向适当的监管机构以及受影响的用户报告；

——修改后的医疗器械软件要再确认和再发布，且修改在确保问题纠正和避免另外问题的正式控制下进行；

——制造商考虑哪些其他的医疗器械软件可能受到影响并采取适当的措施。

软件问题解决关注的主要是以下综合控制体系的运行：

- 分析问题报告并识别问题的所有含义；
- 对一些变更做出决定，并识别其所有的副作用；
- 在保持包括风险管理文档在内的软件配置项一致性的同时实施变更；
- 验证变更的实施。

软件维护过程利用软件问题解决过程。软件维护过程处理关于问题报告的高层次决策(问题是否存在，问题是否对安全有显著影响，需要什么变更，何时实施变更)，并用软件问题解决过程分析问题报告，以发现所有的含义并产生可能的变更请求，该请求识别所有需要变更的配置项和所有必需的验证步骤。

B.6.3 修改的实施

此项活动要求制造商用已建立的过程做出修改。如果还未定义维护过程，可用适当的开发过程任务来做出修改。制造商也宜确保修改不会引起对医疗器械软件其他部分的负面影响。除非把医疗器械软件当作新的开发项目来看待，否则分析修改对整个医疗器械软件的影响是必要的。利用回归分析和测试确保变更未在医疗器械软件其他地方产生问题。回归分析是基于对相关文档的评审(例如：软件需求规范、软件设计规范、源代码、测试计划、测试用例及测试脚本等)确定变更的影响，以便确定需要运行的必要的回归测试。回归测试是重新运行先前已在程序上正确执行的测试用例，并将当前结果与先前结果进行比较，以便发现软件变更的非预期影响。应给出理由证明将要执行的回归测试的总量是合理的，以确保医疗器械软件未修改的部分仍然做出修改之前那样运行。

B.7 软件风险管理过程

软件风险管理是整个医疗器械风险管理的一部分，对其进行孤立地阐述是不充分的。本标准要求使用符合 YY/T 0316 的风险管理过程，如 YY/T 0316 所规定的那样，风险管理专门讨论对医疗器械使用相关风险进行有效管理的框架。YY/T 0316 的一部分是关于所识别风险的控制，这些风险又与在风险分析过程中识别的每个危险(源)有关。本标准中的软件风险管理过程预期为软件的风险控制提供附加要求，包括在风险分析期间已识别的潜在促成危险情况的软件，或用于控制医疗器械风险的软件。由于以下两个原因，本标准中包括软件风险管理过程：

a) 本标准预期的读者需要理解其在软件这一职责范围内对风险控制措施的最低要求；

b) 通用风险管理标准 YY/T 0316，在本标准中作为规范性引用文件而提供，不特别阐述软件的风险控制和风险控制在软件开发生存周期中的位置。

软件风险管理是整个医疗器械风险管理的组成部分。软件风险管理活动要求的计划、规程和文档可以是一系列的独立文件或单一文件，或者只要满足本标准中的所有要求，可将其与医疗器械风险管理活动和文档相整合。

B.7.1 促成危险情况的软件分析

通过器械的危险(源)分析期望能识别危险情况和相应的风险控制措施，以将危险情况的概率和/或严重程度降低到可接受水平。也期望将风险控制措施分配给预期实现那些风险控制措施的软件功能。

然而，并不期望在软件体系结构形成之前识别所有的器械危险情况。在软件体系结构形成时已知道软件功能如何在软件组件中实现，并且可以评价将风险控制措施分配给软件功能的实际可行性。在那时宜修订器械危险（源）分析以包括：

- 经修正的危险情况；
- 经修正的风险控制措施和软件需求；
- 由软件引起的新的危险情况，如与人的因素有关的危险情况。

软件体系结构宜包括隔离软件组件的可信赖的策略，以使其不以不安全的方式相互作用。

B.8 软件配置管理过程

软件配置管理过程是在软件的整个生存周期中应用管理性和技术性规程的过程，以识别和定义系统内的软件项（包括文档），控制项目的修改和发布，将项目和变更请求的状态形成文件并进行报告。软件配置管理对重建软件项，对识别其组成部分以及提供对其做出变更的历史记录是必需的。

B.8.1 配置标识

此项活动要求制造商对软件配置项及其版本进行唯一标识。这种标识对于识别包括在医疗器械软件中的软件配置项及其版本是必需的。

B.8.2 变更控制

此项活动要求制造商控制软件配置项的变更，将识别变更请求和有关其处置的信息形成文件。此项活动是必需的，以确保不对软件配置项做出未授权的或非预期的变更，并确保经批准的变更请求得到充分地实现和验证。

变更请求可以由变更控制部门、管理人员或技术领导按照软件配置管理计划批准。经批准的变更请求与软件的实际修改和验证有可追溯性。要求每个实际的变更与变更请求相关联，并存在文档表明变更请求得到了批准。文档可以是变更控制部门的会议纪要、批准签名或数据库中的记录。

B.8.3 配置状态报告

此项活动要求制造商保持软件配置项的历史记录。此项活动是必需的以确定何时、为什么做出变更。具有访问此信息的权限是必需的，以确保软件配置项仅包含经授权的修改。

B.9 软件问题解决过程

软件问题解决过程是一个分析和解决问题（包括不符合）的过程，无论问题的性质或来源，包括那些在实施开发、维护或其他过程期间发现的问题。其目标是提供一种及时、负责、形成文件的方法以确保发现的问题得到分析和解决，并辨别问题的趋势。有时在软件工程文献中将此过程称为“缺陷追踪”。在 ISO/IEC 12207[12] 和 IEC 60601-1-4[7] 修正案 1 中被称为“问题解决”。在本标准中称之为“软件问题解决”。

此活动要求制造商在识别出问题或不符合时，使用软件问题解决过程。此项活动是必需的以确保所发现问题与安全（如 YY/T 0316 中所确定）的潜在关联性得到分析和评价。

5.1 要求一项或多项软件开发计划或规程是为了阐明如何处理问题或不符合。这包括在生存周期的各阶段以正式和形成文件的方式确定软件问题解决过程的各个方面，以及确定何时将问题和不符合输入到软件问题解决过程。

附 录 C
（资料性附录）
与其他标准的关系

C.1 总则

本标准适用于医疗器械软件的开发和维护。这里软件是医疗器械子系统或医疗器械本身。当开发医疗器械时，本标准与其他适用的标准一起使用。

医疗器械管理标准，诸如 YY/T 0287[5]（参见 C.2 和附录 D）和 YY/T 0316（参见 C.3），为组织提供管理环境，为开发产品奠定基础。而像 IEC 60601-1[6]（参见 C.4）和 IEC 61010-1[9]（参见 C.5）这类安全标准则为创建安全的医疗器械给出特定的指导。当软件是这些医疗器械的一部分时，对于如何开发和维护安全的医疗器械软件，本标准提供更详细地指导。对于许多其他标准，诸如 ISO/IEC 12207[12]（参见 C.6），GB/T 20438.3[4]（参见 C.7）和 ISO/IEC 90003[17]等，可将其视为实现本标准中需求的方法、工具和技术的来源。图 C.1 表示这些标准的关系。

在引用其他标准中的章条或要求的地方，引用条款中的术语是其他标准中定义的术语，而不是本标准中定义的术语。

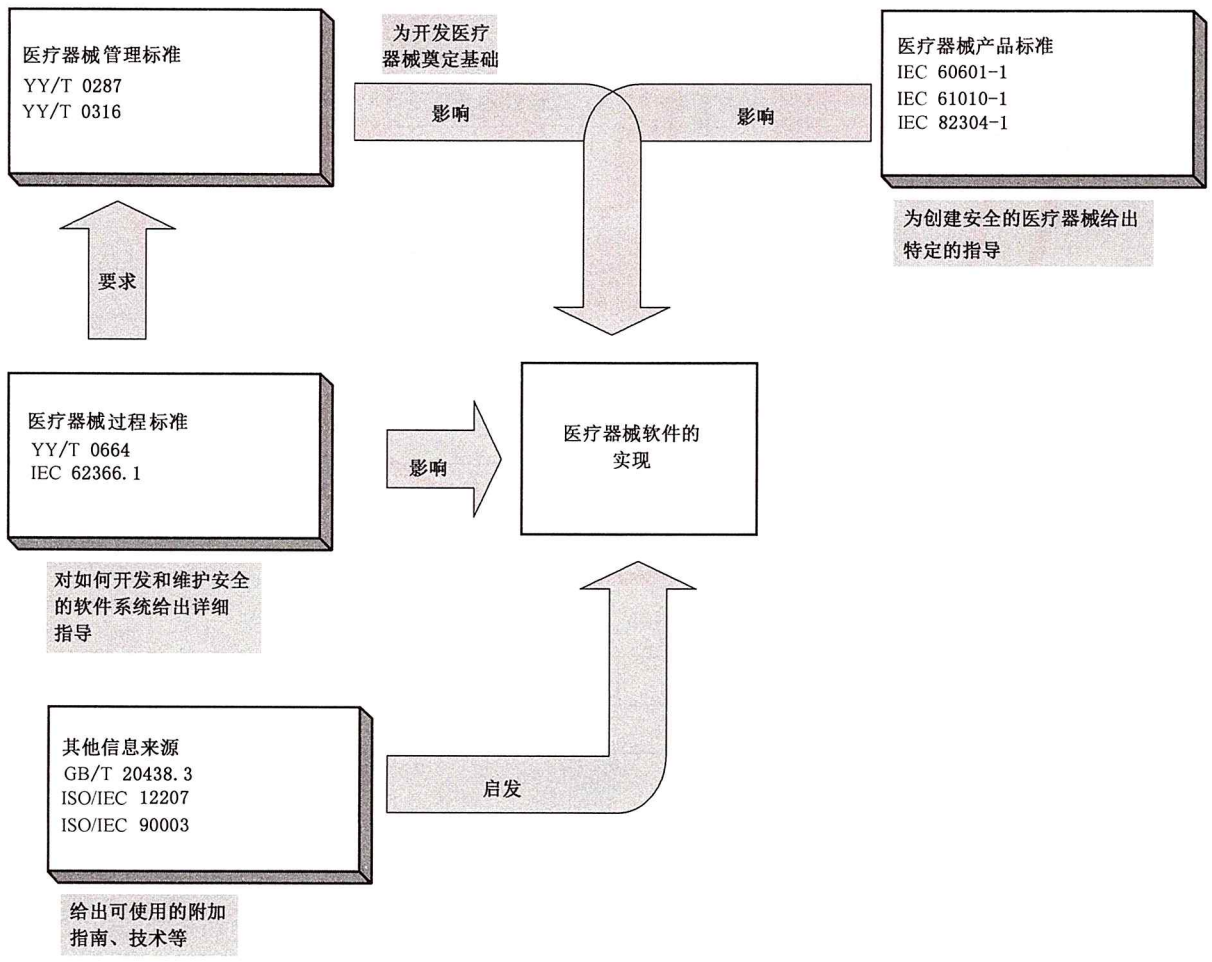


图 C.1 重要医疗器械标准与本标准的关系

C.2 与 YY/T 0287 的关系

本标准要求制造商使用质量管理体系。当制造商使用 YY/T 0287[5] 时，本标准的要求直接与YY/T 0287的一些要求有关，如表 C.1 所示。

表 C.1 与 YY/T 0287—2017 的关系

本标准章条号	YY/T 0287—2017 的相关章条号
5.1 软件开发策划	7.3.2 设计和开发策划
5.2 软件需求分析	7.3.3 设计和开发输入
5.3 软件体系结构设计	
5.4 软件详细设计	
5.5 软件单元的实现	
5.6 软件集成和集成测试	
5.7 软件系统测试	7.3.4 设计和开发输出 7.3.5 设计和开发评审
5.8 软件在系统级别应用的发布	7.3.6 设计和开发验证 7.3.7 设计和开发确认
6.1 建立软件维护计划	7.3.9 设计和开发更改的控制
6.2 问题和修改分析	
6.3 修改的实施	7.3.6 设计和开发验证 7.3.7 设计和开发确认
7.1 促成危险情况的软件分析	
7.2 风险控制措施	
7.3 风险控制措施的验证	
7.4 软件变更的风险管理	
8.1 配置标识	7.5.8 标识 7.5.9 可追溯性
8.2 变更控制	7.5.8 标识 7.5.9 可追溯性
8.3 配置状态报告	
9 软件问题解决过程	

C.3 与 YY/T 0316—2016 的关系

表 C.2 表示本标准对 YY/T 0316—2016 要求的风险管理过程做了进一步阐述的条款。

表 C.2　与 YY/T 0316—2016 的关系

YY/T 0316—2016 章条号	本标准的相关章条号
4.1 风险分析过程	
4.2 医疗器械预期用途和与安全有关特征的识别	
4.3 危险(源)的识别	7.1 促成危险情况的软件分析
4.4 估计每个危险情况的风险	4.3 软件安全分级
5 风险评价	
6.1 降低风险	
6.2 风险控制方案分析	7.2.1 确定风险控制措施
6.3 风险控制措施的实施	7.2.2 在软件中实施的风险控制措施 7.3.1 验证风险控制措施
6.4 剩余风险评价	
6.5 风险/受益分析	
6.6 由风险控制措施产生的风险	
6.7 风险控制的完整性	
7 综合剩余风险的可接受性评价	
8 风险管理报告	7.3.2 将可追溯性形成文件
9 生产和生产后的信息	7.4 软件变更的风险管理

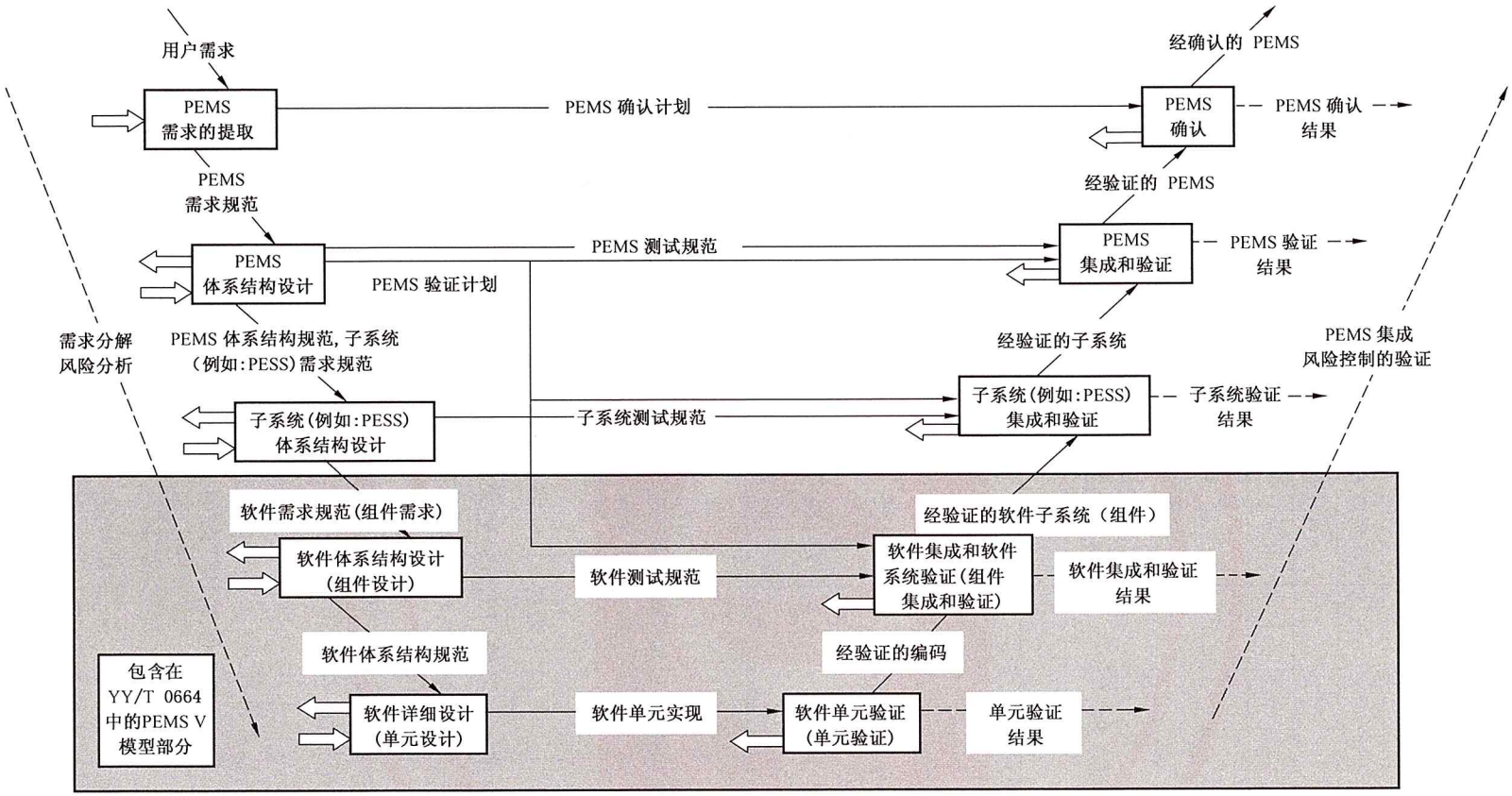
C.4　与 IEC 60601-1:2005＋IEC 60601-1:2005/AMD1:2012 中可编程医用电气系统(PEMS)要求的关系

C.4.1　总则

对软件的要求是对可编程医用电气系统(PEMS)要求的子集。本标准确定的对软件的要求，是 IEC 60601-1:2005＋IEC 60601-1:2005/AMD1:2012 对 PEMS 要求的补充，但并非与其不兼容。因为 PEMS 包括非软件要素，不是所有 IEC 60601-1:2005＋IEC 60601-1:2005/AMD1:2012 对 PEMS 的要求都在本标准中阐述。随着 IEC 60601-1:2005 和 IEC 60601-1:2005 / AMD1:2012 的出版，IEC 62304 目前是 IEC 60601-1 的规范性引用文件，符合 IEC 60601-1:2005＋IEC 60601-1:2005/AMD1:2012 第 14 章(因此符合该标准)要求符合 YY/T 0664 的部分要求(而非整个标准，因为 IEC 60601-1:2005＋IEC 60601-1:2005/AMD1:2012 不要求符合 IEC 62304 的生产后和维护要求)。重要的是 IEC 60601-1:2005＋IEC 60601-1:2005/AMD1:2012 仅在软件是 PEMS 的一部分时适用，若软件自身为医疗器械则不适用。

C.4.2　软件与 PEMS 开发的关系

图 C.2 所示的 V-模型描述了 PEMS 开发期间发生的活动；可以看出，从软件需求规范到软件项集成为软件系统，本软件标准的要求在 PEMS 组件级上是适用的。该软件系统是可编程电气子系统(PESS)的一部分，PESS 又是 PEMS 的一部分。



说明：

方框代表典型的开发生存周期活动；

实线箭头表示活动输入/转出的典型交付物；

虚线箭头表示仅属于风险管理文档的交付物；

⇨ 来自问题解决过程的输出；

⇦ 对问题解决过程的输入。

图 C.2　软件作为 V 模型的一部分

C.4.3 开发过程

符合本标准的软件开发过程(见第5章)要求明确规定一个软件开发计划并遵照执行;它不要求使用任何特别的生存周期模型,但确实要求该计划包括某些活动并具有某些属性。这些要求与IEC 60601-1中对PEMS的开发生存周期、需求规范、体系结构、设计和实现、验证的要求有关。本标准中有关软件开发的要求比IEC 60601-1中的要求更详细。

C.4.4 维护过程

符合本标准的软件维护过程(见第6章)要求在对软件做出变更时,建立规程并遵照执行。这些要求相当于IEC 60601-1中对PEMS修改的要求。关于软件维护时必要的活动,本标准中对软件维护的要求比IEC 60601-1中对PEMS修改的要求更详细。

C.4.5 其他过程

本标准中的其他过程对软件明确规定了附加的要求,该要求超出IEC 60601-1中对PEMS的类似要求。在大多数情况下,IEC 60601-1中有对PEMS的通用要求,本标准中的过程是在此基础上的进一步阐述。

本标准中的软件风险管理过程相当于对IEC 60601-1中为PEMS确定的风险管理要求的补充。

本标准中的软件问题解决过程相当于IEC 60601-1中对PEMS问题解决的要求。

本标准中的软件配置管理过程明确规定了IEC 60601-1对PEMS的要求中所没有的,除文档外的附加要求。

C.4.6 IEC 60601-1:2005+IEC 60601-1:2005/AMD1:2012中可编程医用电气系统(PEMS)要求的覆盖范围

表C.3表示IEC 60601-1对PEMS的要求与本标准中相应的要求。

表C.3 与IEC 60601-1的关系

IEC 60601-1:2005+IEC 60601-1:2005/AMD1:2012对PEMS的要求	YY/T 0664有关PEMS软件子系统的要求
14.1 概述 14.2和14.12的要求应适用于PEMS,除非: ——可编程电子子系统(PESS)不提供基本安全或基本性能所必需的功能;或 ——应用4.2描述的风险管理,表明任何PESS的失效不会导致不可接受的风险。 不论14.2~14.12的要求是否适用,14.13的要求适用于预期接入IT-网络的任何PEMS。 当14.2~14.13的要求适用时,YY/T 0664—2008中4.3,第5章、第7~9章的要求也应适用于每个PESS软件的开发或修改	4.3 软件的安全性级别 IEC 60601-1对PEMS的要求仅适用于软件安全B级和C级。本标准包括一些适用于软件安全A级的要求。 符合IEC 60601-1所要求的软件开发过程不包括第6章所要求的生产后监视和维护
14.2 文档 第14章要求的文档应按照正式的文件控制程序,进行评审、批准、发布和更改	5.1 软件开发策划 除软件开发策划活动中的特定要求之外,作为风险管理文档一部分的文件需要按YY/T 0316予以保持。另外,对于质量体系要求的文件,YY/T 0287[5]要求对其进行控制

表 C.3（续）

IEC 60601-1:2005+IEC 60601-1:2005/AMD1:2012 对 PEMS 的要求	YY/T 0664 有关 PEMS 软件子系统的要求
14.3 风险管理计划 按 4.2.2 形成的风险管理计划应包括对 PEMS 确认计划（见 14.11）的引用	无特定要求。 无特定的软件确认计划。PEMS 确认计划是系统级上的，因而超出本软件标准的范围。然而本标准确实要求从危险（源）到特定的软件原因，到风险控制措施，再到风险控制措施的验证（见 7.3）均具有可追溯性
14.4 PEMS 开发生存周期 PEMS 开发生存周期应形成文件	5.1 软件开发策划 5.1.1 软件开发计划 由软件开发计划阐明的项目构成一个软件开发生存周期
PEMS 开发生存周期应包含一组已定义的里程碑	
在每个里程碑，应确定将要完成的活动和验证这些活动的方法	5.1.6 软件验证策划 必须对验证任务、里程碑和验收准则进行策划
应确定每个活动，包括其输入和输出	5.1.1 软件开发计划 活动在本标准中定义。要生成的文档在每个活动中定义
每个里程碑应识别在此里程碑结束前一定有完成的风险管理活动	
应通过制定详细的活动、里程碑和进度表计划，来为特定的开发定制 PEMS 开发生存周期	5.1.1 软件开发计划 本标准允许在开发计划中将开发生存周期形成文件。这意味着开发计划包含定制的开发生存周期
PEMS 开发生存周期应包括对文档的要求	5.1.1 软件开发计划 5.1.8 文档策划
14.5 问题解决 适当时，应在 PEMS 开发生存周期的所有阶段和活动内或相互间建立和维护一个文件化的问题解决体系	9 软件问题解决过程
根据产品类型，问题解决体系可以： ——作为 PEMS 开发生存周期的一部分形成文件； ——允许报告影响基本安全或基本性能的潜在或现存的问题； ——包括对每个涉及风险问题的评定； ——确定将问题解决必须要满足的准则； ——确定解决每个问题所采取的措施	5.1.1 软件开发计划 9.1 准备问题报告
14.6 风险管理过程	7 软件风险管理过程
14.6.1 已知的或可预见的危险（源）的识别 在编制已知的或可预见的危险（源）列表时，制造商应考虑那些与 PEMS 软件和硬件方面相关的危险（源），包括 PEMS 接入 IT-网络、第三方来源组件和遗留子系统的危险（源）	7.1 促成危害处境的软件分析 本标准没有特别提及网络/数据耦合

表 C.3（续）

IEC 60601-1:2005+IEC 60601-1:2005/AMD1:2012 对 PEMS 的要求	YY/T 0664 有关 PEMS 软件子系统的要求
14.6.2 风险控制 为实现每个风险控制措施，应选择和确定合适的已确认的工具和程序。这些工具和程序应适用于确保每个风险控制措施能有效地降低已识别的风险	5.1.4 软件开发标准、方法和工具的策划 本标准要求确定的特定工具和方法用于一般开发，不用于每个风险控制措施
14.7 需求规范 对于 PEMS 及其各子系统（例如：PESS），应有形成文件的需求规范	5.2 软件需求分析 本标准仅阐述 PEMS 的软件子系统
系统或者子系统的需求规范，应包含并区分由其自身实施的任何基本性能和任何风险控制措施	5.2.1 定义来自系统需求的软件需求并将其形成文件 5.2.2 软件需求内容 5.2.3 将风险控制措施纳入软件需求 本标准不要求对与基本性能和风险控制措施有关的需求与其他需求进行区分，但确实要求所有需求得到唯一识别
14.8 体系结构 对于 PEMS 及其各子系统，应明确规定符合需求规范的体系结构	5.3 软件体系结构设计
适当时，为把风险降低到可接受的水平，体系结构规范应采用： a） 高完善性元器件； b） 失效安全功能； c） 冗余设计； d） 多样性； e） 功能划分； f） 防护性设计，例如通过限制可得到的输出能量或采用限制执行机构的行程的方法来限制潜在危险的影响	5.3.5 判定风险控制所必需的隔离 划分是被唯一确定的技术，其所以被确定识别，是因为需要说明如何保证划分的完整性
体系结构规范应考虑： a） 对 PEMS 子系统及其组件的风险控制措施的配置； b） 组件失效模式及其效应； c） 共同原因的失效； d） 系统性失效； e） 测试的间隔持续时间和诊断覆盖范围； f） 可维护性； g） 可合理预见的误使用的防护； h） 如适用，IT-网络规范	本标准中不包括
14.9 设计和实现 适当时，设计应分解为各子系统，每个子系统都有设计和测试规范	5.4 软件详细设计 5.4.2 为每个软件单元开发详细设计 本标准不要求详细设计的测试规范
关于设计环境的描述数据应形成文件	5.4.2 为每个软件单元开发详细设计
14.10 验证 所有实现基本安全、基本性能或风险控制措施的功能都需要得到验证	5.1.6 软件验证策划 每项活动都要求验证

表 C.3（续）

IEC 60601-1:2005+IEC 60601-1:2005/AMD1:2012 对 PEMS 的要求	YY/T 0664 有关 PEMS 软件子系统的要求
应制定验证计划以表明这些功能是如何被验证的。计划应包括： ——在每个里程碑，对各个功能进行验证； ——验证策略、活动、技术及执行验证人员的适当独立程度的选择和形成文件； ——验证工具的选择和运用； ——验证的覆盖准则	5.1.6 软件验证策划 人员的独立性不包括在本标准中。考虑在 YY/T 0287 中覆盖
验证应根据验证计划执行。验证活动的结果应形成文件	在大部分活动中有验证要求
14.11 PEMS 确认 PEMS 确认计划应当包含基本安全和基本性能的确认	本标准不覆盖软件确认。PEMS 确认是系统级活动，超出本标准的范围
PEMS 确认采用的方法应形成文件	本标准不覆盖软件确认。PEMS 确认是系统级活动，超出本标准的范围
应根据 PEMS 确认计划实施 PEMS 确认。PEMS 确认活动的结果应形成文件	本标准不覆盖软件确认。PEMS 确认是系统级活动，超出本标准的范围
全面负责 PEMS 确认的人员应独立于设计组。制造商应将独立性程度的解释说明形成文件	本标准不覆盖软件确认。PEMS 确认是系统级活动，超出本标准的范围
设计组成员不应承担其自己设计部分的确认工作	本标准不覆盖软件确认。PEMS 确认是系统级活动，超出本标准的范围
风险管理文档中应记录 PEMS 确认组成员和设计组成员之间的所有专业关系	本标准不覆盖软件确认。PEMS 确认是系统级活动，超出本标准的范围
风险管理文档中应包括 PEMS 确认方法和结果的引用	本标准不覆盖软件确认。PEMS 确认是系统级活动，超出本标准的范围
14.12 修改 如果任何部分或者全部设计是对早期设计的修改，则作为全新设计适用本章所有条款，或任何早期设计文档的持续有效性应在文件化修改/更改程序下进行评定	6 软件维护过程 本标准采用的方法：软件维护宜进行策划，修改的实现宜利用软件开发过程或已建立的软件维护过程
当软件被修改时，YY/T 0664—2008 中 4.3，第 5 章、第 7～9章的要求也应适用于修改	
14.13 预期接入 IT-网络的 PEMS 如果 PEMS 预期接入未经 PEMS 制造商确认过的 IT-网络，制造商为实现这样的连接应提供有效的说明，包括以下内容： a) PEMS 连接到 IT-网络的目的； b) 与 PEMS 相连的 IT-网络所要求的特性； c) 与 PEMS 相连的 IT-网络所需的配置； d) PEMS 网络连接的技术规范，包括数据安全规范； e) 在 PEMS，IT-网络和 IT-网络上的其他设备间的预期信息流，以及预期通过 IT-网络的路由；和	接入 IT-网络的要求不包括在本标准中

表 C.3（续）

IEC 60601-1:2005+IEC 60601-1:2005/AMD1:2012 对 PEMS 的要求	YY/T 0664 有关 PEMS 软件子系统的要求
注 1：这可以包括与基本安全和基本性能有关的有效性、数据和系统安全的各方面（参见附录 H 中 H.6 和 IEC 80001-1:2010）。 f) 为达到 PEMS 与 IT-网络连接目的所需特性的 IT-网络失效时的危险情况清单。 在随附文件中，制造商应告知责任方： ——PEMS 与包含其他设备的 IT-网络的连接可能导致对患者、操作者、第三方带来以往没有识别的风险； ——责任方宜识别、分析、评价和控制这些风险； 注 2：IEC 80001-1:2010 为责任方解决这些风险提供了指南。 ——对 IT-网络的后续修改可能引入新的风险，需要进行补充分析； ——IT-网络的更改包括： • IT-网络配置的更改； • 与 IT-网络连接的新增项； • 与 IT-网络连接中断的项； • 与 IT-网络连接的设备的更新； • 与 IT-网络连接的设备的升级	接入 IT-网络的要求不包括在本标准中

C.5 与 IEC 61010-1 的关系

IEC 61010-1[9]的范围包括电气测试和测量设备，电气控制设备和电气实验室设备。仅部分实验室设备用于医疗环境或作为体外诊断设备（IVD）使用。

由于法律法规或规范性引用文件的原因，将体外诊断设备划归为医疗器械，然而却未将其纳入 IEC 60601-1[6]的范围之内。严格来说，这不仅归因于体外诊断设备不是与患者直接接触的医疗器械这样的事实；而且也归因于此类产品是为在不同实验室的许多不同应用而制造的事实。因而作为体外诊断仪器或其附件来使用的情况是很少的。

如果将实验室设备用作体外诊断设备，所获得的测量结果应按照医疗准则进行评价。此时要求应用 YY/T 0316 进行风险管理。如果此类产品也包含可能导致危险情况的软件，例如软件引起的失效导致医疗数据（测量结果）的意外改变，则应考虑本标准。

IEC 61010-1:2010 第 17 章中有对风险评定的通用要求，它比 YY/T 0316 中全面的风险管理要求更加简化。单独应用 IEC 61010-1 第 17 章不符合本标准风险管理所要求的准则，该准则基于全部 YY/T 0316的风险管理要求。出于这种考虑，本标准期望当 IVD 医疗器械有软件相关的风险时，其风险管理过程的实施遵循 YY/T 0316，而不是仅遵循 IEC 61010-1 的第 17 章。符合 IEC 61010-1 的第 17 章注中所述，就可以符合 IEC 61010-1 的第 17 章：

注：IEC 61010-1 附录 J 中概述了一个风险评定程序。其他的风险评定程序包含 YY/T 0316、SEMI S10-1296、IEC 61508、ISO 14121-1 和 ANSI B11.TR3 之中。也可使用其他已建立的实施类似步骤的程序。

图 C.3 中的流程图表示将 IEC 61010-1 第 17 章与本标准联合应用的情况。

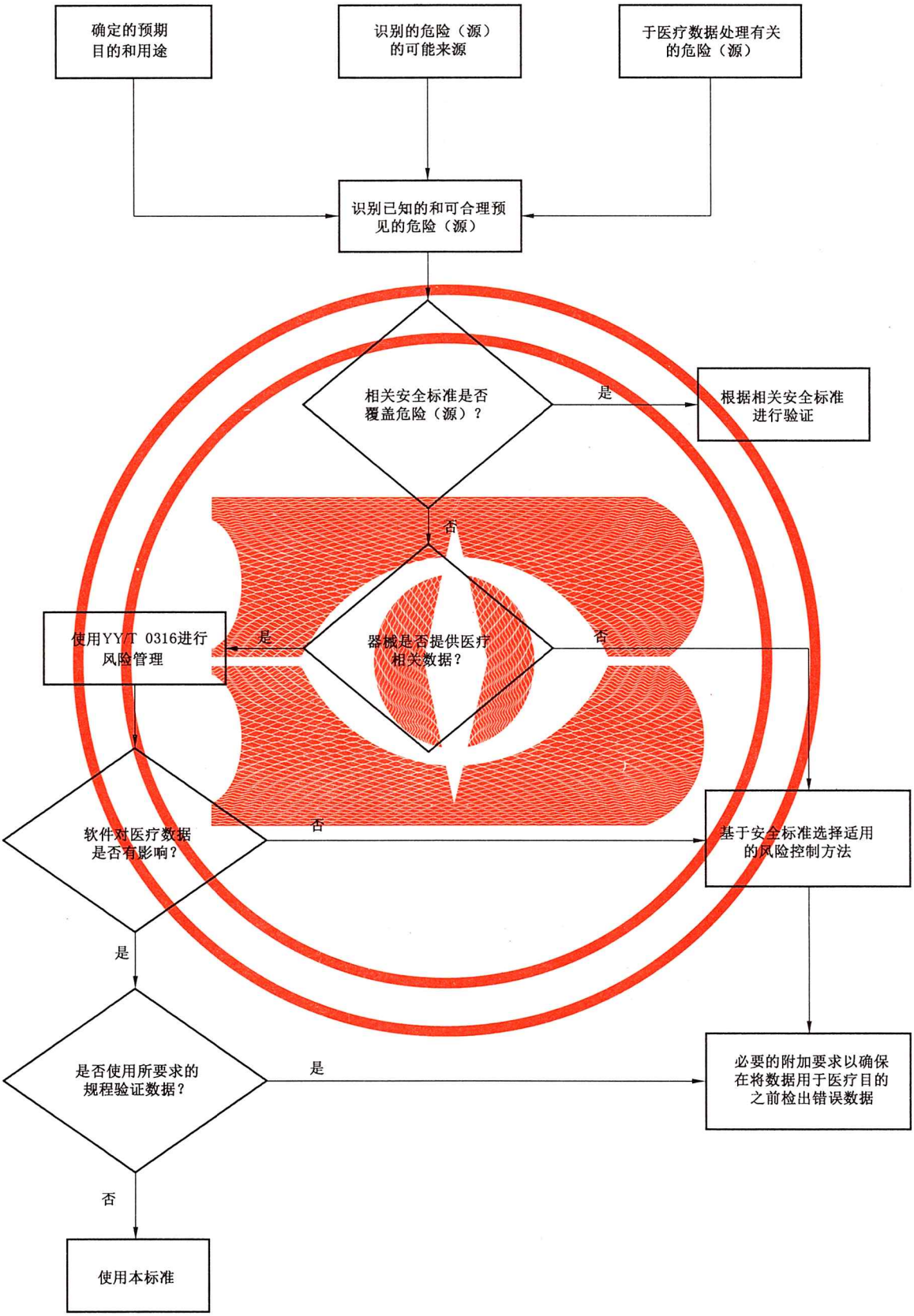


图 C.3　YY/T 0664 与 IEC 61010-1 联合应用

C.6 与 ISO/IEC 12207 的关系

本标准源于 ISO/IEC 12207[12] 的方法和概念，ISO/IEC 12207[12] 规定了对软件生存周期过程的通用要求，也就是不限于医疗器械。

本标准主要在以下几个方面不同于 ISO/IEC 12207，本标准：

- 不包括系统方面（的内容），如系统需求、系统体系结构和确认；
- 省略了一些被视作重复活动的过程，这些活动在其他地方为医疗器械形成了文件；
- 增加（安全）风险管理过程和软件发布过程；
- 将文档编制和验证支持过程纳入开发和维护过程；
- 把每个过程的过程实现和策划活动合并为开发和维护过程的一个单一活动；
- 按安全要求对需求进行分级；
- 不把过程明确地分类为主要或支持过程，也不像 ISO/IEC 12207 那样组合过程。

这些变化大部分由裁剪标准以满足医疗器械行业要求的愿望所驱使，通过以下几点实现：

- 主要关注安全方面的要求以及医疗器械风险管理标准 YY/T 0316；
- 选取在监管环境中有用的适当过程；
- 考虑到软件开发是涵盖于质量体系（覆盖 ISO/IEC 12207 的一些过程和要求）之中的；
- 降低抽象程度以使其易于使用。

本标准并不与 ISO/IEC 12207 相矛盾。ISO/IEC 12207 可在建立包括本标准要求的、构造良好的软件开发生存周期模型时提供帮助。

表 C.4 由 ISO/IEC JTC1/SC7 制定，表明本标准与 ISO/IEC 12207 的关系。

表 C.4 与 ISO/IEC 12207:2008 的关系

YY/T 0664 的过程		ISO/IEC 12207:2008	
活动	任务	过程	活动/任务
5 软件开发过程			
5.1 软件开发策划	5.1.1 软件开发计划	7.1.1 软件实现	7.1.1.3.1 软件实现策略 7.1.1.3.1.1 7.1.1.3.1.3 7.1.1.3.1.4 6.3.1.3.2 项目策划 6.3.1.3.2.1
	5.1.2 保持软件开发计划更新	6.3.2 项目评定与控制	6.3.2.3.2 项目控制 6.3.2.3.2.1
	5.1.3 引用系统设计和开发的软件开发计划	6.4.3 系统体系结构设计 6.4.5 系统集成 7.2.5 软件确认过程	6.4.3.3.1 建立体系结构 6.4.3.3.1.1 6.4.5.3.1 集成 6.4.5.3.1.1 7.2.5.3.1 过程实现 7.2.5.3.1.4
	5.1.4 软件开发标准、方法和工具的策划	7.1.1 软件实现	7.1.1.3.1 软件实现策略 7.1.1.3.1.3

表 C.4（续）

YY/T 0664 的过程		ISO/IEC 12207:2008	
活动	任务	过程	活动/任务
5.1 软件开发策划	5.1.5 软件集成和集成测试策划	7.1.6 软件集成	7.1.6.3.1 软件集成 7.1.6.3.1.1
	5.1.6 软件验证策划	7.2.4 软件验证 7.1.5 软件构建 7.1.6 软件集成 7.1.7 软件合格性测试	7.2.4.3.1 过程实现 7.2.4.3.1.4 7.2.4.3.1.5 7.1.5.3.1 软件构建 7.1.5.3.1.5 7.1.6.3.1 软件集成 7.1.6.3.1.5 7.1.7.3.1 软件合格性测试 7.1.7.3.1.3
	5.1.7 软件风险管理策划	6.3.4 风险管理过程	
	5.1.8 文档策划	7.2.1 软件文档管理	7.2.1.3.1 过程实现 7.2.1.3.1.1
	5.1.9 软件配置管理策划	7.2.2 软件配置管理 7.2.8 软件问题解决	7.2.2.3.1 过程实现 7.2.2.3.1.1 7.2.8.3.1 过程实现 7.2.8.3.1.1
	5.1.10 受控的支持项	6.2.2 基础设施管理	6.2.2.3.2 基础设施的建立 6.2.2.3.2.1 6.2.2.3.3 基础设施的维护 6.2.2.3.3.1
	5.1.11 验证前软件配置项的控制	7.2.2 软件配置管理	7.2.2.3.2 配置标识 7.2.2.3.2.1
5.2 软件需求分析	5.2.1 定义来自系统需求的软件需求并将其形成文件	6.4.3 系统体系结构设计	6.4.3.3.1 建立体系结构 6.4.3.3.1.1
	5.2.2 软件需求内容	7.1.2 软件需求分析	7.1.2.3.1 软件需求分析 7.1.2.3.1.1
	5.2.3 将风险控制措施纳入软件需求		
	5.2.4 医疗器械风险分析的再评价	无	无
	5.2.5 更新系统需求	7.1.2 软件需求分析	7.1.2.3.1 软件需求分析 7.1.2.3.1.1 a)和 b)
	5.2.6 验证软件需求	7.2.4 软件验证	7.2.4.3.2 验证 7.2.4.3.2.1

表 C.4（续）

YY/T 0664 的过程		ISO/IEC 12207:2008	
活动	任务	过程	活动/任务
5.3 软件体系结构设计	5.3.1 将软件需求转换为体系结构	7.1.3 软件体系结构设计	7.1.3.3.1 软件体系结构设计 7.1.3.3.1.1
	5.3.2 为软件项接口开发体系结构		7.1.3.3.1 软件体系结构设计 7.1.3.3.1.2
	5.3.3 规定未知来源软件项的功能和性能需求	无	无
	5.3.4 规定未知来源软件项所要求的系统硬件和软件	无	无
	5.3.5 判定风险控制所必需的隔离	无	无
	5.3.6 验证软件体系结构	7.1.3 软件体系结构设计	7.1.3.3.1 软件体系结构设计 7.1.3.3.1.6
5.4 软件详细设计	5.4.1 将软件体系结构细化为软件单元	7.1.4 软件详细设计	7.1.4.3.1 软件详细设计 7.1.4.3.1.1
	5.4.2 为每个软件单元开发详细设计		
	5.4.3 为接口开发详细设计		7.1.4.3.1 软件详细设计 7.1.4.3.1.2
	5.4.4 验证详细设计	7.1.4 软件详细设计	7.1.4.3.1 软件详细设计 7.1.4.3.1.7
5.5 软件单元的实现和验证	5.5.1 实现每个软件单元	7.1.5 软件构建	7.1.5.3.1 软件构建 7.1.5.3.1.1
	5.5.2 制定软件单元的验证过程	7.1.4 软件详细设计 7.1.5 软件构建	7.1.4.3.1 软件详细设计 7.1.4.3.1.5 7.1.5.3.1 软件构建 7.1.5.3.1.5
	5.5.3 软件单元的验收准则	7.1.5 软件构建	7.1.5.3.1 软件构建 7.1.5.3.1.5
	5.5.4 补充的软件单元验收准则	7.1.5 软件构建 7.2.4 软件验证	7.1.5.3.1 软件构建 7.1.5.3.1.2
	5.5.5 软件单元的验证	7.1.5 软件构建	7.1.5.3.1 软件构建 7.1.5.3.1.2
5.6 软件集成和集成测试	5.6.1 软件单元集成	7.1.6 软件集成	7.1.6.3.1 软件集成 7.1.6.3.1.2
	5.6.2 验证软件集成	7.1.6 软件集成 6.4.5 系统集成	7.1.6.3.1 软件集成 7.1.6.3.1.2 6.4.5.3.1 集成 6.4.5.3.1.2

表 C.4（续）

YY/T 0664 的过程		ISO/IEC 12207:2008	
活动	任务	过程	活动/任务
5.6 软件集成和集成测试	5.6.3 测试集成软件	7.1.7 软件合格性测试	7.1.7.3.1 软件合格性测试 7.1.7.3.1.1
	5.6.4 软件集成测试的内容	7.1.7 软件合格性测试	7.1.7.3.1 软件合格性测试 7.1.7.3.1.3
	5.6.5 评价软件集成测试规程	无	无
	5.6.6 进行回归测试	7.1.6 软件集成	7.1.6.3.1 软件集成 7.1.6.3.1.2
	5.6.7 集成测试记录的内容	7.1.6 软件集成	7.1.6.3.1 软件集成 7.1.6.3.1.2
	5.6.8 使用软件问题解决过程	7.2.4 软件验证	7.2.4.3.1 过程实现 7.2.4.3.1.6
5.7 软件系统测试	5.7.1 为软件需求建立测试项	7.1.6 软件集成 7.1.7 软件合格性测试	7.1.6.3.1 软件集成 7.1.6.3.1.4 7.1.7.3.1 软件合格性测试 7.1.7.3.1.1
	5.7.2 使用软件问题解决过程	7.2.4 软件验证	7.2.4.3.1 过程实现 7.2.4.3.1.6
	5.7.3 变更后再测试	7.2.8 软件问题解决	7.2.8.3.1 过程实现 7.2.8.3.1.1
	5.7.4 评价软件系统测试	7.1.7 软件合格性测试	7.1.7.3.1 软件合格性测试 7.1.7.3.1.3
	5.7.5 软件系统测试记录的内容	7.1.7 软件合格性测试	7.1.7.3.1 软件合格性测试 7.1.7.3.1.1
5.8 软件在系统级别应用的发布	5.8.1 确保软件验证的完成	6.4.9 软件运行 7.2.2 软件配置管理	6.4.9.3.2 运行的激活和审查 6.4.9.3.2.1 6.4.9.3.2.2 7.2.2.3.6 发布管理和交付 7.2.2.3.6.1
	5.8.2 将已知的剩余反常形成文件	7.2.2 软件配置管理 7.1.7 软件合格性测试	7.2.2.3.5 配置评价 7.2.2.3.5.1 7.1.7.3.1 软件合格性测试 7.1.7.3.1.3
	5.8.3 评价已知的剩余反常		
	5.8.4 将所发布的版本形成文件	7.2.2 软件配置管理过程	7.2.2.3.6 发布管理和交付 7.2.2.3.6.1
	5.8.5 将所发布软件的创建过程形成文件		
	5.8.6 确保活动和任务的完成		
	5.8.7 将软件归档		
	5.8.8 确保所发布软件的可靠交付		

表 C.4（续）

YY/T 0664 的过程		ISO/IEC 12207:2008	
活动	任务	过程	活动/任务
6 软件维护过程		6.4.10 软件维护过程	
6.1 建立软件维护计划		6.4.10 软件维护	无
6.2 问题和修改分析	6.2.1 形成文件并评价反馈	无	无
	6.2.1.1 监控反馈	6.4.10 软件维护	无
	6.2.1.2 形成文件并评价反馈		
	6.2.1.3 评价问题报告对安全的影响	6.4.10 软件维护	无
	6.2.2 使用软件问题解决过程	6.4.10 软件维护	无
	6.2.3 分析变更请求	6.4.10 软件维护	无
	6.2.4 批准变更请求	6.4.10 软件维护	无
	6.2.5 与用户和监管机构沟通	6.4.10 软件维护	无
6.3 修改的实施		无	无
	6.3.1 使用已建立的过程实施修改	6.4.10 软件维护	无
	6.3.2 修改后软件系统的再发布	7.2.2 软件配置管理	无
7 软件风险管理过程		6.3.4 风险管理过程 这是基于 ISO/IEC 16085 的。虽然有一些共性，但它并没有考虑处理医疗器械软件开发在风险管理方面的具体要求	
8 软件配置管理过程			
8.1 配置标识	8.1.1 建立标识配置项的方法	7.2.2 软件配置管理	无
	8.1.2 标识未知来源软件	无	无
	8.1.3 标识系统配置文档	7.2.2 软件配置管理	无
8.2 变更控制	8.2.1 批准变更请求	7.2.2 软件配置管理	无
	8.2.2 实施变更	6.4.10 软件维护	无
	8.2.3 验证变更	7.2.2 软件配置管理	无
	8.2.4 为变更的可追溯性规定方法		
8.3 配置状态报告		7.2.2 软件配置管理	无
9 软件问题解决过程			
9.1 编写问题报告		7.2.8 软件问题解决	无
9.2 调查问题		7.2.8 软件问题解决	无
9.3 通知相关方		7.2.8 软件问题解决	无

表 C.4（续）

YY/T 0664 的过程		ISO/IEC 12207:2008	
活动	任务	过程	活动/任务
9.4 使用变更控制过程		7.2.2 软件配置管理 6.4.10 软件维护	无
9.5 保持记录		7.2.8 软件问题解决	无
9.6 分析问题的趋势		7.2.8 软件问题解决	无
9.7 验证软件问题的解决		7.2.8 软件问题解决	无
9.8 测试文档的内容		ISO/IEC 12207:2008 中的所有测试任务都要求文档	无

C.7 与 GB/T 20438 的关系

有人提出一个问题：因为与安全关键软件的设计有关，本标准是否宜遵循 GB/T 20438 的原则？本标准实现安全的方法与 GB/T 20438 的方法有根本的不同。考虑到医疗器械的有效性，本标准认为与其使用有关的剩余风险是合理的。以下是对本标准观点的解释。

GB/T 20438 阐明三个主要问题：

a） 风险管理生存周期和生存周期过程；

b） 安全完整性等级的定义；

c） 为软件开发推荐技术、工具和方法，以及负责执行不同任务的人员的独立程度。

对问题 a），本标准通过对 YY/T 0316（医疗器械行业的风险管理标准）的规范性引用将其内容包含。此项引用的结果是采用 YY/T 0316 的方法开展风险管理活动，并作为医疗器械软件软件过程的组成部分。

对问题 b），本标准采取比 GB/T 20438 更简单的方法。后者将软件分级为四个“安全完整性水平”，而“安全完整性水平”是根据可靠性目标定义的。可靠性目标在风险分析后确定，风险分析则同时对软件失效引起伤害的严重度和概率进行量化。

基于失效引起的风险，本标准将软件分级定义为三个软件安全级别，从而简化了问题 b）。在分级之后，不同的软件安全级别要求不同的过程，其意图是进一步降低软件的失效概率（和/或严重度）。

对问题 c），本标准不阐述。鼓励本标准的读者利用 GB/T 20438 作为良好软件方法、技术和工具的来源，同时承认现在和将来的其他方法能够提供同样良好的结果。关于某项软件活动（如验证）的负责人员相对于其他软件活动（如设计）的负责人员的独立性问题，本标准不做推荐。特别地，本标准不要求有一个独立的安全评定人员，因为这是 YY/T 0316 的要求。

附 录 D
（资料性附录）
实施

D.1 引言

本附录对如何将本标准在制造商的过程中实施做了概述。同时也考虑到像 YY/T 0287[5] 等其他标准要求充分的和类似的过程。

D.2 质量管理体系

对于包含医疗器械软件的医疗器械制造商，本标准在 4.1 中要求建立质量管理体系（QMS）。同时本标准不要求质量管理体系必须通过认证。

D.3 评价质量管理过程

推荐借助制造商负责下的审核、检查或分析手段，评价已建立并形成文件的质量管理体系过程是否完整地覆盖了软件生存周期过程。识别到的任何差距都可以通过扩展质量管理过程得到弥补，也可对其单独描述。如果制造商已有现成的用于规范软件开发、验证和确认的过程描述，则也宜对其进行评价，以确定它们与本标准一致的程度。

D.4 将本标准的要求整合到制造商的质量管理过程

本标准可以通过调整或扩充已在质量管理体系中建立的过程，或整合新的过程来实施。本标准并不规定如何实施；制造商可用任何合适的方式实施。

当医疗器械软件由自身未建立形成文件的质量管理体系的“初始设备制造商（OEM）”或分包商开发时，制造商负责确保本标准中描述的过程得到适当实施。

D.5 用于未经质量管理体系认证的小型制造商的检查表

制造商宜确定软件的最高软件安全级别（A、B 或 C）。表 D.1 列出了本标准中描述的所有活动。对 YY/T 0287 的引用可能有助于确定其在质量管理体系中的对应条款。基于所要求的软件安全级别，制造商宜对照现有的过程评定所要求的每项活动。如果要求已经被覆盖，宜给出对相关过程描述的引用。

如果有不符之处，需要采取措施改进过程。

此表也可用于措施实施之后的过程评价。

表 D.1 用于未经质量管理体系认证的小型制造商的检查表

活动	YY/T 0287—2017 的有关章条号	现有程序是否覆盖？	如果是：引用	采取的措施
5.1 软件开发策划	7.3.2 设计和开发策划	是/否		
5.2 软件需求分析	7.3.3 设计和开发输入	是/否		

表 D.1（续）

活动	YY/T 0287—2017 的有关章条号	现有程序是否覆盖？	如果是：引用	采取的措施
5.3 软件体系结构设计		是/否		
5.4 软件详细设计		是/否		
5.5 软件单元的实现		是/否		
5.6 软件集成和集成测试		是/否		
5.7 软件系统测试	7.3.4 设计和开发输出 7.3.5 设计和开发评审	是/否		
5.8 软件在系统级别应用的发布	7.3.6 设计和开发验证 7.3.7 设计和开发确认	是/否		
6.1 建立软件维护计划	7.3.9 设计和开发更改的控制	是/否		
6.2 问题和修改分析		是/否		
6.3 修改的实施	7.3.6 设计和开发验证 7.3.7 设计和开发确认	是/否		
7.1 促成危险情况的软件分析		是/否		
7.2 风险控制措施		是/否		
7.3 风险控制措施的验证		是/否		
7.4 软件变更的风险管理		是/否		
8.1 配置标识	7.5.8 标识 7.5.9 可追溯性	是/否		
8.2 变更控制	7.5.8 标识 7.5.9 可追溯性	是/否		
8.3 配置状态报告		是/否		
9 软件问题解决过程		是/否		

参 考 文 献

[1] GB/T 19000—2016 质量管理体系 基础和术语(ISO 9000:2015,IDT)

[2] GB/T 19001—2016 质量管理体系 要求(ISO 9001:2015,IDT)

[3] GB/T 20157—2006 信息技术 软件维护(ISO/IEC 14764:1999,IDT)

[4] GB/T 20438.3—2017 电气/电子/可编程电子安全相关系统的功能安全 第3部分:软件要求(IEC 61508-3:2010,IDT)

[5] YY/T 0287—2017 医疗器械 质量管理体系 用于法规的要求(ISO 13485:2016,IDT)

[6] IEC 60601-1:2005+IEC 60601-1:2005/AMD1:2012 Medical Electrical Equipment—Part 1: General requirements for basic safety and essential performance

[7] IEC 60601-1-4:1996+IEC 60601-1-4:1996/AMD1:1999 Medical Electrical Equipment—Part 1-4:General requirements for safety—Collateral standard:Programmable electrical medical systems (withdrawn)

[8] IEC 60601-1-6 Medical Electrical Equipment—Part 1-6:General requirements for basic safety and essential performance—Collateral Standard—Usability

[9] IEC 61010-1:2010 Safety Requirements for electrical equipment for measurement, control and laboratory use—Part 1:General requirements

[10] IEC 62366-1:2015 Medical devices—Part 1: Application of usability engineering to medical devices

[11] IEC 82304-1:2016 Healthcare software systems—Part 1:General requirements

[12] ISO/IEC 12207:2008 Systems and software engineering—Software life cycle processes

[13] ISO/IEC 15504-5:2012 Information technology—Process assessment—Part 5: An exemplar software life cycle process assessment model

[14] ISO/IEC 25010:2011 Systems and software engineering—Systems and software Quality Requirements and Evaluation (SQuaRE)—System and software quality models

[15] ISO/IEC 33001:2015 Information technology—Process assessment—Concepts and terminology

[16] ISO/IEC 33004:2015 Information technology—Process assessment—Requirements for process reference, process assessment and maturity models

[17] ISO/IEC/IEEE 90003:2018 Software engineering—Guidelines for the application of ISO 9001:2015 to computer software

[18] ISO/IEC Guide 51:2014 Safety aspects—Guidelines for their inclusion in standards

[19] IEEE 610.12:1990 IEEE Standard Glossary of Software Engineering Terminology

[20] IEEE 1044:2009 IEEE Standard Classification for Software Anomalies

[21] U.S. Department Of Health and Human Services. Food and Drug Administration,Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices, May 11, 2005.

[22] U.S. Department Of Health and Human Services. Food and Drug Administration, General Principles of Software Validation; Final Guidance for Industry and FDA staff.January 11,2002.

中华人民共和国医药
行业标准
医疗器械软件 软件生存周期过程
YY/T 0664—2020
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)68533533 发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 4.25 字数 122 千字
2020年11月第一版 2020年11月第一次印刷
*
书号:155066·2-35343 定价 68.00 元

YY/T 0664-2020