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

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。

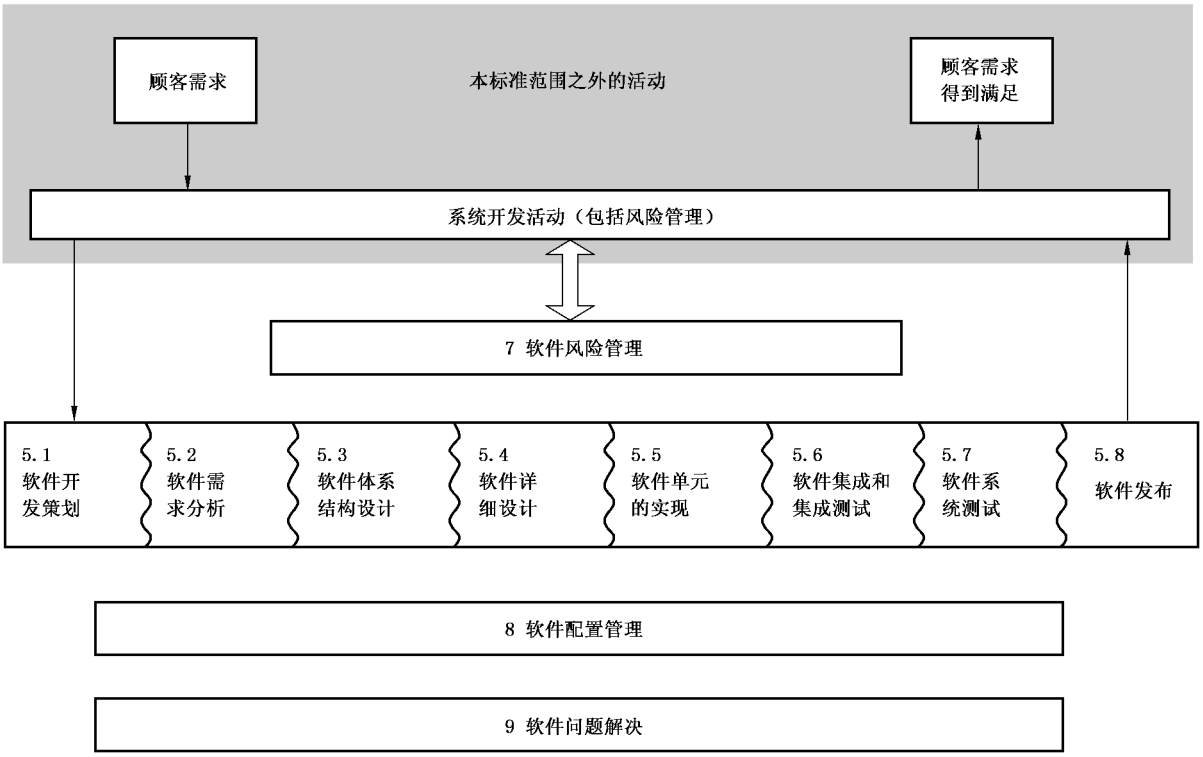

图 1　软件开发过程和活动图示

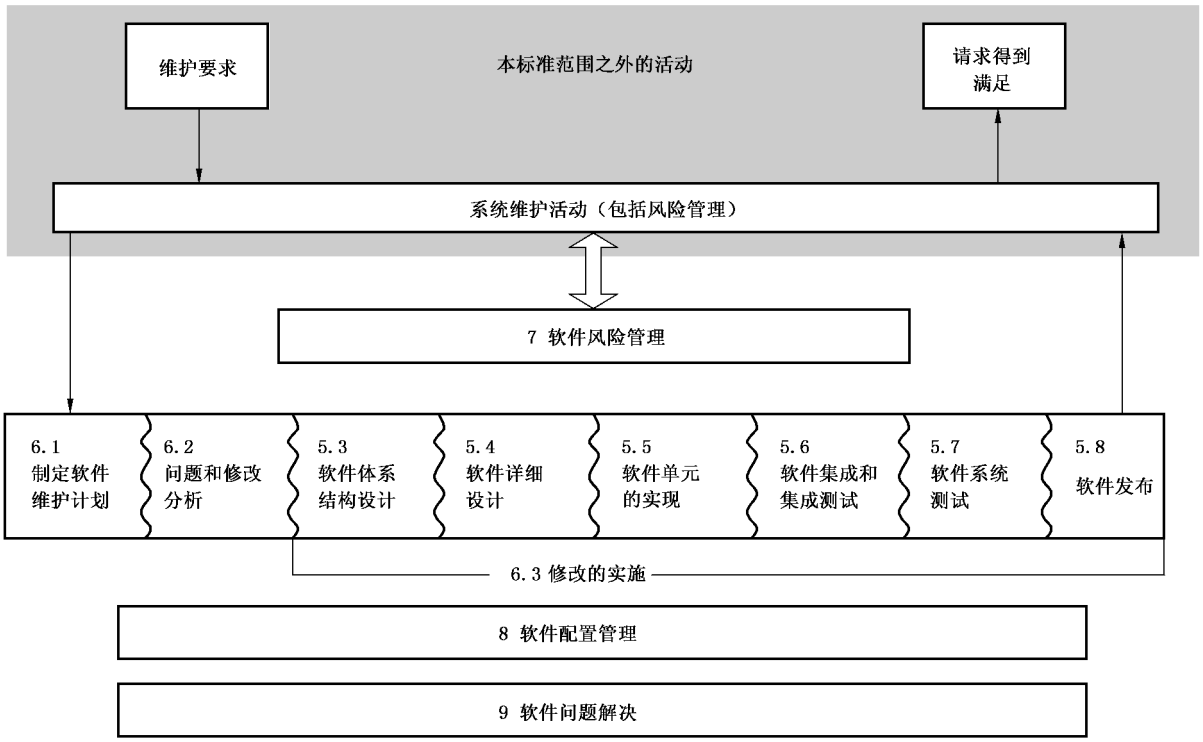

图 2　软件维护过程和活动图示

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[11]。

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[6]，IEC 82304-1[11]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