ICS 11.040
C 30

YY

中华人民共和国医药行业标准

YY/T 0664—2008/IEC 62034:2006

医疗器械软件　软件生存周期过程

Medical device software—Software life cycle processes

(IEC 62034:2006,IDT)

2008-04-25 发布　　2009-06-01 实施

国家食品药品监督管理局　发布

目　次

前　言

本标准等同采用 IEC 62304:2006《医疗器械软件　软件生存周期过程》(英文版)。

IEC 62304:2006《医疗器械软件　软件生存周期过程》给出了在第 3 章中定义的术语索引,本标准将该索引删除。

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。

IEC 62304:2006《医疗器械软件　软件生存周期过程》(英文版)中的术语和附录 C 部分引用 ISO 14971:2000条款,由于 ISO 14971:2007 版已经发布,本标准中引用 YY/T 0316—2008/ISO 14971:2007 的相应部分。

本标准的附录 A、附录 B、附录 C 和附录 D 均为资料性附录。

本标准由国家食品药品监督管理局医疗器械司提出。

本标准由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:医疗器械质量管理和通用要求标准化技术委员会、北京国医械华光认证有限公司。

本标准主要起草人:秦树华、陈志刚、米兰英、武俊华、李慧民。

引　言

软件往往是医疗器械技术的一个组成部分。建立包括软件的医疗器械的安全性和有效性，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完成预期目的。

本标准为医疗器械软件的安全设计和维护提供了包括必要活动和任务的生存周期过程的框架。本标准为每个生存周期过程规定了要求。每个生存周期过程进一步划分为一组活动，多数活动又进一步划分为一组任务。

作为主要的基础，设想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。国际标准 YY/T 0316 很好地描述了风险管理过程。因此本标准只是利用规范性引用文件 YY/T 0316 这个有利条件，对软件需要增加一些较小补充的风险管理要求，特别是与危害有关的软件影响因素的识别。这些要求汇总并纳入第 7 章作为软件风险管理过程。

在风险管理过程的危害判定活动中，确定软件是否为危害的影响因素。在确定软件是否是影响因素时，需要考虑可能由软件间接造成的危害（例如：提供可能导致给予不当治疗的误导信息）。使用软件来控制风险的决策，在风险管理过程的风险控制活动中做出。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。这些活动见图 1，并在第 5 章中描述。因为现场的许多事故是和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。软件维护过程被认为和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。见图 2 和第 6 章的描述。

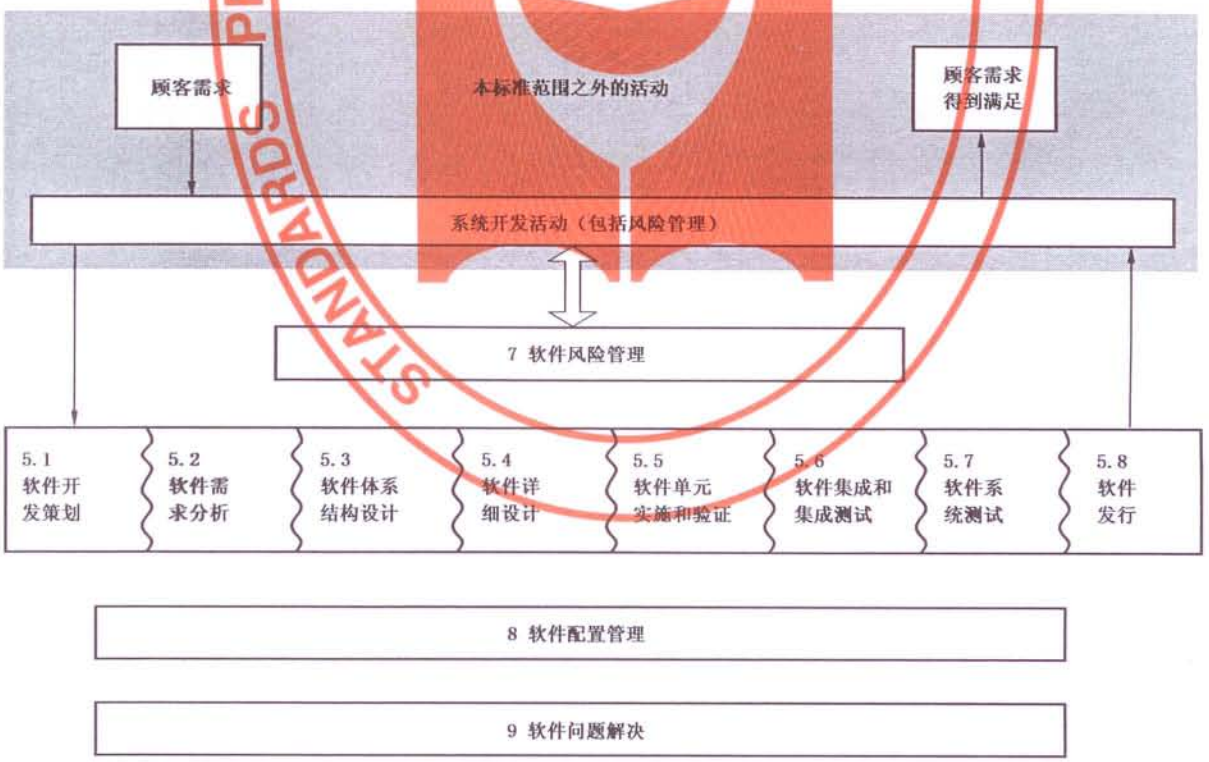


图 1　软件开发过程和活动概示

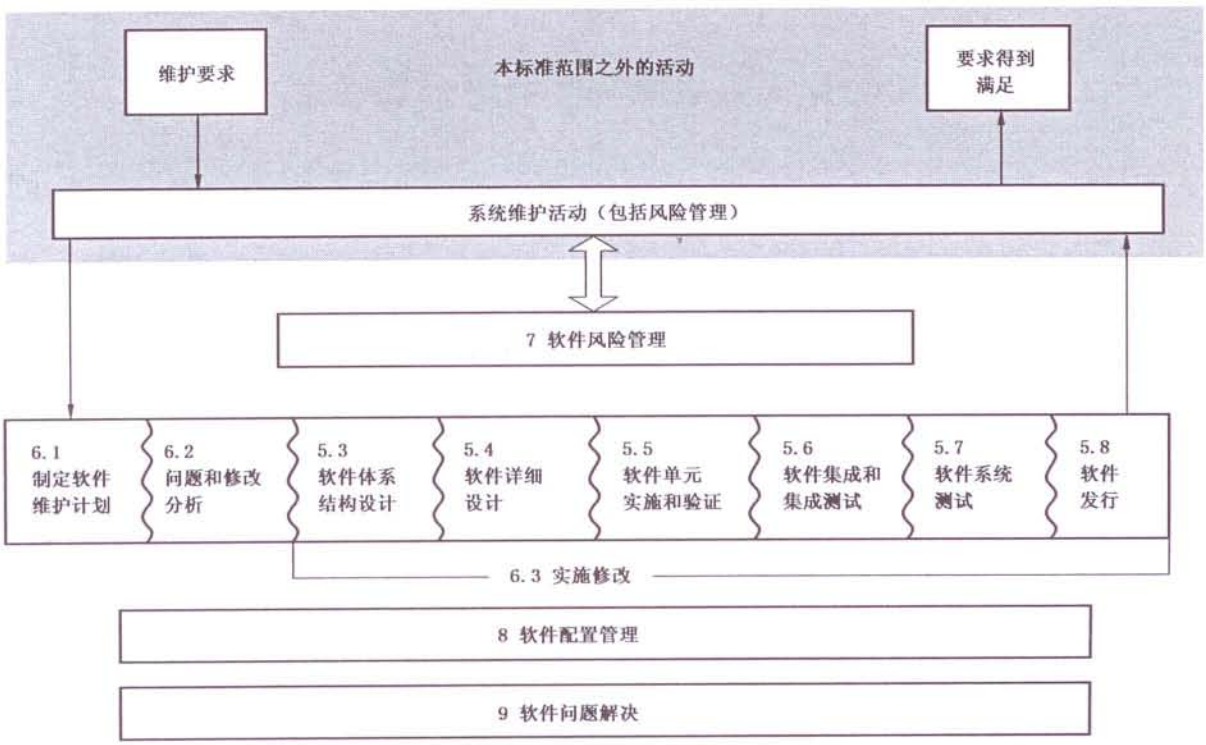


图 2　软件维护过程和活动概示

本标准确定开发安全的医疗器械软件必需考虑的两个补充过程，即软件配置管理过程（第 8 章）和软件问题解决过程（第 9 章）。

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、活动或任务以确定符合本标准。

本标准并不规定要形成的文件的名称、格式或明确的内容。本标准要求任务文件，但如何组合编排这些文件的决定留给标准的使用者来做。

本标准并不规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 提供本标准各章的理由说明。附录 B 提供本标准规定的指南。

对于本标准：

- “应（shall）”意思是为符合本标准，符合一项要求是强制性的；
- “应当（should）”意思是为符合本标准，符合一项要求是推荐性的但不是强制性的；
- “可（may）”用于描述达到符合一项要求的许可方式；
- “建立（establish）”意思是规定、形成文档和实施；和
- 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性。

医疗器械软件　软件生存周期过程

1　范围

1.1　*目的

本标准规定了**医疗器械软件**的生存周期要求。在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。

当软件本身是**医疗器械**，或当软件是最终**医疗器械**的嵌入部分或组成部分时，本标准适用于该**医疗器械软件**的开发和维护。

本标准不覆盖**医疗器械**的确认和最终发行，即使当该**医疗器械**完全由软件组成时。

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。本标准和其他相关标准之间的关系见附录 C 所示。

1.4　符合性

符合本标准意指按照软件安全性级别，实施在本标准中确定的所有**过程**、**活动**和**任务**。

注：对每项要求所赋予的软件安全性级别在标准要求之后的正文中确定。

用检查本标准所要求的所有文档（包括**风险管理**文档和对软件安全性级别所要求的**过程**、**活动**和**任务**的评定）的方法来确定符合性。见附录 D。

注 1：此种评定可以由内部的或外部的审核来实现。

注 2：即使规定了要完成的**过程**、**活动**和**任务**，实施这些**过程**和执行这些**活动**和**任务**的方法是灵活的。

注 3：在任何包含“适当时（as appropriate）”的要求没有完成时，为说明理由而形成文档对于本评定是必要的。

注 4：本标准中用术语“符合（compliance）”的地方，GB/T 8566 中用术语“符合（conformance）”。

2　*规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

YY/T 0316　医疗器械　**风险管理**对医疗器械的应用（YY/T 0316—2008，ISO 14971:2007，IDT）

3　*术语和定义

下列术语和定义适用于本标准。

3.1

活动　activity

一组中单个或多个相互关联或相互作用的**任务**。

3.2

异常　anomaly

任何偏离于所预期的需求说明书、设计文件、标准等的情况，或任何偏离于一些人员的感知或经验的情况。**异常**可能在（但不限于）对**软件产品**或适用文件进行评审、测试、分析、编辑或使用**过程**中发现。

[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

更改要求 change request

对软件产品进行更改所做的形成文档的说明

3.5

配置项 configuration item

能在给定的基准点上单独标识的实体。

注：基于 GB/T 8566—2007，定义 3.6。

3.6

交付物 deliverable

一项活动或任务的要求结果或输出(包括文件)。

3.7

评价 evaluation

系统地确定一个实体项目满足其规定准则的程度。

[GB/T 8566—2007，定义 3.9]

3.8

损害 harm

对人体健康的实际伤害或损坏，或是对财产或环境的损坏。

[ISO/IEC 导则 51:1999，定义 3.3]

3.9

危害 hazard

损害的潜在源。

[ISO/IEC 导则 51:1999，定义 3.5]

3.10

制造商 manufacturer

在上市和/或投入服务前，对医疗器械的设计、制造、包装或作标记、系统的装配或者改装医疗器械负有责任的自然人或法人，不管上述工作是由他自己或由第三方代其完成。

[YY/T 0316—2008，定义 2.8]

3.11

医疗器械 medical device

制造商的预期用途是为下列一个或多个特定目的用于人类的，不论单独使用或组合使用的仪器、设备、器具、机器、用具、植入物、体外试剂或校准物、软件、材料或者其他相似或相关物品。

这些目的是：

——疾病的诊断、预防、监护、治疗或者缓解；

——损伤的诊断、监护、治疗、缓解或者补偿；

——解剖或生理过程的研究、替代、调节或者支持；

——支持或维持生命；

——妊娠控制；

——医疗器械的消毒；

——通过对取自人体的样本进行体外检查的方式来提供医疗信息。

其作用于人体体表或体内的主要设计作用不是用药理学、免疫学或代谢的手段获得，但可能有这些手段参与并起一定辅助作用。

注1：本定义由全球协调工作组(GHTF)制定。见参考目录[15]。(YY/T 0287—2003)

[YY/T 0287—2003，定义 3.7]

注2：每个国家用于法规的定义中会有一些区别。

3.12

医疗器械软件 medical device software

旨在包括在被开发的**医疗器械**内的已开发的**软件系统**，或者预期本身用作**医疗器械**而开发的**软件系统**。

3.13

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、不适当或是违反规范的**软件产品**的实际或潜在特性的记录。

注1：本标准不要求每个**问题报告**都导致**软件产品**更改。在有误解、错误或可忽略事件时，**制造商**可拒绝**问题报告**。

注2：**问题报告**可以涉及已发行的**软件产品**或仍在开发中的**软件产品**。

注3：本标准要求**制造商**对涉及已发行产品的**问题报告**，实施额外的决策制定步骤(见第6章)，以确保管理**活动**的识别和实施。

3.14

过程 process

一组将输入转化为输出的相互关联或相互作用的**活动**。

[GB/T 19000:2000，定义 3.4.1]

注：术语“**活动**”包括资源的使用。

3.15

回归测试 regression testing

要求用于确定**系统**组件的更改没有对功能性、可靠性或性能产生不良影响，并且没有引入另外的缺陷的测试。

[ISO/IEC 90003:2004，定义 3.11]

3.16

风险 risk

损害严重度和其发生概率的结合。

[ISO/IEC 导则 51:1999 定义 3.2]

3.17

风险分析 risk analysis

系统运用可得资料，判定**危害**并估计**风险**

[ISO/IEC 导则 51:1999 定义 3.10]

3.18

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—2008 定义 2.19]

3.19

风险管理 risk management

用于**风险**分析、**评价**、控制和监视工作的管理方针、程序及其实践的**系统**运用。

[YY/T 0316—2008 定义 2.22]

3.20

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—2008 定义 2.23]

3.21

安全性 safety

免除于不可接受的**风险**

[ISO/IEC 导则 51:1999 定义 3.1]

3.22

保密安全 security

对信息和数据的保护,这样,未经授权的人员或**系统**不能阅读或修改它们,不能拒绝授权人员或**系统**对它们的访问。

[GB/T 8566—2007 定义 3.25]

3.23

严重伤害 serious injury

直接或间接导致下列结果的伤害或疾病:

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,或

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伤。

注:永久性**损害**意味着人体结构或功能的不可恢复的**损害**或伤害,微不足道的**损害**或伤害除外。

3.24

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

跨越软件从定义需求到制作发行这一时间段的概念结构,其:

——识别包括在**软件产品**开发中的**过程**、**活动**和**任务**,

——描述**活动**和**任务**之间的顺序和依赖关系,和

——识别经**验证**的规定**交付物**完整性的里程碑。

注:基于 GB/T 8566—2007,定义 3.11。

3.25

软件项 softw are item

计算机程序中任一可识别的部分。

[ISO/IEC 90003:2004,定义 3.14,经修正的]

注:三个术语标明软件分解。顶级是**软件系统**。底级是不能进一步分解的**软件单元**。包括顶层和底层的所有组合层面,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**的定义和大小是**制造商**的责任。

3.26

软件产品 softw are product

一组计算机程序、规程以及可能的相关文档和数据。

[GB/T 8566—2007 定义 3.26]

3.27

软件系统 softw are system

编制以完成特定功能或一组功能的**软件项**的整合体。

3.28

软件单元 softw are unit

不可再分的**软件项**。

注:**软件单元**可用于软件配置管理或测试的目的。

3.29

未知来源软件(缩写 SOUP)　SOUP software of unknown provenance (acronym)

已经开发且通常可得到的,并且不是为用以包含在**医疗器械**内而开发的**软件项**(也通称为成品**软件**),或以前开发的、不能得到其开发**过程**足够记录的软件。

3.30

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。

[GB/T 8566—2007,定义 3.31]

3.31

任务　task

需要做的单项工作。

3.32

可追溯性　traceability

在开发**过程**中的两个或多个产品间能建立关联的程度。

[IEEE 610.12:1990]

3.33

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:"已验证"一词用于表示相应的状态。

[GB/T 19000—2000,定义 3.8.4]

注 2:在设计和开发中,**验证**涉及检查给定**活动**的结果以确定该项**活动**符合规定要求的**过程**。

3.34

版本　version

某一配置项的已标识了的实例。

注 1:**软件产品**某**版本**的修改产生一个新**版本**,但要求软件配置管理**活动**。

注 2:基于 GB/T 8566—2007,定义 3.37。

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和适用的法规要求的**医疗器械软件**。

注 1:可通过利用符合下列要求的质量管理体系,证实此能力:

——YY/T 0287[7],或

——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:适用于**软件**的质量管理体系要求的指南见 ISO/IEC 90003[11]。

4.2　*风险管理

制造商应使用符合 YY/T 0316 的**风险管理过程**。

4.3　*软件的安全性级别

a)　**制造商**应按照**软件系统**引起的**危害**对于患者、操作者或其他人员的可能影响,赋予每个**软件系统**一个软件安全性级别(A、B 或 C)。

基于如下的严重度,应初步赋予软件相应安全性级别:

A 级:不可能对健康有伤害或损坏。

B 级:可能有**不严重的伤害**。

C级：可能死亡或严重伤害。

如果危害可能由软件系统未能象规定的那样起作用引起，则此项失效的概率应假定为100%。

如果软件失效引起死亡或严重伤害的风险，随后由硬件风险控制措施降低到可接受水平（如YY/T 0316所规定），或者降低失效后果或者降低由失效引起的死亡或严重伤害的概率，软件安全性级别可从C降低到B；如果软件失效引起的非严重伤害风险同样通过硬件风险控制措施降低到可接收水平，软件安全性级别可从B降低到A。

b) 制造商应依据风险控制措施所控制的危害的可能影响，对实施风险控制措施起作用的每个软件系统赋予一个软件安全性级别。

c) 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性级别形成文档。

d) 当一个软件系统分解为软件项，及当一个软件项又进一步分解为几个软件项时，此类软件项应继承原软件项（或软件系统）的软件安全性级别，除非制造商以文件形式证明分类为不同的安全性级别的理由。此类理由说明应解释新的软件项是如何被分开的，以便可对其另行分级。

e) 如果以分解方式产生的软件项的安全级别和其源软件项不同，制造商应对每个软件项的软件安全级别形成文档。

f) 为符合本标准，无论特定级别的软件项是否需要一个过程，此过程是否有必要应用于一组软件项，制造商应使用此组中最高级别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有使用较低级别的理由的说明文件。

g) 对每个软件系统，在赋予软件安全性级别以前，均应应用C级要求。

注：在随后的要求中，对该项要求必须实施的软件安全性级别，以[……级]形式标示于该要求之后。

5 软件开发过程

5.1 软件开发策划

5.1.1 软件开发计划

制造商应制定一项（或多项）软件开发计划，以便实施适合于所开发软件系统的范围、规模和软件安全性级别的软件开发过程的活动。在一个（或多个）计划中应完整地规定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（包括文件）；

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

d) 软件配置和更改管理，包括未知来源软件配置项和用于支持开发的软件；和

e) 在生存周期每个阶段的软件产品、交付物和活动中发现的用于处理问题的软件问题解决方案。

[A、B、C级]

注1：软件开发生存周期模型可依照软件系统每个软件项的软件安全性分级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。其意图并不意味应当使用特定的生存周期模型。

注3：本标准中其他过程和开发过程分开描述。这并不意味着它们必须作为单独的活动和任务来实施。其他过程的活动和任务可以整合到开发过程中。

注4：软件开发计划可以参考现有的过程或规定新过程。

注5：软件开发计划可以整合到一个全系统的开发计划中。

5.1.2 保持软件开发计划更新

在适当时，制造商应在开发进行的同时更新计划。

[A、B、C级]

5.1.3 引用系统设计和开发的软件开发计划

a) **制造商**应在软件开发计划中引用**系统**需求，作为软件开发的输入。

b) **制造商**应在软件开发计划中包括或引用用于协调软件开发和为满足 4.1 必需的设计开发确认的规程。

[A、B、C 级]

注：如果**软件系统**是一个独立的**系统**(仅为软件的器械)，在**软件系统**需求和**系统**需求之间也许没有什么区别。

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和 C 级**软件项**的开发有关的：

a) 标准；

b) 方法，和；

c) 工具。

[C 级]

5.1.5 软件集成和集成测试策划

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 SOUP)并在集成过程中完成测试。

[B、C 级]

注：将集成测试和**软件系统**测试结合在一个单一的计划和一组**活动**中是可接受的。

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) 需要**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；和

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实施**软件风险管理过程**的**活动**和**任务**的计划，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**中所形成文档的信息。对每个已识别的文档或文档类型，应包括或引用如下信息：

a) 标题、名称或命名约定；

b) 目的；

c) 文件的预期阅读者；和

d) 开发、评审、批准和修改的程序和职责。

[A、B、C 级]

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) 受控项目的级别、型式、类别或清单；

b) 软件配置管理**活动**和**任务**；

c) 负责进行软件配置管理和**活动**的组织；

d) 它们和其他组织的关系，诸如软件开发或维护；

e) 当将这些项目处于配置控制之下时；和

f) 何时应用问题解决过程。

[A、B、C 级]

5.1.10 受控的支持项

受控项应包括用于医疗器械软件开发并对其有影响的工具、项目或设置。

[B、C 级]

注：此类项目的示例包括编译器/汇编器版本，生成文件，批文件和特定的环境设置。

5.1.11 验证前的软件配置项的控制

制造商应计划在验证软件配置项之前，使其处于形成文档的配置管理控制之下。

[B、C 级]

5.2 * 软件需求分析

5.2.1 由系统需求确定软件需求并形成文档

对每个医疗器械软件系统，制造商应从系统层面需求中确定软件系统需求并形成文档。

[A、B、C 级]

注：如果软件系统是一个独立的系统(仅为软件的器械)，在软件系统需求和系统需求之间也许没有什么区别。

5.2.2 软件需求内容

在适用于医疗器械软件，制造商应在软件需求中包括：

a) 功能和能力需求；

注 1：示例包括：

——性能(如软件的目的、计时要求)；

——物理特征(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)，和；

——升级或多种未知来源软件或其他器械版本所需的兼容性。

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、字母数字混编的、格式)；

——范围；

——限制，和；

——默认值。

c) 软件系统和其他系统之间的接口；

d) 软件控制的报警、警告和操作者信息；

e) 保密安全需求

注 3：示例包括：

——有关危及敏感信息的需求；

——身份验证；

——授权；

——审核跟踪，和；

——沟通的完整性。

f) 对人为错误敏感的适用性工程要求和培训；

注 4：示例包括有关以下内容的要求：

——对人工操作的支持；

——人机交互；

——对人员的约束，和；

——需要引起重视的区域。

注 5：有关适用性工程要求的信息见 IEC 60601-1-6。

g) 数据定义和数据库需求；

注6：示例包括：

——格式；

——配合；

——功能。

h) 对已交付的医疗器械软件在操作和维护的一个或多个地点的安装和验收要求；

i) 与操作和维护方法有关的要求；

j) 要编制的用户文档；

k) 用户维护要求；和；

l) 法规要求。

[A、B、C级]

注7：所有这些要求在软件开发之初可能得不到。

注8：GB/T 16261.1[8]提供可能对确定软件需求有用的质量特性信息。

5.2.3 在软件需求中包括风险控制措施

制造商应将在软件中所实施的对于硬件失效和潜在软件缺陷的风险控制措施包括在适合于医疗器械软件的要求中。

[B、C级]

注：这些要求在软件开发之初可能得不到，并且在软件设计过程中可以更改，风险控制措施可进一步确定。

5.2.4 医疗器械风险分析的再评价

制造商应在制定并适当更新软件需求时，对医疗器械风险分析进行再评价。

[A、B、C级]

5.2.5 更新系统需求

制造商应确保对现有的需求(包括系统需求)进行再评价和适当时更新，作为软件需求分析活动的结果。

[A、B、C级]

5.2.6 验证软件需求

制造商应对软件需求进行验证并形成文档：

a) 实施包括有关风险控制在内的系统需求；

b) 需求不互相矛盾；

c) 避免使用含糊不清的术语表示；

d) 用表述的术语来制定测试准则和实施测试，以确定是否满足测试准则；

e) 可以进行唯一性标识；和；

f) 对于系统要求或其他来源是可追溯的。

[A、B、C级]

注：本标准不要求使用正式的规格语言。

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描述软件结构和标明软件项的形成文档的体系结构。

[B、C级]

5.3.2 为软件项接口开发体系结构

制造商应为软件项和软件项外的组件(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形成文档。

[B、C级]

5.3.3 规定 SOUP 项目的功能和性能需求

如果软件项被识别为 SOUP，制造商应规定 SOUP 项目预期用途所必需的功能和性能需求。

[B、C 级]

5.3.4 规定 SOUP 项目所要求的系统硬件和软件

如果软件项被识别为 SOUP，制造商应规定为支持 SOUP 项目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 判定风险控制所必需的隔离

制造商应判定风险控制所必要的软件项之间的隔离，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。隔离的有效性可以由处理器间没有共同资源来保证。

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档：

a) 软件体系结构实现包括与风险控制有关的系统和软件需求；

b) 软件体系结构能支持软件项间和软件项与硬件之间的接口；和

c) 医疗器械体系结构支持任何 SOUP 项目的正常运行。

[B、C 级]

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

制造商应细化软件体系结构直至其表现为软件单元。

[B、C 级]

5.4.2 为每个软件单元开发详细设计

制造商应对软件项的每个软件单元开发详细设计并形成文档。

[C 级]

5.4.3 为接口开发详细设计

制造商应对软件单元和外部组件(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开发详细设计并形成文档。

[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档：

a) 实现软件体系结构；和

b) 不和软件体系结构相矛盾。

[C 级]

5.5 * 软件单元的实现和验证

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 制定软件单元的验证过程

制造商应为验证每个软件单元制定策略、方法和规程。在以测试验证时，应评价测试程序的正确性。

[B、C 级]

注：将集成测试和软件系统测试结合进一项单个计划和一组活动是可接受的。

5.5.3 软件单元的验收准则

适当时，在集成为较大的软件项之前，制造商应为软件单元制定验收准则，并确保软件单元符合验收准则。

[B、C 级]

注：验收准则示例：

——软件编码是否实现了包括风险控制措施在内的要求？

——软件编码是否和软件单元的详细设计所形成文档的接口有矛盾？

——软件编码是否符合编程规程或编码标准？

5.5.4 补充的软件单元验收准则

当在设计中出现时，制造商应包括下列各项（适当时）的补充验收准则：

a) 合适的事件序列；

b) 数据和控制流；

c) 计划的资源配置；

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；和；

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的验证并将结果形成文档。

[B、C 级]

5.6 * 软件集成和集成测试

5.6.1 软件单元集成

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

制造商应按照集成计划（见 5.1.5）对软件集成的下列方面进行验证和记录：

a) 软件单元已经集成到软件项和软件系统中；和

b) 系统的硬件项、软件项和人工操作的支持（例如：人机接口、联机帮助菜单、语音识别、声控）已经集成进系统中。

[B、C 级]

注：只是对各项按照计划集成进行验证，不对按预期实施进行验证。验证很可能以某种形式的检验实现。

5.6.3 测试集成的软件

制造商应按照集成计划（见 5.1.5）对集成的软件项进行测试并将结果形成文档。

[B、C 级]

5.6.4 集成测试内容

对于软件集成测试，制造商应说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：

——要求的软件功能性；

——风险控制措施的实施；

——规定计时和其他活动状态；

——内部和外部接口的规定功能；和；

——在包括可预见误用在内的异常条件下测试。

注2：将集成测试和软件系统测试结合进一项单一计划和一组活动是可接受的。

5.6.5 验证集成测试规程

制造商应评价集成测试规程的正确性。

[B、C级]

5.6.6 进行回归测试

当软件项已集成时，制造商应进行适当的回归测试，以证实未将缺陷引入到原先集成的软件中。

[B、C级]

5.6.7 集成测试记录的内容

制造商应：

a) 将测试结果形成文档(通过/未通过和异常清单)；

b) 保留充分的记录，以使测试能够重复进行；和

c) 标明测试者。

[B、C级]

注：要求b)可以通过保留如下内容来实现，例如：

——表示所要求的操作和预期结果的测试情况的详细说明；

——设备的记录；

——用于测试的测试环境(包括软件工具)的记录。

5.6.8 软件问题解决过程的使用

制造商应将软件集成和集成测试时发现的异常输入软件问题解决过程中。

[B、C级]

注：见第9章。

5.7 * 软件系统测试

5.7.1 为软件需求制定测试项

制造商应为软件系统测试制定并实施一组测试，表达为输入触发、预期输出、通过/未通过准则和规程，以便覆盖全部的软件需求。

[B、C级]

注1：将集成测试和软件系统测试结合成一项单一的计划和一组活动是可接受的。在较早的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，也可进行组合需求的测试，特别是在需求之间存在相关性的情况下。

5.7.2 使用软件问题解决过程

制造商应将在软件系统测试中发现的异常输入到软件问题解决过程。

[B、C级]

5.7.3 更改后再测试

当更改是在软件系统测试中做出时，制造商应：

a) 重复测试、进行改进测试或进行补充测试，适当时验证纠正问题时所做更改的有效性；

b) 进行适当的测试，以证实没有引入非预期的副作用；和

c) 实施7.4中规定的有关风险管理活动。

[B、C级]

5.7.4 验证软件系统测试

制造商应验证：

a) 所用的验证策略和测试规程是适当的；

b) 软件系统测试规程可追溯到软件需求；

c) 所有的软件需求都已测试过或以其他方式验证过；和

d) 测试结果满足要求的通过/未通过准则。

[B、C 级]

5.7.5 软件系统测试记录内容

制造商应：

a) 将测试结果形成文档(通过/未通过和异常清单)

b) 保存充分的记录，以使测试可重复

c) 标明测试者。

[B、C 级]

注：要求 b)可以通过保留如下内容来实现，例如：

——表示要求措施和预期结果的测试情况的详细说明；

——设备记录；

——测试环境(包括软件工具)的记录。

5.8 * 软件发行

5.8.1 确保软件验证的完成

在软件发行之前，制造商应确保软件验证已经完成，已对其结果进行了评价。

[B、C 级]

5.8.2 将已知的剩余异常形成文档

制造商应将所有已知的剩余异常形成文档。

[B、C 级]

5.8.3 评价已知的剩余异常

制造商应确保所有已知的剩余异常情况已被评价，从而确保其不会构成不可接受的风险。

[B、C 级]

5.8.4 将发行的版本形成文档

制造商应将即将发行的软件产品版本形成文档。

[A、B、C 级]

5.8.5 将已发行软件的创建过程形成文档

制造商应将用于创建已发行软件的规程和环境形成文档。

[B、C 级]

5.8.6 确保活动和任务的完成

制造商应确保所有的活动和任务连同所有相关文件编制是完整的。

[B、C 级]

5.8.7 软件归档

制造商应将下列内容归档：

a) 软件产品和配置项；和

b) 文档。

最小存档时间确定为不短于制造商规定的器械寿命期或有关法规要求规定的时间。

[B、C 级]

5.8.8 保证软件发行的可重复性

制造商应建立规程，以确保已发行的软件产品能可靠地交付到使用地点，而没有讹误的或未授权的更改。这些规程应说明包含软件产品的媒介的生产和处理情况，适当时，包括：

——复制；

——媒介标记；

——包装；

——防护；
——存储，和；
——交付。
[B、C 级]

6 软件维护过程

6.1 * 制定软件维护计划

制造商应为进行维护过程的活动和任务，制定一项(或多项)软件维护计划。计划应说明以下内容：
a) 用于以下目的的规程：
——接收；
——形成文档；
——评价；
——解决过程，和；
——跟踪。
医疗器械软件发行后引起的反馈；
b) 是否将反馈作为问题加以考虑的准则；
c) 软件风险管理过程的应用；
d) 应用软件问题解决过程以分析和解决在医疗器械软件发行后出现的问题；
e) 应用软件配置管理过程(第 8 章)管理对现有系统的更改；和
f) 评价并实施未知来源软件(SOUP)下列事项的规程：
——升级；
——缺陷修复；
——补丁和；
——废弃。
[A、B、C 级]

6.2 * 问题和修改分析

6.2.1 形成文档并评价反馈

6.2.1.1 监控反馈

制造商应从其组织内部和用户两方面监控对已发行的软件产品的反馈。
[A、B、C 级]

6.2.1.2 形成文档并评价反馈

反馈应形成文档并进行评价，以确定已发行的软件产品是否存在问题。任何这样的问题应以问题报告的形式记录(见第 9 章)。问题报告应包括实际的或潜在的不良事件和对规范的偏离。
[A、B、C 级]

6.2.1.3 评价问题报告对安全性的影响

应对每个问题报告进行评价，以决定其对已发行的软件产品安全性有何种影响，是否有必要对已发行的软件产品进行更改以解决问题。
[A、B、C 级]

6.2.2 应用软件问题解决过程

制造商应利用软件问题解决过程(见第 9 章)阐明问题报告。
[A、B、C 级]

注：当完成本活动时，应当知道对软件系统或其软件项的安全性级别的任何更改。

6.2.3 分析更改请求

除第9章所要求的分析之外，制造商还应就每个更改请求对组织、对已发行的软件产品以及对与其有接口的系统的影响进行分析。

[B、C级]

6.2.4 更改请求的批准

制造商应评价并批准修改已发行软件产品的更改请求。

[A、B、C级]

6.2.5 联系用户和管理者

制造商应判定识别影响已发行软件产品的经批准的更改请求。

按照当地法规要求，制造商应告知用户和法规管理者如下信息：

a) 已发行软件产品中的任何问题和不更改继续使用的后果；和

b) 已发行软件产品的任何可获得的更改的性质，以及如何获得并安装更改内容。

[A、B、C级]

6.3 *修改的实施

6.3.1 用已制定的过程实施修改

制造商应利用软件开发过程(见第5章)或已建立的维护过程实施修改。

[A、B、C级]

注：有关软件更改的风险管理要求见7.4。

6.3.2 修改的软件系统的再发行

制造商应按照5.8发行已更改的软件系统。修改可以作为软件系统完整再发行的一部分发行；或作为包含经更改的软件项的修改包和为安装此项更改的必要工具用作对现有的软件系统的更改发行。

[A、B、C级]

7 *软件风险管理过程

7.1 *促成危害处境的软件分析

7.1.1 判定可能促成危害处境的软件项

制造商应确定在YY/T 0316的医疗器械风险分析活动(见4.2)中判定的可能促成危害处境的软件项。

[B、C级]

注：危害处境可能是软件失效的直接结果，或在软件中实施风险控制措施失效的结果。

7.1.2 判定促成危害处境的可能原因

制造商应判定上面确定的软件项和促成危害处境可能原因。

制造商应考虑的可能原因，适当时包括：

a) 不正确的或不完整的功能性说明；

b) 在已识别的软件项功能性中的软件缺陷；

c) 来自未知来源软件(SOUP)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，和；

e) 合理可预见的误用。

[B、C级]

7.1.3 评价公布的未知来源软件异常清单

如果来自未知来源软件的失效或意外结果是促成危害处境的软件项的可能原因，制造商至少应评价未知来源软件项供应商公布的任何异常清单，此未知来源软件项与用于医疗器械的未知来源软件项的版本有关，以确定是否有任何导致事件序列的异常，此事件序列会促成危害处境。

[B、C 级]

7.1.4 将可能原因形成文档

制造商应在风险管理文件中将软件项促成危害处境的可能原因形成文档。(见 YY/T 0316)。

[B、C 级]

7.1.5 将事件序列形成文档

制造商应在风险管理文件中将可能导致在 7.1.2 中所判定的危害处境的事件序列形成文档。

[B、C 级]

7.2 风险控制措施

7.2.1 规定风险控制措施

对于在风险管理文件中形成文档的每个促成软件项危害处境的可能原因,制造商应规定风险控制措施并形成文档。

[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危害的可能影响,赋予软件项一个软件安全性级别;和

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补充的详细资料。

7.3 风险控制措施的验证

7.3.1 验证风险控制措施

对在 7.2 中形成文档的每个风险控制措施的实施应进行验证,并将此验证形成文档。

[B、C 级]

7.3.2 将任何新事件序列形成文档

如果风险控制措施作为软件项实施,制造商应评价该风险控制措施,以判定可能导致危害处境的任何新的事件序列,并在风险管理文件中形成文档。

[B、C 级]

7.3.3 将可追溯性形成文档

制造商应将软件危害的可追溯性形成文档,适当时有:

a) 从危害处境到软件项;

b) 从软件项到特定软件原因;

c) 从软件原因到风险控制措施,和;

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 软件更改的风险管理

7.4.1 分析医疗器械软件有关安全性的更改

制造商应分析对医疗器械软件(包括未知来源软件)的更改以确定是否:

a) 引入了促成危害处境的附加的可能原因,和;

b) 要求的附加软件风险控制措施。

[A、B、C 级]

7.4.2 分析软件更改对现有风险控制措施的影响

制造商应分析对软件的更改,包括对未知来源软件的更改,以确定软件更改是否会干扰现有风险控

制措施。

[B、C 级]

7.4.3 基于分析完成风险管理活动

制造商应在这些分析的基础上完成 7.1、7.2 和 7.3 中所确定的有关风险管理活动。

[B、C 级]

8 *软件配置管理过程

8.1 *配置标识

8.1.1 制定配置项标识的方法

制造商应为项目所控制的配置项及其版本的唯一性标识制定一个方案。此方案应包括其他的软件产品或实体，诸如未知来源软件和形成的文档。

[A、B、C 级]

8.1.2 标识未知来源软件(SOUP)

对使用的每个未知来源软件的配置项，包括标准程序库，制造商应将其下列内容形成文档：

a) 标题；

b) 制造商，和；

c) 未知来源软件的唯一标志符。

[A、B、C 级]

注：未知来源软件的唯一标志符可以是，例如，版本，发行日期，补丁编号或升级指示。

8.1.3 判定系统配置文档

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档。

[A、B、C 级]

8.2 *更改控制

8.2.1 批准更改请求

制造商应只对经批准的更改请求做出配置项更改。

[A、B、C 级]

注 1：批准更改请求的决定可以是整合到更改控制过程或其他过程的一部分。本条只要求更改的批准先于其实施。

注 2：在生存周期的不同阶段，更改请求可使用不同的的验收过程，如计划所述，见 5.1.1e)和 6.1e)。

8.2.2 实施更改

制造商应按更改请求中的规定实施更改。制造商应识别并实施由更改产生的所需重复的任何活动，包括对软件系统和软件项的软件安全性分级的更改。

[A、B、C 级]

注：本条说明了应当如何实施更改以达到充分的更改控制。这并不意味着实施是更改控制过程的组成部分。实施应当利用计划的过程，见 5.1.1e)和 6.1e)。

8.2.3 验证更改

制造商应验证更改，包括重复已因更改失效的任何验证，并考虑 5.7.3 和 9.7。

[A、B、C 级]

注：本条只要求更改经过验证。这并不意味着验证是更改控制过程的组成部分。验证应当利用计划的过程，见 5.1.1e)和 6.1e)。

8.2.4 规定更改的可追溯性方法

制造商应制定审核追踪，可借以追溯下列各项：

a) 更改请求；

b) 有关的问题报告，和；

c) 更改请求的批准。

[A、B、C 级]

8.3 *配置状态记录

制造商应保留包括系统配置的受控配置项的可检索历史记录。

[A、B、C 级]

9 *软件问题解决过程

9.1 准备问题报告

制造商应为在软件产品中检出的每个问题准备一份问题报告。问题报告按如下分类：

a) 类型；

示例 1：纠正，预防，或适应新环境

b) 范围；

示例 2：更改的多少，受影响的器械模型编号，受影响的支持性附件，涉及的资源，更改的时间

c) 危害度

示例 3：对性能、安全性或保密性的影响

[A、B、C 级]

注：问题可以在软件发行之前或之后、在制造商的组织内部或外部发现。

9.2 研究问题

制造商应：

a) 研究问题，如有可能识别问题原因；

b) 利用软件风险管理过程评价问题和安全性的相关性(第 7 章)；

c) 把研究和评价结果形成文档，和；

d) 为纠正问题所需的措施拟定更改请求，或将不采取措施的理由形成文档。

[A、B、C 级]

注：如果问题与安全性无关，制造商不必按照软件问题解决过程纠正问题。

9.3 通知相关方

适当时，制造商应通知存在问题的相关方。

[A、B、C 级]

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

9.4 应用更改控制过程

制造商应遵照更改控制过程的要求(见 8.2)，批准并实施所有的更改请求。

[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，包括对其验证的记录。

适当时，制造商应更新风险管理文件。(见 7.4)

[A、B、C 级]

9.6 分析问题的趋势

制造商应在问题报告中进行分析，以找出问题的趋势。

[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) 问题已经解决，问题报告已经关闭；

b) 不良趋势已扭转；

c) 更改请求已在适当的软件产品和活动中执行；和

d) 已引入其他的问题。

[A、B、C 级]

9.8 测试文档内容

当在一项更改之后，进行**软件项**和**系统**的测试、再测试或回归测试时，**制造商**应在测试形成的文档中包括：

a) 测试结果；

b) 发现的**异常**；

c) 所测试**软件**的**版本**；

d) 相关的硬件和**软件**测试配置；

e) 相关的测试工具；

f) 测试日期，和；

g) 测试者身份标识。

[A、B、C 级]

附 录 A
（资料性附录）
本标准要求的理由说明

本附录提供本标准各章的理由说明。

A.1 理由说明

本标准的基本要求是在**医疗器械软件**的开发和维护中要遵循的一组**过程**，**过程**的选择适合于对患者和其他人员的**风险**。遵循上述**过程**的理由是认为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：

——为了确定软件中每一**软件项**运行产生的**风险**所要求的**过程**

——为使在已确定**风险**的基础上，选定的每一个**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**实施于选定的**软件项**。

因此，声称符合本标准应当包括一个形成文档的**风险**分析，它识别包括软件并可能导致**危害**处境的可预见的事件序列（见 YY/T 0316）。可能由软件间接引起的**危害**（例如，提供可能造成给予不适当的治疗的误导信息）应当包括在此**风险**分析内。

作为第一类**过程**的一部分所要求的所有**活动**，在标准正文中被标识为“[A、B、C 级]”的形式，表明对它们的要求和其适用的软件级别无关。

活动是对 A、B、C 所有级别的要求基于下述理由：

——**活动**产生有关**风险管理**或软件安全性分级的计划；

——**活动**产生一个输出，此输出作为**风险管理**或软件安全性分级的输入；

——**活动**是**风险管理**或软件安全性分级的一部分。

——**活动**建立一个支持**风险管理**或软件安全性分级的管理**系统**、文档编制或记录保持**系统**。

——**活动**通常发生在相关软件的分级未知时；

——**活动**可能引起更改，从而可能使相关软件的现有软件安全性分级失效。这包括发行后有关安全性的问题的发现和分析。

另一类**过程**只是对软件安全性级别为 B 或 C 的**软件系统**或**软件项**的要求。作为这些**过程**的部分所要求的**活动**，在标准正文中被标识为“[B、C 级]”或“[C 级]”，表明它们是依据其适用的软件分级，有选择性要求的。

对 B 和 C 级软件有选择性地要求的**活动**基于下述理由：

——通过在设计、测试或其他**验证**中更详细或更严格的要求来提高软件可靠性的活动；

——支持 B 级或 C 级要求的另一个**活动**的管理**活动**；

——支持与安全性有关问题的纠正**活动**；

——产生与安全性有关的软件设计、实施、**验证**和发行的记录的**活动**。

对 C 级软件有选择地要求的**活动**基于下列理由：

——通过在设计、测试或其他**验证**中更详细或更严格的要求或对特定问题的关注来进一步提高软件可靠性的**活动**。

注意本标准中规定的所有**过程**和**活动**，在保证高质量软件的开发和维护中被考虑为有价值的。作为对于 A 级软件的要求的这些**过程**和**活动**的许多省略（A 级软件按照定义不能引起**危害**），并不意味着这些**过程**和**活动**是无价值的或不推荐的。这些省略是要承认：不会引起**危害**的软件易于通过下述**活动**保证其安全性和有效性，即主要是通过在**医疗器械**设计期间的全部确认**活动**（本标准范围以外），以及通过一些简单的软件生存周期控制**活动**。

A.2 按级别要求的摘要

表 A.1 归纳了每个要求赋予哪一个软件安全性级别。本表是资料性的，仅为方便而提供。标准的此部分为每个要求确定了相应的软件安全性级别。

表 A.1 软件安全性级别要求摘要

章 和 条	A级	B级	C级
第四章 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		×	×
5.1.4			×
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 5.8.4	×	×	×
5.8.1、5.8.2、5.8.3、5.8.5、5.8.6、5.8.7、5.8.8		×	×
6.1 6.1	×	×	×
6.2 6.2.1、6.2.2、6.2.4、6.2.5	×	×	×
6.2.3		×	×
6.3 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）
对本标准规定的指南

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，本标准确定需要完成的最低限度的活动和任务，以提供信任：软件是以可能生产出高度可靠和安全的软件产品的方式开发的。

本附录为对本标准要求的应用提供指南。它没有增加或另外更改本标准的要求。本附录可用于更好的理解本标准的要求。

注意在本标准中，活动是过程中引出的条款，任务是在活动内规定的。例如，对软件开发过程规定的活动是：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、软件单元实现和验证、软件集成和集成测试、软件系统测试和软件发行。这些活动中的任务都有单独的要求。

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性分级，应当在风险分析过程已经确定了（由于软件系统失效可能引起何种损害）之后完成。

因为过程之间这样的逻辑依赖性，在本标准中以隐含“瀑布”或“单程的”生存周期模型的序列描述过程是最容易的。然而，其他的生存周期也可以用。象 GB/T 8566[9]中所定义的一些开发（模型）策略，包括（也见第 B.1 章）：

——瀑布：“单程的”策略，也称为“瀑布”，由实施单一时间开发过程组成。简单地：确定顾客需要、规定需求、系统设计、系统实施、测试、定位和交付。

——增量式开发模型：“增量式开发模型”策略确定客户要求并规定系统要求，然后以一系列的软件构建其余的开发。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，等等，直到系统完整为止。

——渐进：“渐进”策略也在构建中开发系统，但是不同于增量式开发模型策略（考虑到对用户需求事先没有充分理解，所有要求不能预先确定）。在这个策略中，顾客要求和系统需求事先部分确定，然后在每个后续的构建中细化。

表 B.1 GB/T 8566 中规定的开发（模型）策略

开发策略	首先规定全部要求？	多重的开发周期？	分配过渡时期软件？
瀑布 （单程的）	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。瀑布形生存周期模型通过延迟过程的开始时间，直到该过程的输入都已经完成并批准以达到此目的。

其他生存周期，尤其是渐进的生存周期，允许在该**过程**的所有输入都获得之前产生**过程输出**。例如，在整个软件体系结构完成之前，一个新的**软件项**可以被确定、分级、完成和**验证**。此类生存周期带有**风险**：一个**过程**输出的更改或开发将使另一个**过程**输出无效的**风险**。因此，所有的生存周期都用一个综合的配置管理**系统**以确保所有的**过程**输出都达到一致的状态，并且保持依赖性。

不管所用的**软件开发生存周期**是什么，下列各项原则是重要的：

——所有的**过程**输出应当保持一致的状态；无论何时，任一**过程**输出被建立或更改，所有相关的**过程**输出应当迅速更新以保持其相互之间的一致性，并保持本标准明示或隐含要求的所有依赖性；

——当需要作为输入来进一步对软件进行工作时，所有的**过程**输出应当是可用的；

——在任何**医疗器械软件**发行之前，所有的**过程**输出应当是相互一致的，并且应当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**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**。因此，当**医疗器械**体系结构包括一个新获得的部件(这可能是购买的部件或未知来源的部件)诸如包括未知来源软件的打印机/绘图机，**制造商**有责任必须将获得的部件包括在**医疗器械**的**风险管理**中。设想通过**医疗器械风险管理**的适当实施，**制造商**有可能理解该部件并且认识到其包括未知来源软件。**制造商**应用本标准应当将**软件风险管理过程**作为**医疗器械风险管理过程**的一部分来实行。

医疗器械软件生产后经验适用于已发行的**医疗器械软件**的维护。软件维护包括所有技术和管理方法的组合包括监督措施，此组合作用于**问题报告**，以将项目保持在或复原到其可以实现要求的功能以及已发行**软件产品**的更改请求的状态。例如，这包括问题的改正、法规报告、再确认和预防措施。见 GB/T 20157[10]。

B.2 参考标准

ISO/IEC 90003[11]为将质量管理体系应用于软件开发提供指南。此指南不是本标准所要求的，但强烈推荐。

B.3 术语和定义

可能时，用国际标准中的定义来规定术语。

本标准选用三个术语描述**软件系统**(顶级)的分解。**软件系统**可以是**医疗器械**的子**系统**(见 IEC 60601-1-4[2])或**医疗器械**本身。不再为测试或软件配置管理目的而进一步分解的最低级是**软件单元**。构成的所有层次，包括顶级和底级，可以称为**软件项**。而一个**软件系统**则由一个或多个**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**的清晰度和粒度是**制造商**的责任。使这些术语模糊化，让用户可将其应用于许多不同的开发方法和**医疗器械**中采用的软件类型。

B.4 通用要求

没有已知的方法可保证任何种类软件 100%的安全性。

提高**医疗器械软件**的安全性有三个主要的原则：

——**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**作为应用适当的软件工程方法和技术的

总体框架的质量管理体系的组成部分。这三个概念的结合允许医疗器械制造商遵循一个清晰构成的并持续可重复的决策过程，以提高医疗器械软件的安全性。

B.4.1 质量管理体系

一组形成规则并有效的软件过程包括诸如管理、基础设施、改进和培训这样的组织过程。为了避免重复，并将本标准的重点集中在软件工程上，这些过程已从本标准中省略。这些过程由质量管理体系所覆盖。YY/T 0287[7]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默认为符合国家或地区法规要求。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

软件开发充分地参与风险管理活动，以确保所有和医疗器械软件相关的合理可预见的风险得到考虑。

要求制造商应用一个符合 YY/T 0316 的风险管理过程，明确地进行医疗器械风险管理，而不要在本软件工程标准中规定一个合适的风险管理过程。由软件促成的危害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确定。

B.4.3 软件的安全性分级

与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的软件有关的风险被用作软件安全性分级方案的输入，进而确定在软件开发和维护中所采用的过程。

风险是损害的严重度及其发生概率的结合。然而，关于用传统的统计方法，如何确定软件失效发生概率没有共识。所以，在本标准中，软件系统分级是以软件失效产生的损害严重度为基础（假定失效将要发生）。对实施风险控制措施有作用的软件系统，依据其控制的损害严重度分级。

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性分级。

仅仅在下列情况下，确定与软件项失效有关的风险才是可能的：

——一个系统的结构和一个软件的体系结构，根据软件项的用途和其与其他软件和硬件项目的接口确定其作用；

——系统更改是否受控；

——在对体系结构和规定的风险控制措施进行风险分析之后。

本标准要求所有级别的软件以最少量的活动达到上述条件。

当全组的软件项被确定，且风险管理活动已识别了软件项是如何与安全性有关时，软件体系结构活动的终点即为开发的起始点，所以这是可根据软件项的安全性作用对其进行决定性分级的起始点。

这一点对应于 YY/T 0316 中的风险控制的开始点。

在这一点之前，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，或减少软件失效引起损害的机会。在这一点之后，风险管理过程应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被用于那个项目的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其对软件分级是有用的，例如，对所研究的领域集中注意力，但这样的分级应当看作是初步的，不应当用于说明过程的省略是正确的。

软件安全性分级方案不期望与 YY/T 0316 的风险分级相一致。然而 YY/T 0316 分级方案计划依据风险的严重性和可能性对风险进行分级，软件安全性分级方案依据应用于软件系统和软件项的开发和维护过程对其分级。

随着设计的进展，新的风险可能变得明显。因此，风险管理应当作为开发过程的组成部分应用。这允许开展确定全套软件项的体系结构设计，包括那些要求正确起作用以确保安全运行和防止其故障引起损害的软件项。

软件体系结构应当促进安全运行所要求的软件项的划分，并应当描述用以确保那些软件项的有效划分的方法。

如 B.3 所述，本标准选用三个术语描述**软件系统**（最高级）的分解。

图 B.1 以图形说明在**软件系统**内对**软件项**的可能划分，和在分解中软件安全性级别如何应用于成组的**软件项**。

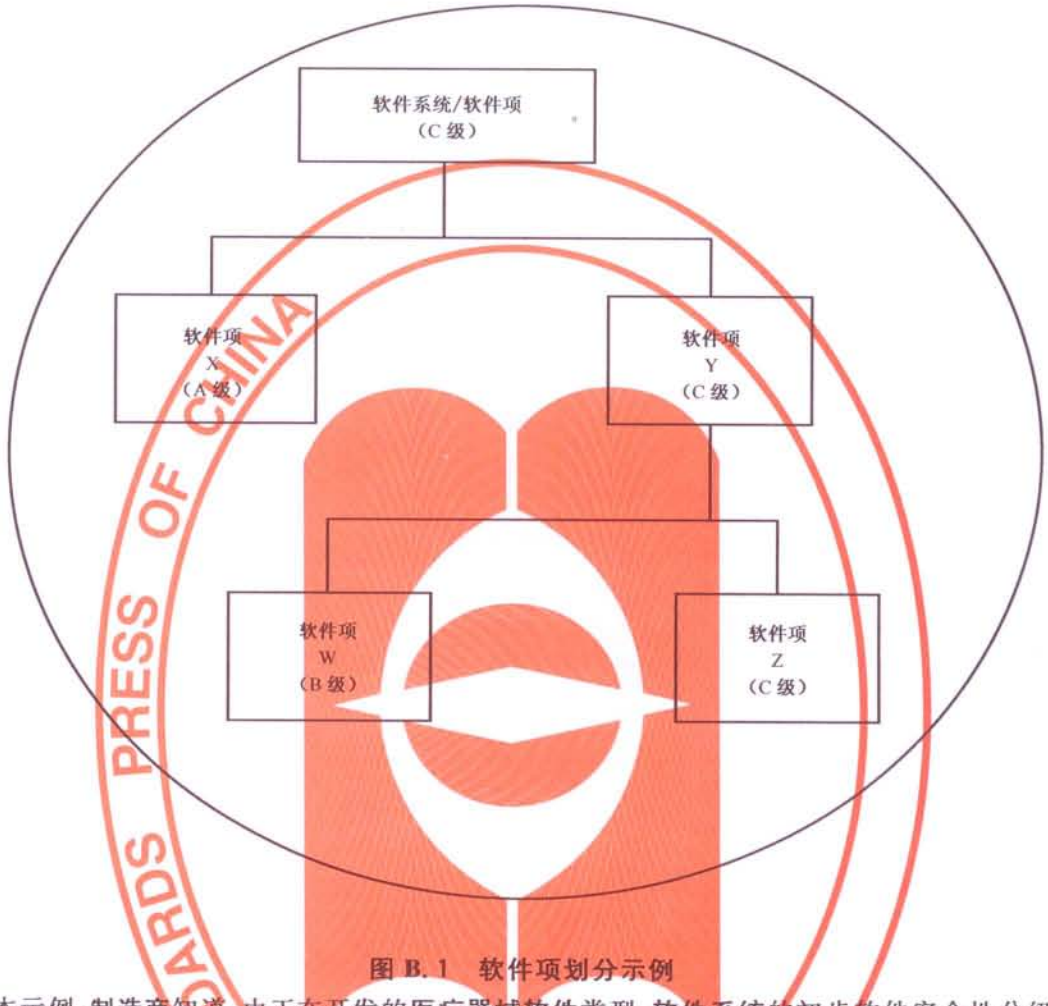


图 B.1　软件项划分示例

对本示例，**制造商**知道，由正在开发的**医疗器械软件**类型，**软件系统**的初步软件安全性分级是软件安全性 C 级。在软件体系结构设计期间**制造商**决定用 3 个**软件项**—X、W 和 Z 划分**系统**，如图示。**制造商**能将构成可能导致死亡或**严重伤害**的**危害**的所有**软件系统**划分为**软件项** Z，并将剩下的构成可能导致不**严重伤害**的**软件系统**划分为**软件项** W。**软件项** W 分级为软件安全性 B 级，**软件项** Z 分级为软件安全性 C 级。因此，**软件项** Y 必须按 4.3d）分级为 C 级。按此要求，**软件系统**也是软件安全性 C 级。**软件项** X 已分级为软件安全性 A 级。**制造商**可将**软件项** X 和 Y 之间，以及**软件项** W 和 Z 之间划分的理由说明形成文档，以保证划分的完整性。如果不可能划分，则**软件项** X 和 Y 必须分级为软件安全性 C 级。

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**进行计划，以降低软件引起的**风险**，将程序和目标告知开发组成员，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**可以在一个单一的或多重计划中将**任务**形成文档。有些**制造商**可能已制定适用于开发他们所有的**医疗器械软件**的方针和程序。在这种情况下，计划可以简单地参考现有的方针和程序。有些**制造商**可能为每个**医疗器械软件产品**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**和参考的通用程序。另一种可能性是为每个**医疗器械软件产品**的开发编制一个或一组计划。

策划应当规定并实现开发过程所需要的详细程度，并应当与风险水平相适应。例如，较高风险的系统或项目应遵循较严格的开发过程，任务应当更详细地说明。

策划是反复的活动，在开发的进展过程中应当经过再检查和更新。当对系统及开发系统所需的努力程度理解得更多时，计划可以逐步拓展以包含更多更好的信息。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性分级可能更改。或者，可以做出决定，将未知来源软件包含到系统中去。更新计划以反映当前对系统的认知，和对系统或系统中的项目所需的严格程度的认知，以便能对开发过程进行适当控制是很重要的。

B.5.2 软件需求分析

本活动要求制造商为医疗器械软件编制并验证软件需求。建立可验证的需求对于确定要做什么、确定医疗器械软件显示的可接受的特性、证实完成的医疗器械软件已完备可用是十分必要的。为证实要求已如设想的那样实施，每个要求应当以这种方式表明：即能建立客观准则以确定其是否已经正确实施。如果器械的风险管理过程将要求加在软件上以控制已识别的风险，这些要求在软件需求中应以这种方式确定：以使得追踪风险控制措施到软件需求成为可能。所有的软件需求应当以这种方式判定：即使得证实要求与软件系统测试之间的可追溯性成为可能。如果在一些国家法规批准要求符合特定的法规或国际标准，此符合性要求应当在软件需求中形成文档。因为软件需求确定了在软件中要实现什么，在完成对需求的分析活动之前，要求对该需求进行一个评价。

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改编成正式形成文档的医疗器械要求。软件需求是把软件满足顾客需求和设计输入形成正式文档的技术说明。软件功能规范通常和软件需求包括在一起，并详细确定软件如何满足其要求，即使许多不同的替代方案也可满足需求。软件设计规范规定将如何设计并对其进行分解，以实现其需求和功能规范。

通常，软件需求、功能规范和设计规范已经写成成套的一个或多个文件。现在可将此资料考虑为普通数据库中的数据项。每个数据项可有一个或多个属性，确定其目的和与数据库中其他项的连接。该方法允许显示和打印最适合每组预期用户（如，营销、制造商、测试者、审核者）的信息的不同观点，并支持可追溯性，以证实适当的实现要求和测试案例测试要求的程度。支持此方法的工具可以象用超文本链接标示语言的超文本文档（HTML）一样简单，或者象计算机辅助软件工程（CASE）工具和需求分析工具一样复杂有能力。

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策通常是在系统设计期间做出。一些或所有的系统需求分配在软件中实现。软件需求分析活动是由分析系统需求过程分配给软件的需求，和派生出完整的一组反映分配需求的软件需求组成的。

为确保系统的完整性，制造商应当提供一个对系统需求进行协商更改和澄清的机制，以纠正在母系统需求或软件需求中的不切实际、不一致性或模糊性。

收集和分析系统和软件需求的过程可以是重复的。本标准不要求将过程严格地划分成两层。实际上，常常同时罗列出系统体系结构和软件体系结构，随后将系统和软件需求以分层的形式形成文档。

B.5.3 软件体系结构设计

本活动要求制造商确定软件的主要结构组件、其外部可见特性以及它们之间的关系。如果一个组件的特性会影响其他的组件，则在软件体系结构中应当对该特性进行描述。对于可能影响软件之外的医疗器械组件的特性，这种描述尤其重要。体系结构的决定对于实施风险控制措施是极端重要的。没有理解（并形成文档）可能影响其他组件的组件特性，几乎不可能表示系统是安全的。软件体系结构是确保软件需求的正确实现所必需的。如果所有的软件需求不能由已确定的软件项来实现，软件体系结构将是不完整的。由于软件的设计和实现依靠体系结构，所以为完成这项活动，要对体系结构进行验证。体系结构的验证一般由技术评价来完成。

在软件体系结构活动期间对软件项的分级为随后的软件过程选择创造基础。分级的记录作为风险

管理文档的一部分，置于更改控制之下。

许多后续的事件可能使分级无效。包括举例如下：

——系统规范、软件说明或体系结构的更改；

——在风险分析中发现的错误，尤其是不可预见的危害；和

——要求不可行性的发现，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，应当对软件系统和软件项的分级进行再评价，可能需要修订。这有可能引发返工以对软件项应用附加过程，作为其升级到更高级别的结果。运用软件配置管理过程（第8章）确保所有必要的返工被识别和完成。

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确定的软件项和接口，以建立软件单元及其接口。虽然软件单元常常被认为是单一的功能或模块，该观点不一定是适当的。我们已经定义软件单元是不再细分成更小的项目的软件项。软件单元可以单独进行测试。制造商应当确定软件单元的详细层次。详细设计规定运算法则、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。详细设计也必然涉及到软件产品的包装。有必要将每个软件单元及其接口的设计形成文档，以便软件单元能正确地完成。详细设计填入了构建软件所必需的细节。应当充分地完善详细设计，不要求程序设计员做出特别的设计决策。

软件项可以被分解，所以只有一些新软件项实现原始软件项的有关安全性的要求。其余的软件项不实现有关安全性的功能，可以被重新分级入较低的软件安全性级别。然而，这样做的决定本身是风险管理过程的一部分，并在风险管理文件中形成文档。

因为实现依靠详细设计，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由技术评价进行。子条款5.4.4要求制造商验证详细设计活动的输出。设计确定了如何实现要求。如果设计含有缺陷，编码就不能正确地实现要求。

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

——预期事件的实现、输入、输出、接口、逻辑流，CPU分配，存贮资源配置，错误和例外的定义，错误和例外的隔离，和错误的纠正；

——缺省状态的定义，在其中用事件和转换来处理所有可能导致危害处境的故障；

——变量的初始化，存贮器管理；和

——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更改。

B.5.5 软件单元的实现和验证

此项活动要求制造商编写并验证软件单元代码。详细设计编译成源代码。编码表示终点的分解，和可执行软件开始点的组合。为了持续地达到需要的编码特性，应当用编码标准确定优选的编码类型。编码标准示例包括：可理解性要求、语言使用规则或限制和复杂性管理。对每个单元的编码进行验证，以确保其功能如详细设计所规定，并符合特定的编码标准。

5.5.5要求制造商验证编码。如果编码没有正确地实现设计，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软件项的较高级集合，并验证所形成的软件项按照预期运行。

集成方法的范围可从非递增的集成到任何形式的递增集成。安装的软件项的性质规定所选择的集成方法。

软件集成测试集中在传递数据和控制软件项的内部和外部接口间的交汇。外部接口是那些和包括操作系统软件在内的其他软件和医疗器械硬件的接口。

集成测试的严格程度和与集成测试有关的文件的详细程度应当和与器械有关的风险、器械对有潜

在危害作用的软件的依赖性、及在较高风险器械功能方面特定软件项的作用相当。例如，虽然所有的软件项都应当进行测试，但对安全性有影响的软件项应当受到更直接，彻底和详细的测试。

当适用时，集成测试证实在其输入和输出域边界的程序工作情况，认定程序对无效的、非预期的和特殊输入的响应。当给定输入组合或非预期顺序的输入或当违反规定的计时要求时，即显示程序动作。适当时，计划中的测试要求应当包括：白盒测试类型作为集成测试的一部分而执行。

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，是一种用所测试的软件项的内部任务的清楚的了解来选取测试数据的测试技术。白盒测试用对软件项的特定了解来检验输出。只有当测试者知道软件项的预定作用时，测试才是准确的。然后测试者可以看软件项是否偏离其预期目标。白盒测试不能保证完整的规范要求已经实现，因其专注于测试软件项的实现。黑盒测试，也通称为性能的、功能的、不透明盒和闭盒测试，专注于测试功能规范，不能保证实现的所有部分都进行了测试。因而黑盒测试是针对规范，并发现遗漏的错误，指出没有满足规范的那一部分。白盒测试是针对实现，将发现遗漏错误，指出实现的一部分是有缺陷的。为全面测试软件产品，黑盒测试和白盒测试两者可能都要求做。

在5.6和5.7中规定的计划和测试文档可能是限于特定开发阶段或开发原型的单独文档。它们也可以组合，使单一文档或成套文档覆盖多个分部的要求。文档的全部或部分可以包括进较高层的项目文档中，诸如一个软件或项目质量保证计划或阐明对硬件和软件所有要求进行测试的一个完整的测试计划。在这些情况下，应当建立对照来标明不同的项目文档是如何与每个软件集成任务相关联。

软件集成测试可以在模拟的环境里，在实际的目标硬件上或在整个的医疗器械上进行。

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，这些集成的软件项必须适当地发挥作用。

B.5.7 软件系统测试

此项活动要求制造商通过验证已经成功实现的软件要求，以验证软件的功能性。

软件系统测试证实软件具有规定的功能性。这项测试是对根据软件需求建立的程序功能性和性能进行验证。

软件系统测试集中在功能(黑盒)测试，虽然可能需要使用白盒测试(见以前部分)方法来更有效地完成某些测试，如启动压力条件或缺陷、以及增加条件测试的代码覆盖率。测试类型和测试阶段的组织是灵活的，但对于需求覆盖率、风险控制、适用性以及测试类型(如缺陷测试、安装测试、压力测试)应该被证明并以文档形式记录下来。

软件系统测试是对集成软件的测试，可在模拟的环境里，在实际的目标硬件上，或在整个的医疗器械上进行。

当对软件系统做出更改(即使是小的更改)时，应当决定回归测试的程度(不仅仅是个别更改的测试)以确保没有引入非预期的副作用。此项回归测试(以及不全面重复软件系统测试的理由说明)应当进行策划并形成文档。

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、部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职责。

如果在测试期间未覆盖的异常可以被重复，但是已做出决策不修复它们，那么就需要对这些异常与危害分析相联系进行评价，以验证其不影响器械的安全性。应当充分理解异常的根本原因和征兆，并应当把不修复它们的理由说明形成文档。

5.7.4要求对软件系统测试的结果进行评价，以确保获得预期结果。

B.5.8 软件发行

此项活动要求制造商将所发行的医疗器械软件的版本形成文档，说明软件版本是如何创建的，并遵循软件发行的适当规程。

制造商应当能表示所发行的软件是按开发过程开发的。将来需要的话，制造商也应当能够收回软

件和用于软件生成的工具，并应当以将软件的受损或误用减到最低的方式存储、包装、交付。应当建立确定的规程以确保适当地完成这些工作，并有一致的结果。

B.6 软件维护过程

B.6.1 制定软件维护计划

在以下两方面，软件维护过程不同于软件开发过程：

——允许制造商用比完整的软件开发过程更简捷的过程来实现快速更改，作为对紧急问题的响应。

——响应有关已发行产品的软件问题报告，制造商不仅要处理问题，也要满足当地法规（一般是通过主动的监督方案从现场收集问题数据，并就问题与使用者和管理者沟通。）

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建立或识别实施维护活动和任务的规程。为了在维护期间实施纠正措施，控制更改，管理已修订软件的发行，制造商应当形成文档并解决已报告的问题和来自用户的要求，以及管理医疗器械软件的更改。当医疗器械软件因为一个问题或改进或适应的需要，进行对代码和有关文件的修改时，就启动此过程。目标是修改已发行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行的环境或平台。本章规定的活动对于维护过程是特定的；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效果的反馈，验证报告的问题，考虑、选择并获得实施修改选项的批准。问题和其他更改请求可能影响医疗器械的性能、安全性或法规许可。为了确定是否因为一项问题报告而存在任何影响，或是否由于纠正问题的改进或实现要求导致任何影响而进行一次分析是有必要的。作为软件维护活动的一部分而实施的软件更改，对于嵌入在医疗器械内的风险控制措施是否有不利影响，通过跟踪或回归分析来验证特别重要。验证修改过的软件并不在软件（这个软件以前不引起危害或降低风险）中引起危害或降低风险也是很重要的。如果软件更改现在可能引起危害或降低风险，则软件项的软件安全性分级有可能已改变。

区分开软件维护（第6章）和软件问题解决（第9章）是很重要的。

软件维护过程的焦点是对软件产品发行后出现的反馈的充分响应。作为医疗器械的一部分，软件维护过程需要确保：

——有关安全性的问题报告得到处理并报告给适当的管理当局和受到影响的用户；

——在确保问题纠正并避免进一步出现问题的正式控制改进以后，应对软件产品进行再确认和再发行。

——制造商考虑有什么其他的软件产品可能受到影响并采取适当的措施。

软件问题解决的焦点是运行如下全面的控制体系：

- 分析问题报告，识别问题的所有含义；
- 对一些更改做出决定，识别它们所有的副作用；
- 在维护包括风险管理文档的软件配置项的一致性的同时，实施更改；
- 验证更改的实施。

软件维护过程应用软件问题解决过程。软件维护过程处理关于问题报告（是否存在问题，问题是否对安全性有显著影响，需要什么更改，何时实施更改）的高层次决策，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更改请求（识别所有需要更改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来做出修改。如果维护过程还没有确定，可以用适当的开发过程任务来做出修改。制造商也应当确保修改不会引起对医疗器械软件其他部分的负面影响。除非医

疗器械软件是作为新的开发项目来对待，分析修改对于整个医疗器械软件的影响是必需的。必须给出理由来证明将要进行的确保医疗器械软件没有修改的部分仍然如做出修改之前那样运行的回归测试的数量是合理的。

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，孤立阐述是不充分的。本标准要求应用符合YY/T 0316的风险管理过程。如YY/T 0316所规定的那样，风险管理特别涉及到有关医疗器械使用的风险的有效管理的框架。YY/T 0316的一部分属于控制与在风险分析中已识别的每个危害有关的已识别的风险。本标准中的软件风险管理过程预期提供对软件(包括在风险分析期间识别的可能促成危害处境的软件，或用于控制医疗器械风险的软件)风险控制的附加要求。由于以下两个原因，软件风险管理过程包括在本标准中：

a) 本标准的预期读者需要理解他们在软件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在软件开发生存周期中风险控制的位置。

软件风险管理是整个医疗器械风险管理的一部分。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单独文档或单一文档，或者只要本标准中的所有要求已满足时，它们可以与医疗器械风险管理活动相整合并编制成文档。

B.7.1 促成危害处境的软件分析

预期器械的危害分析将确定危害处境和相应的风险控制措施，以降低那些危害处境的概率和/或严重程度到可接收的水平。也预期将风险控制措施分配给将要执行那些风险控制措施的软件功能。

然而，不期望在软件体系结构形成之前识别所有的器械危害处境。在那时已知道在软件部件中如何实现软件功能，可以评价分配给软件功能的风险控制措施的实用性。在那时应当修订器械危害分析以包括：

- 已修订的危害处境；
- 已修订的风险控制措施和软件需求；
- 由软件引起的新的危害处境，如与人的因素有关的危害处境。

软件体系结构应当包括划分软件部件的可信的策略，以使它们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，此过程用以识别和确定系统内的软件项(包括文档)、控制项目的修改和发行以及报告项目状态和更改请求并将其形成文档。软件配置管理对于重建软件项，以识别其组成部分并提供对其做出更改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目及其版本进行唯一性标识。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 更改控制

此项活动要求制造商控制软件配置项目的更改，将识别更改请求的信息形成文档，并提供处理更改请求的形成的文档。此项活动对于确保不对软件配置项做出未授权的或非预期的更改、并确保经批准的更改请求被充分完成和验证是必需的。

更改请求可以由更改控制部门、管理人员或技术领导按照软件配置管理计划批准。批准的更改请求对于软件的实际修改和验证有可追溯性。要求是每个实际的更改与更改请求相联系，并存在形成的文档表示更改请求得到批准。形成的文档可以是更改控制部门的纪要、批准签名或数据库中的记录。

B.8.3 配置状态记录

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**对确定何时、为什么做出更改是必需的。有权使用此信息对确保软件配置项仅包含授权的修改是必需的。

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**,无论它们的特性或来源如何,包括那些在实施开发、维护或其他**过程**期间发现的问题。目标是提供及时的、形成文档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。在软件工程文献中有时将此**过程**称为"缺陷追踪"。在GB/T 8566[9]和IEC 60601-1-4[2]修正1中被称为"问题解决"。在本标准中我们已经选择称之为"软件问题解决"。

此**活动**要求在**制造商**识别出问题或不符合时,应用软件问题解决**过程**。此项**活动**是确保对已发现的可能与安全性有关联(如YY/T 0316中所确定)的问题的分析和**评价**所必需的。

一项或多项软件开发计划或规程如5.1所要求是为了阐述如何处理问题或不符合。这包括在生存周期的每个阶段,确定将要正式形成文档的软件问题解决**过程**的要求,以及何时将问题和不符合进入软件问题解决**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。考虑软件为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[7]（见第 C.2 章和附录 D）和 YY/T 0316（见第 C.3 章），为开发产品的组织提供打基础的管理环境。像 IEC 60601-1[1]（见第 C.4 章）和 GB 4793[4]（见第 C.5 章）这类的安全标准为创造安全的医疗器械给出特定的指导。当软件是医疗器械的一部分时，本标准对开发和维护安全的医疗器械软件要求做什么提供更详细的指导。许多其他标准，诸如 GB/T 8566[9]（见第 C.6 章），GB/T 20438.3[3]（见第 C.7 章）和 ISO/IEC 90003[11]等可以被看作是用于实现本标准中要求的方法、工具和技术的来源。图 C.1 表示这些标准的关系。

在从其他标准中引用条款或要求的地方，在引用条款中所定义的术语是其他标准中定义的术语，不是本标准中定义的术语。

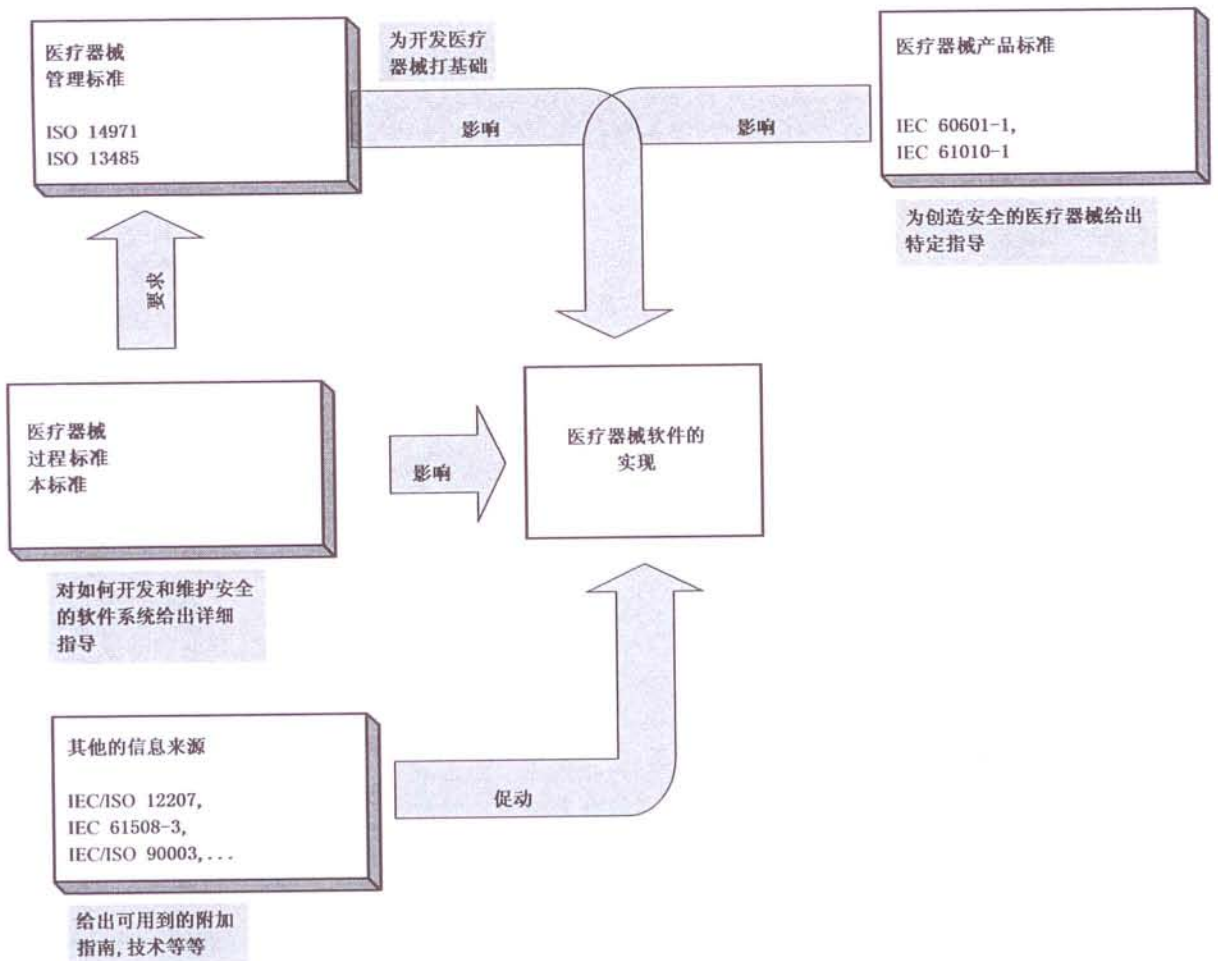


图 C.1 关键性医疗器械标准和本标准的关系

C.2 与 YY/T 0287 的关系

本标准要求制造商采用质量管理体系。当制造商应用 YY/T 0287[7]时，ISO 62304 的要求直接和表 C.1 所示的 YY/T 0287 的一些要求有关。

表 C.1 与 YY/T 0287—2003 的关系

本标准条款	YY/T 0287—2003 的相关条款
5.1 软件开发策划	7.3.1 设计和开发策划
5.2 软件需求分析	7.3.2 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 软件单元实现与验证	
5.6 软件集成和集成测试	
5.7 软件系统测试	7.3.3 设计和开发输出 7.3.4 设计和开发评审
5.8 软件发行	7.3.5 设计和开发验证 7.3.6 设计和开发确认
6.1 制定软件维护计划	7.3.7 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	7.3.5 设计和开发验证 7.3.6 设计和开发确认
7.1 促成危害处境的软件分析	
7.2 风险控制措施	
7.3 风险控制措施的验证	
7.4 软件更改的风险管理	
8.1 配置标识	7.5.3 标识和可追溯性
8.2 更改控制	7.5.3 标识和可追溯性
8.3 配置状态记录	
9 软件问题解决过程	

C.3 与 YY/T 0316 的关系

表 C.2 表示本标准对 YY/T 0316 要求的风险管理过程扩展要求的条款。

表 C.2 与 YY/T 0316—2008 的关系

YY/T 0316—2008 条款	本标准的相关条款
4.1 风险分析过程	
4.2 医疗器械预期用途和与安全性有关特性的判定	
4.3 危害的判定	7.1 促成危害处境的软件分析
4.4 估计每个危害处境的风险	4.3 软件的安全性级别
5 风险评价	

表 C.2（续）

YY/T 0316—2008 条款	本标准的相关条款
6.1 降低风险	7.2.1 规定风险控制措施
6.2 风险控制方案分析	7.2.1 规定风险控制措施
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	7.3.2 将任何新事件序列形成文档
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	7.3.3 将可追溯性形成文档
9 生产和生产后信息	7.4 软件更改的风险管理

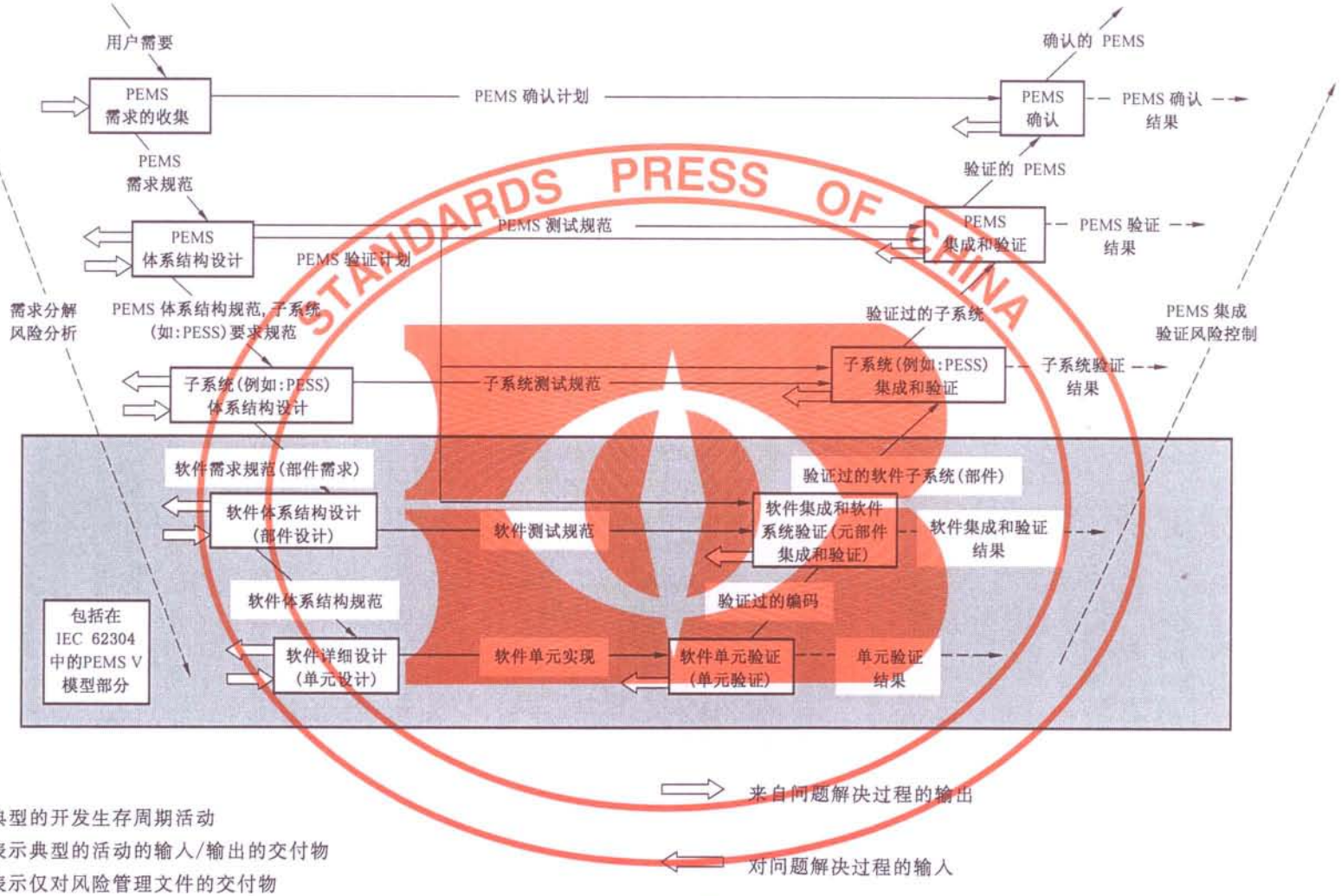
C.4 与 IEC 60601-1:2005 的可编程医用电气系统(PEMS)要求的关系

C.4.1 总则

对软件的要求是对可编程医用电气系统(PEMS)的要求的子集。本标准确定的对软件的要求，是IEC 60601-1[1]对 PEMS 要求的补充，但并非与其不相容。因为 PEMS 包括非软件成分，不是所有对PEMS 的 IEC 60601-1 要求都在本标准中阐述。

C.4.2 软件与 PEMS 开发的关系

利用描述 PEMS 开发期间发生过程的图 C.2 所说明的 V-模型，可以看到从软件需求规范/说明书到软件项集成为软件系统，本软件标准的要求已应用到 PEMS 部件级上。此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。



图释：

方框代表典型的开发生存周期活动

实线箭头表示典型的活动的输入/输出的交付物

虚线箭头表示仅对风险管理文件的交付物

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(第5章)要求规定并遵守一个软件开发计划,不要求应用任何特定的生存周期模型,但是要求计划包括确定的活动,具有确定的属性。这些要求与IEC 60601-1中对PEMS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。本标准中的要求比IEC 60601-1中对软件开发的要求更详细。

C.4.4 维护过程

符合本标准的软件维护过程(第6章)要求当对软件做出更改时,制定并遵守规程。这些要求与IEC 60601-1中对PEMS修改的要求一致。就软件维护所必须做的,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规定对软件的附加要求,超出IEC 60601-1中对PEMS的类似要求。在多数情况下,IEC 60601-1中有对PEMS的通用要求,本标准中的过程在其通用要求基础上扩展。

本标准中的软件风险管理过程与IEC 60601-1中对PEMS确定的附加风险管理要求一致。

本标准中的软件问题解决过程与IEC 60601-1中对PEMS的问题解决要求一致。

本标准中的软件配置管理过程规定了在IEC 60601-1中对PEMS未出现的附加要求,未形成文档的除外。

C.4.6 IEC 60601-1中可编程医用电气系统(PEMS)的要求的覆盖范围

表C.3表示IEC 60601-1中对PEMS的要求和本标准中的相应要求。

表C.3 与IEC 60601-1的关系

IEC 60601-1:2005的PEMS要求	本标准有关PEMS软件子系统的要求
14.1 总则 本条款的要求应适用于PEMS,除非: ——PESS不涉及基本安全性或基本性能;或 ——YY/T 0316的应用证明PESS失效并不导致不可接受的风险。	4.3 软件的安全性级别 IEC 60601-1的PEMS要求将仅适用于软件安全性的B级和C级。本标准包括一些对软件安全性A级的要求。
14.2 文件 除YY/T 0316要求的记录和文件之外,应保存应用第14章所形成的文件,并应形成风险管理文档的一部分。	4.2 风险管理
第14章所要求的文件应依照正式的文件控制程序进行评审、批准、发行和更改。	5.1 软件开发策划 除软件开发策划活动中的规定要求之外,作为风险管理文档一部分的文件要求按YY/T 0316保持。另外,对于质量体系要求的文件,YY/T 0287[7]要求对文件进行控制。
14.3 风险管理计划 YY/T 0316—2008的3.5要求的风险管理计划也应包括对PEMS确认计划的引用(见14.11)	没有特定要求。 没有特定的软件确认计划。PEMS确认计划是在系统级上,因而超出本软件标准的范围。本标准确定要求从危害到特定的软件原因,到风险控制措施,到风险控制措施的验证(见7.3)的可追溯性。
14.4 PEMS开发生存周期 应将PEMS开发生存周期形成文档。	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确定的里程碑	

表 C.3（续）

IEC 60601-1:2005 的 PEMS 要求	本标准有关 PEMS 软件子系统的要求
在每个里程碑点，应确定要完成的活动和适用于那些活动的验证方法。	5.1.6 软件验证策划 必须策划验证任务、里程碑点和验收准则。
应确定每项活动，包括其输入和输出。	5.1.1 软件开发计划 活动在本标准中确定。形成的文档在每个活动中确定。
每个里程碑点应识别必须在该里程碑点之前完成的风险管理活动。	
通过制定详细活动、里程碑和时间表的计划为特定的开发剪裁 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档。这意味着开发计划包含剪裁的开发生存周期。
PEMS 开发生存周期应包括文件编制要求。	5.1.1 软件开发计划 5.1.8 文件编制策划
14.5 问题解决 适当时，应开发并保存 PEMS 开发生存周期之内和其所有阶段和活动之间的形成解决问题的文件体系。	9 软件问题解决过程
依据产品类型，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性或基本性能的潜在或现有的问题； ——包括对每个问题的有关风险的评定； ——确定问题关闭所必须满足的准则； ——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害的识别 当编制已知的或可预见的危害表时，制造商应考虑那些与 PEMS 软件和硬件要求有关的危害，包括那些与网络/数据耦合、由第三方来源的部件和沿用子系统有关的危害。	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。
14.6.2 风险控制 应选取并确定合适的确认过的工具和程序来实现每个风险控制措施。这些工具和程序应适于保证每个风险控制措施令人满意地降低已判定的风险。	5.1.4 软件开发标准、方法和工具策划 本标准要求特定工具和方法的确定用于一般开发，不用于每个风险控制措施。
14.7 需求规范 对 PEMS 和其每个子系统（例如对于一个 PESS）应有形成文档的需求规范。	5.2 软件需求分析 本标准仅阐述 PEMS 的软件子系统。
系统或子系统的需求规范应包括并区分任何由该系统或子系统实现的基本性能和风险控制措施。	5.2.1 由系统需求确定软件需求并形成文档 5.2.2 软件需求内容 5.2.3 在软件需求中包括风险控制措施 本标准并不要求与基本性能和风险控制措施有关的要求和其他要求相区别，但是要求所有需求都唯一性地被确定。

表 C.3（续）

IEC 60601-1:2005 的 PEMS 要求	本标准有关 PEMS 软件子系统的要求
14.8 体系结构 对于 PEMS 和其每个子系统，应规定满足一个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，体系结构规范应利用： a) 有高集成度的部件； b) 自动防故障功能； c) 冗余度； d) 多样性； e) 功能性划分； f) 防御设计，例如，通过限制可得到的输出功率，或通过引入方法来限制执行机构的移动，对潜在危害的限制。	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，其所以被唯一确定，是因为有说明如何保证划分的完整性的要求。
体系结构规范应考虑： g) 将风险控制措施分配到 PEMS 的子系统和部件； h) 部件的失效模式及其效应； i) 共同原因的失效； j) 系统的失效； k) 测试间隔持续时间和诊断覆盖范围； l) 可维修性； m) 预防合理可预见的误用； n) 如果适用，网络/数据耦合说明。	这不包括在本标准中。
14.9 设计和实现 适当时，应将设计分解为几个子系统，每个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。
有关设计环境的描述性数据应包括在风险管理文档中。	5.4.2 为每个软件单元开发详细设计
14.10 验证 实现基本安全性、基本性能或风险控制措施等的所有功能都要求验证。	5.1.6 软件验证策划 每项活动都要求验证。
应形成验证计划以表示如何验证这些功能。计划应包括： ——在哪个里程碑点应对每个功能实施验证； ——验证策略、活动、技术和执行验证人员的适当独立程度的选取和形成文件； ——验证工具的选取和利用； ——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。
应依照验证计划实施验证。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 确认计划应包括基本安全性和基本性能的确认，并应要求检查 PEMS 的非预期功能。	本标准不覆盖软件确认。PEMS 确认是系统级的活动，在本标准的范围之外。

表 C.3（续）

IEC 60601-1:2005 的 PEMS 要求	本标准有关 PEMS 软件子系统的要求
PEMS 确认应依照 PEMS 确认计划完成。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。
对 PEMS 确认负有全部责任的人员应独立于设计组。制造商应将独立性级别的理由说明形成文件。	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。
设计组的成员不应对其自己的设计的 PEMS 确认负责。	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。
所有 PEMS 确认组成员和设计组成员间的所有专业关系应在风险管理文档中形成文件。	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。
PEMS 确认方法和结果的引用应包括在风险管理文档中。	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 如果任何或所有设计是由对早期设计的修改产生，则或者像是一个全新设计，本条款全部适用，或任何以前设计文件的持续有效性应在形成文件的修改/更改程序下进行评定。	6 软件维护过程 本标准采用的方法：软件维护应当进行策划，修改的实现应当利用软件开发过程或已建立的软件维护过程。
14.13 PEMS 和其他设备通过网络/数据耦合相连接 如果 PEMS 预期和 PEMS 制造商控制范围之外的其他设备通过网络/数据耦合连接，其技术描述应： a) 确定 PEMS 达到其预期用途所必需的网络/数据耦合特性； b) 以表列出提供规定特性用的网络/数据耦合的失效所导致的危害处境； c) 指导负责的组织： ——PEMS 与包括其他设备的网络/数据耦合的连接，可能导致患者、操作人员或第三方的事先未识别的风险； ——负责组织应当识别、分析、评价并控制这些风险； ——随后对网络/数据耦合进行更改有可能引入新的风险并要求附加的分析；和 ——对网络/数据耦合进行更改，包括： · 网络/数据耦合配置的更改； · 附加项目与网络/数据耦合的连接； · 项目与网络/数据耦合断开连接； · 更新与网络/数据耦合连接的设备； · 升级与网络/数据耦合连接的设备。	对网络/数据耦合的要求不包括在本标准中。

C.4.7 与 IEC 60601-1-4 中要求的关系

IEC 60601-1-4 将会继续使用，直到 IEC 60601-1:2005 的过渡期结束。

表 C.4 表示 IEC 60601-1-4[2]的要求和本标准中的相关要求。这并不表明本标准中的有关要求完全覆盖 IEC 60601-1-4 中的要求。60601-1-4 要求的许多部分由符合 YY/T 0316 所覆盖。IEC 60601-1-4中的某些要求没有在本标准中阐述。

表 C.4　与 IEC 60601-1-4 的关系

来自 IEC 60601-1-4:1996 加修正 1:1999 的 PEMS 要求	本标准的有关要求
6.8 随附文件	
6.8.201	4.2 和 4.3c)
52.201 记录	
52.201.1	4.1
52.201.2	4.1 和 4.2
52.201.3	4.2
52.202 风险管理计划	
52.202.1	4.2
52.202.2	5.1.1,5.1.5
52.202.3	4.1,5.1.2
52.203 开发生存周期	
52.203.1	5.1.1
52.203.2	5.1.1
52.203.3	
52.203.4	5.1.7
52.203.5	7
52.204 风险管理过程	
52.204.1	4.2
52.204.2	4.2.7
52.204.3	
52.204.3.1	
52.204.3.1.1	4.2,7.1
52.204.3.1.2	4.2,7.1.2
52.204.3.1.3	4.2
52.204.3.1.4	4.2,7.1.2e)
52.204.3.1.5	4.2,7.1.2
52.204.3.1.6	4.2,7.1
52.204.3.1.7	4.2
52.204.3.1.8	4.2
52.204.3.1.9	4.2
52.204.3.1.10	4.2
52.204.3.2	
52.204.3.2.1	4.2
52.204.3.2.2	4.2,4.3
52.204.3.2.3	

表 C.4（续）

来自 IEC 60601-1-4:1996 加修正 1:1999 的 PEMS 要求	本标准的有关要求
52.204.3.2.4	
52.204.3.2.5	4.2
52.204.4	
52.204.4.1	4.2
52.204.4.2	4.2
52.204.4.3	4.2
52.204.4.4	4.2
52.204.4.5	
52.204.4.6	4.2
52.205 人员资格	4.1
52.206 需求规范	
52.206.1	5.2
52.206.2	7.2.2
52.206.3	
52.207 体系结构	
52.207.1	5.3.1
52.207.2	5.3
52.207.3	
52.207.4	
52.207.5	
52.208 设计和实现	
52.208.1	
52.208.2	
52.209 验证	
52.209.1	5.7.1
52.209.2	5.1.5,5.1.6
52.209.3	5.2.6,5.3.6,5.4.4,5.5.5,5.6,5.7
52.209.4	
52.210 确认	
52.210.1	4.1
52.210.2	4.1
52.210.3	4.1
52.210.4	
52.210.5	
52.210.6	

表 C.4（续）

来自 IEC 60601-1-4:1996 加修正 1:1999 的 PEMS 要求	本标准的有关要求
52.210.7	
52.211 修改	
52.211.1	6
52.211.2	4.1,6[a]
52.212 评定	
52.212.1	4.1

C.5 与 GB 4793 的关系

GB 4793[4]的范围覆盖电气测试和测量设备，电气控制设备和电气实验室设备。仅有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，体外诊断设备划归为**医疗器械**，然而，却没有纳入 GB 4793[1]的范围之内。这不仅可以归因于：严格来说，体外诊断设备不是和患者直接接触的**医疗器械**这样的事实，而且也归因于：此类产品是为在不同的实验室的许多不同的应用目的而制造的事实。而作为体外诊断设备或体外诊断设备的附件来使用是很少的。

如果实验室设备用作体外诊断设备，所获得的测量结果必须要按照医疗准则进行**评价**。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**危害**的软件，例如软件引起的失效导致医疗数据(测量结果)的有害改变，必须考虑本标准。

图 C.3 中的流程图对解释**风险管理过程**的基本方法和本标准的应用提供了有用的帮助：

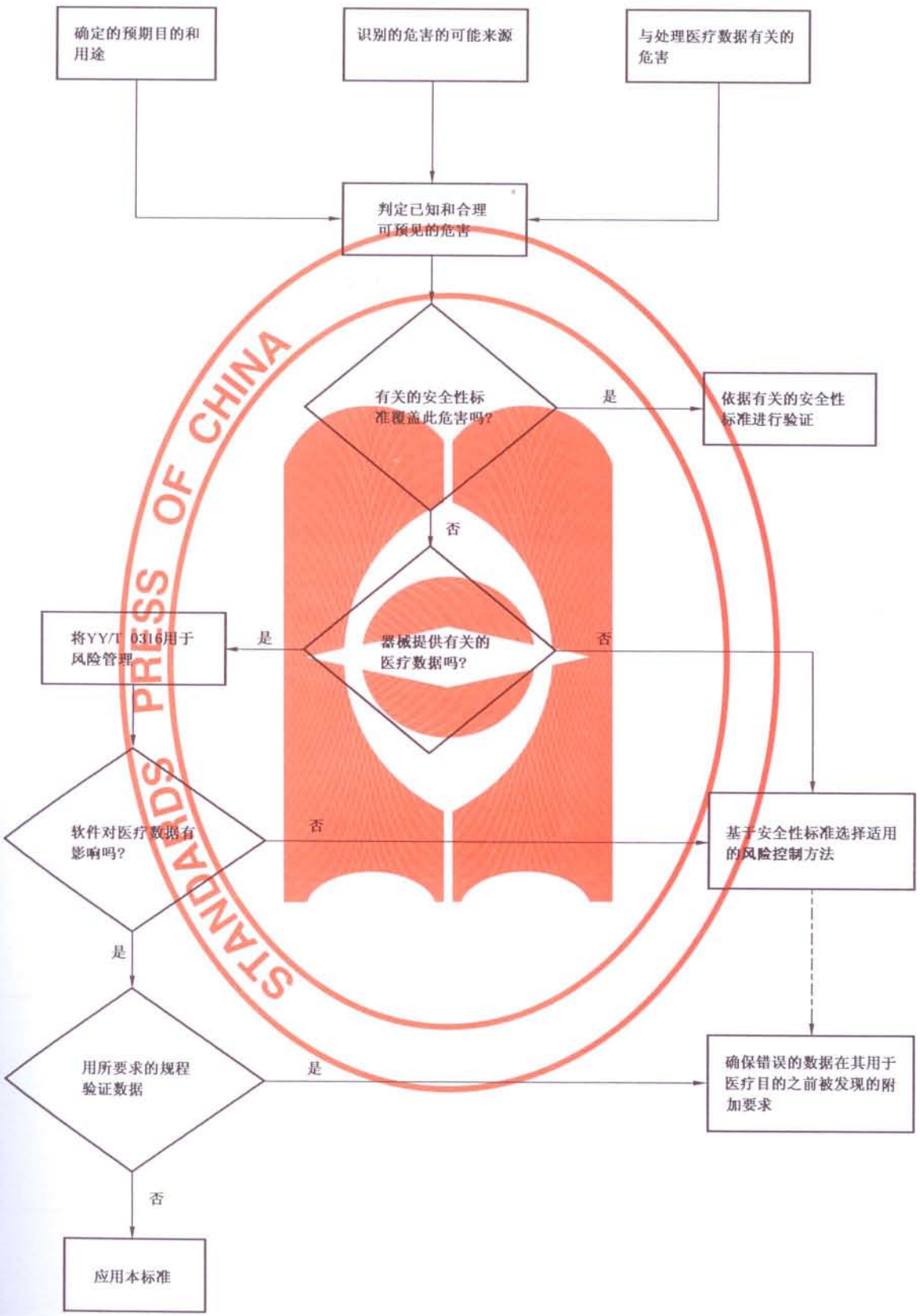


图 C.3 本标准同 GB 4793 的应用

C.6 与 GB/T 8566 的关系

本标准源于 GB/T 8566[9]的方法和概念，GB/T 8566[9]一般地规定了对软件生存周期过程的要求，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 GB/T 8566，其：

- 不包括系统方面，如系统需求、系统体系结构和确认；
- 对医疗器械删减了一些在别处被看作重复性的形成文件的活动的过程；
- 增加(安全性)风险管理过程和软件发行过程；
- 将支持过程的文档和验证包括在开发和维护过程中。
- 把每个过程的过程实现和策划活动归入开发和维护过程中的单个活动；
- 按安全性需要把需求分级；和
- 不把过程明确地分类为主要的或支持性的，也不象 GB/T 8566 那样来组合过程。

大部分这些更改是源自对标准进行剪裁的愿望，根据医疗器械行业的下列需要而进行的：

- 关注安全性要求和医疗器械风险管理标准 YY/T 0316；
- 选取在法规环境中有用的适当过程；
- 考虑软件开发涵盖于质量体系(其覆盖 GB/T 8566 的一些过程和要求)中；和
- 降低抽象概念水平，使其易于使用。

本标准不与 GB/T 8566 相矛盾。GB/T 8566 在制定包括本标准要求的构造良好的软件开发生存周期模型中，具有辅助作用。

表 C.5 由 ISO/IEC JTC1/SC7 制定，表示本标准和 GB/T 8566 的关系。

表 C.5 与 GB/T 8566 的关系

本标准 过程		GB/T 8566 过程	
活动	任务	活动	任务
5 软件开发过程		5.3 开发过程 6.1 文档编制过程 6.2 配置管理过程 6.4 验证过程 6.5 确认过程 6.8 问题解决过程 7.1 管理过程	
5.1 软件开发策划		5.3.1 过程实现 5.3.3 系统体系结构设计 5.3.7 软件编码和测试 5.3.8 软件集成 5.3.9 软件鉴定测试 5.3.10 系统集成 6.1.1 过程实现 6.2.1 过程实现 6.2.2 配置标识 6.4.1 过程实现 6.5.1 过程实现 6.8.1 过程实现 7.1.2 策划	

表 C.5（续）

本标准 过程		GB/T 8566 过程	
活动	任务	活动	任务
5.1 软件开发策划		7.1.3 执行和控制 7.2.2 建立基础设施 7.2.3 维护基础设施	
	5.1.1 软件开发计划	5.3.1 过程实现 7.1.2 策划	5.3.1.1 5.3.1.3 5.3.1.4 7.1.2.1
	5.1.2 保持软件开发计划更新	7.1.3 执行和控制	7.1.3.3
	5.1.3 引用系统设计和开发的软件开发计划	5.3.3 系统体系结构设计 5.3.10 系统集成 6.5.1 过程实现	5.3.3.1 5.3.10.1 6.5.1.4
	5.1.4 软件开发标准、方法和工具的策划	5.3.1 过程实现	5.3.1.3 5.3.1.4
	5.1.5 软件集成和集成测试策划	5.3.8 软件集成	5.3.8.1
	5.1.6 软件验证策划	6.4.1 过程实现 5.3.7 软件编码和测试 5.3.8 软件集成 5.3.9 软件鉴定测试	6.4.1.4 6.4.1.5 5.3.7.5 5.3.8.5 5.3.9.3
	5.1.7 软件风险管理策划	修正 1:2002-F 3.1.5 风险管理过程	
	5.1.8 文档策划	6.1.1 过程实现	6.1.1.1
	5.1.9 软件配置管理策划	6.2.1 过程实现 6.8.1 过程实现	6.2.1.1 6.8.1.1
	5.1.10 受控的支持项	7.2.2 建立基础设施 7.2.3 维护基础设施	7.2.2.1 7.2.3.1
	5.1.11 验证前的软件配置项的控制	6.2.2 配置标识	6.2.2.1
5.2 软件需求分析		5.3.3 系统体系结构设计 5.3.4 软件需求分析 6.4.2 验证	
	5.2.1 由系统需求确定软件需求并形成文档	5.3.3 系统体系结构设计	5.3.3.1

表 C.5（续）

本标准 过程		GB/T 8566 过程	
活动	任务	活动	任务
5.2 软件需求分析	5.2.2 软件需求内容	5.3.4 软件需求分析	5.3.4.1
	5.2.3 在软件需求中包括风险控制措施		
	5.2.4 医疗器械风险分析的再评价		无
	5.2.5 更新系统要求	5.3.4 软件需求分析	a) b)
	5.2.6 验证软件需求	5.3.4 软件需求分析 6.4.2 验证	5.3.4.2 6.4.2.3
5.3 软件体系结构设计		5.3.5 软件体系结构设计	
	5.3.1 将软件需求转换进体系结构	5.3.5 软件体系结构设计	5.3.5.1
	5.3.2 为软件项接口开发体系结构		5.3.5.2
	5.3.3 规定 SOUP 项目的功能和性能需求		无
	5.3.4 规定 SOUP 项目所要求的系统硬件和软件		无
	5.3.5 判定风险控制所必需的隔离		无
	5.3.6 验证软件体系结构	5.3.5 软件体系结构设计	5.3.5.6
5.4 软件详细设计		5.3.6 软件详细设计 6.4.2 验证	
	5.4.1 将软件体系结构细化为软件单元	5.3.6 软件详细设计	5.3.6.1
	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		5.3.6.2
	5.4.4 验证详细设计	6.4.2 验证	5.3.6.7
5.5 软件单元实现和验证		5.3.6 软件详细设计 5.3.7 软件编码和测试 6.4.2 验证	
	5.5.1 实现每个软件单元	5.3.7 软件编码和测试	5.3.7.1
	5.5.2 制定软件单元的验证过程	5.3.6 软件详细设计 5.3.7 软件编码和测试	5.3.6.5 5.3.7.5
	5.5.3 软件单元的验收准则	5.3.7 软件编码和测试	5.3.7.5
	5.5.4 补充的软件单元验收准则	5.3.7 软件编码和测试 6.4.2 验证	5.3.7.5 6.4.2.5
	5.5.5 软件单元的验证	5.3.7 软件编码和测试	5.3.7.2

表 C.5（续）

本标准 过程		GB/T 8566 过程	
活动	任务	活动	任务
5.6 软件集成和集成测试		5.3.8 软件集成 5.3.9 软件鉴定测试 5.3.10 系统集成 6.4.1 过程实现 6.4.2 验证	
	5.6.1 软件单元集成	5.3.8 软件集成	5.3.8.2
	5.6.2 验证软件集成	5.3.8 软件集成 5.3.10 系统集成	5.3.8.2 5.3.10.1
	5.6.3 测试集成的软件	5.3.9 软件鉴定测试	5.3.9.1
	5.6.4 集成测试内容		5.3.9.3
	5.6.5 验证集成测试规程	6.4.2 验证	6.4.2.2
	5.6.6 进行回归测试	5.3.8 软件集成	5.3.8.2
	5.6.7 集成测试记录的内容	5.3.8 软件集成	5.3.8.2
	5.6.8 软件问题解决过程的使用	6.4.1 过程实现	6.4.1.6
5.7 软件系统测试		5.3.8 软件集成 5.3.9 软件鉴定测试 6.4.1 过程实现 6.4.2 验证 6.8.1 过程实现	
	5.7.1 为软件需求制定测试项	5.3.8 软件集成 5.3.9 软件资格测试	5.3.8.4 5.3.9.1
	5.7.2 使用软件问题解决过程	6.4.1 过程实现	6.4.1.6
	5.7.3 更改后再测试	6.8.1 过程实现	6.8.1.1
	5.7.4 验证软件系统测试	6.4.2 验证 5.3.9 软件鉴定测试	6.4.2.2 5.3.9.3
	5.7.5 软件系统测试记录内容	5.3.9 软件鉴定测试	5.3.9.1
5.8 软件发行		5.3.9 软件资格测试 5.4.2 运行测试 6.2.5 配置评价 6.2.6 发行管理和交付	
	5.8.1 确保软件验证的完成	5.4.2 运行测试 6.2.6 发行管理和交付	5.4.2.1 5.4.2.2 6.2.6.1
	5.8.2 将已知的剩余异常形成文档	6.2.5 配置评价 5.3.9 软件鉴定测试	6.2.5.1 5.3.9.3
	5.8.3 评价已知的剩余异常		

表 C.5（续）

本标准 过程		GB/T 8566 过程	
活动	任务	活动	任务
5.8 软件发行	5.8.4 将发行的版本形成文档	6.2.6 发行管理和交付	6.2.6.1
	5.8.5 将已发行软件创建过程形成文档		
	5.8.6 确保活动和任务的完成		
	5.8.7 软件归档		
	5.8.8 保证软件发行的可重复性		
6 软件维护过程		5.5 维护过程 6.2 配置管理过程	
6.1 制定软件维护计划		5.5.1 过程实现	5.5.1.1
6.2 问题和修改分析		5.5.1 过程实现 5.5.2 问题和修改分析 5.5.3 修改实现 5.5.5 迁移	
	6.2.1 形成文档并评价反馈		
	6.2.1.1 监视反馈	5.5.1 过程实现	5.5.1.1 5.5.1.2
	6.2.1.2 形成文档并评价反馈		
	6.2.1.3 评价问题报告对安全性的影响	5.5.2 问题和修改分析	5.5.2.1 5.5.2.2 5.5.2.3 5.5.2.4
	6.2.2 应用软件问题解决过程	5.5.1 过程实现	5.5.1.2
	6.2.3 分析更改请求	5.5.2 问题和修改分析	5.5.2.1
	6.2.4 更改请求的批准	5.5.2 问题和修改分析	5.5.2.5
	6.2.5 联系用户和管理者	5.5.3 修改实现 5.5.5 迁移	5.5.3.1 5.5.5.3
6.3 修改的实施		5.5.3 修改实现 6.2.6 发行管理和交付	
	6.3.1 用已制定的过程实施修改	5.5.3 修改实现	5.5.3.2
	6.3.2 修改的软件系统的再发行	6.2.6 发行管理和交付	6.2.6.1
7 软件风险管理过程		修改 1:2002 - F 3.15 风险管理过程 62304 中的过程提出在修改 1 中没有提出的风险/危害问题。（在风险测量等方面）有一些通用性，但是分析的焦点是完全不同的。	

表 C.5（续）

本标准 过程		GB/T 8566 过程	
活动	任务	活动	任务
8 软件配置管理过程		5.5 维护过程 6.2 配置管理过程	
8.1 配置标识		6.2.2 配置标识	
	8.1.1 制定标识配置项的方法	6.2.2 配置标识	6.2.2.1
	8.1.2 识别未知来源软件		无
	8.1.3 判定系统配置文档	6.2.2 配置标识	6.2.2.1
8.2 更改控制		5.5.3 更改实现 6.2.3 配置控制	
	8.2.1 批准更改请求	6.2.3 配置控制	6.2.3.1
	8.2.2 实现更改	5.5.3 修改实现 6.2.3 配置控制	5.5.3.2 6.2.3.1
	8.2.3 验证更改	6.2.3 配置控制	6.2.3.1
	8.2.4 规定更改的可追溯性		
8.3 配置状态记录		6.2.4 配置状态统计	6.2.4.1
9 软件问题解决过程		5.5 维护过程 6.2 配置管理 6.8 问题解决过程	
9.1 准备问题报告		6.8.1 过程实现 6.8.2 问题解决	6.8.1.1 b) 6.8.2.1
9.2 研究问题		6.8.2 问题解决 6.8.1 过程实现	6.8.2.1 6.8.1.1 b)
9.3 通知相关方		6.8.1 过程实现	6.8.1.1 a)
9.4 应用更改控制过程		6.2.3 配置控制 5.5.3 修改实现	
9.5 保持记录		6.8.1 过程实现	6.8.1.1 a)
9.6 分析问题的趋势		6.8.1 过程实现 6.8.2 问题解决过程	6.8.1.1 b) 6.8.2.1
9.7 验证软件问题的解决		6.8.1 过程实现	6.8.1.1 d)
9.8 测试文档内容			12207 中的所有测试任务都要求文件编制

C.7 与 GB/T 20438 的关系

与安全关键软件设计有关的本标准，是否应当遵循 GB/T 20438 的原则。问题已经被提出，以下各条解释本标准的观点：

GB/T 20438 阐明 3 项主要的问题：

1) **风险管理**生存周期和生存周期过程；

2) 安全完整性等级的定义；

3) 为软件开发推荐的技术，工具和方法，和负责执行不同**任务**的人员的独立程度。

通过对规范性引用文件 YY/T 0316(**风险管理**的**医疗器械**行业标准)将问题 1)覆盖在本标准中。此项引用的作用是采用 YY/T 0316 的**风险管理**方法，作为**医疗器械软件**的软件**过程**的一个组成部分。

对问题 2)，本标准采取比 GB/T 20438 更简单的方法。后者按照可靠性目标定义将软件分级为 4 个“安全完整性水平”。可靠性目标在**风险**分析后确定，**风险**分析对软件失效引起**损害**的严重度和概率进行量化。

本标准通过在分类之前允许不考虑软件失效概率，简化了问题 2)。仅基于失效引起**损害**的严重度分类为 3 个软件安全性级别。在分类之后，不同的软件安全性级别要求不同的**过程**：意图是进一步降低软件失效概率。

问题 3)不由本标准阐述。鼓励本标准的读者用 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其他方法能够提供同样好的结果。关于负责一个软件**活动**(如**验证**)的人员相对于负责其他**任务**(如设计)的人员的独立性问题，本标准未作推荐。特别是本标准不要求有一个独立的安全评审人员，因为这是 YY/T 0316 所要求。

附 录 D
（资料性附录）
实 施

D.1 引言

本附录对如何在制造商的过程中实施本标准给出了概述。也考虑到象 YY/T 0287[7]等其他标准要求的适当、相当的过程。

D.2 质量管理体系

对于医疗器械制造商，包括本标准中提到的医疗器械软件，在 4.1 中要求建立质量管理体系（QMS）。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

推荐借助在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档的质量管理体系过程已经如何完善地覆盖了软件生存周期过程。任何已识别的差距都可以由质量管理过程的延伸容纳，或可个别的描述。如果制造商已有可用的管理软件开发验证和确认的过程描述，则也应当对其进行评价，以确定它们是否与本标准一致。

D.4 将本标准的要求整合进制造商的质量管理过程

本标准可以通过调节或延伸在质量管理体系中已经建立的过程，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。

当医疗器械软件由未建立文件化的质量管理体系的“初始设备制造商（OEM）”或分包商所开发时，制造商负责确保其适当地实施本标准中描述的过程。

D.5 未经质量管理体系认证的小型制造商的检查表

制造商应当确定软件的最高软件安全性级别（A、B 或 C）。表 D.1 列出本标准中描述的所有活动。对 YY/T 0287 的引用应当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性级别，制造商应当就现有的过程评定所要求的每项活动。如果要求已经被覆盖，应当给出对有关过程描述的引用。

如果有不一致，需要有一个措施来改进过程。

此表也可用于措施实施之后的过程评价。

表 D.1 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—2003 的有关条款	是否包括在现有程序中？	如果是：依据	采取的措施
5.1 软件开发策划	7.3.1 设计和开发策划	是/否		
5.2 软件需求分析	7.3.2 设计和开发输入	是/否		
5.3 软件体系结构设计		是/否		
5.4 软件详细设计		是/否		

表 D.1（续）

活动	YY/T 0287—2003 的有关条款	是否包括在现有程序中？	如果是：依据	采取的措施
5.5 软件单元的实现和验证		是/否		
5.6 软件集成和集成测试		是/否		
5.7 软件系统测试	7.3.3 设计和开发输出 7.3.4 设计和开发评审	是/否		
5.8 软件发行	7.3.5 设计和开发验证 7.3.6 设计和开发确认	是/否		
6.1 制定软件维护计划	7.3.7 设计和开发更改控制	是/否		
6.2 问题和修改分析		是/否		
6.3 修改的实施	7.3.5 设计和开发验证 7.3.6 设计和开发确认	是/否		
7.1 促成危害处境的软件的分析		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 软件更改的风险管理		是/否		
8.1 配置标识	7.5.3 标识和可追溯性	是/否		
8.2 更改控制	7.5.3 标识和可追溯性	是/否		
8.3 配置状态记录		是/否		
9 软件问题解决过程		是/否		

参 考 文 献

[1] IEC 60601-1:2005 医用电气设备 第1部分:对基础安全性和基本性能的通用要求

[2] IEC 60601-1-4:1996 医用电气设备 第1部分:通用安全要求 4.并行标准:可编程医用电气系统 修正案1(1999)

[3] GB/T 20438.3 电气/电子/可编程电子的与安全性有关的系统的功能安全性 第3部分:软件要求(GB/T 20438.3—2006,IEC 61503-3:1998,IDT)

[4] GB 4793—2007 测量、控制和实验室使用的电气设备的安全性要求 第1部分:通用要求(IEC 61010-1:2001,IDT)

[5] ISO 9000:2005 质量管理体系 基础和术语

[6] GB 19001—2000 质量管理体系 要求(idt ISO 9001:2000)

[7] YY/T 0287—2003 医疗器械 质量管理体系 用于法规的要求(ISO 13485:2003,IDT)

[8] GB/T 16261.1—2003 软件工程 产品质量 第1部分:质量模型(ISO/IEC 9126-1:2001,IDT)

[9] GB/T 8566—2007 信息技术 软件生存周期过程(ISO/IEC 12207:1995,MOD)

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

[11] ISO/IEC 90003:2004 软件工程 对计算机软件应用GB 19001:2000的指南

[12] ISO/IEC 指南51:1999 安全性要求 为其包括在标准中的指南

[13] IEEE 610.12:1990 软件工程术语的IEEE标准术语表

[14] IEEE 1044:1993 对于软件异常的IEEE标准分类

[15] IEC 60601-1-6 医用电气设备 第1-6部分:通用安全要求 并行标准:适用性

YY/T 0664—2008/IEC 62034:2006

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—2008/IEC 62034:2006
*
中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码:100045
网址 www.spc.net.cn
电话:68523946 68517548
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 字数 110 千字
2008年8月第一版 2008年8月第一次印刷
*
书号:155066·2-18971 定价 40.00 元