ICS 11.040.01
C 30

YY

中华人民共和国医药行业标准

YY/T 1406.1—2016/IEC/TR 80002-1:2009

医疗器械软件 第1部分:YY/T 0316 应用于医疗器械软件的指南

Medical device software—Part 1:Guidance on the application of ISO 14971 to medical device software

(IEC/TR 80002-1:2009,IDT)

2016-03-23 发布　　2017-01-01 实施

国家食品药品监督管理总局　　发布

中华人民共和国医药
行业标准
医疗器械软件
第1部分：YY/T 0316应用于医疗器械软件的指南
YY/T 1406.1—2016/IEC/TR 80002-1：2009
*
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.org.cn
服务热线：400-168-0010
2017年2月第一版
*
书号：155066·2-31114

版权专有　侵权必究

目　　次

前言 …… Ⅲ
引言 …… Ⅳ
1　总则 …… 1
1.1　范围 …… 1
1.2　规范性引用文件 …… 1
2　术语和定义 …… 1
3　风险管理通用要求 …… 2
3.1　风险管理过程 …… 2
3.2　管理职责 …… 5
3.3　人员资格 …… 6
3.4　风险管理计划 …… 7
3.5　风险管理文档 …… 9
4　风险分析 …… 10
4.1　风险分析过程 …… 10
4.2　医疗器械预期用途和与安全有关特征的识别 …… 11
4.3　危险(源)识别 …… 12
4.4　估计每个危险情况的风险 …… 13
5　风险评价 …… 16
6　风险控制 …… 16
6.1　降低风险 …… 16
6.2　风险控制方案分析 …… 17
6.3　风险控制措施的实施 …… 23
6.4　剩余风险评价 …… 24
6.5　风险/受益分析 …… 24
6.6　由风险控制措施产生的风险 …… 25
6.7　风险控制的完整性 …… 25
7　综合剩余风险的可接受性评价 …… 26
8　风险管理报告 …… 26
9　生产和生产后信息 …… 27
附录 A（资料性附录）　定义的讨论 …… 29
附录 B（资料性附录）　软件原因示例 …… 31
附录 C（资料性附录）　软件相关的潜在隐患 …… 40
附录 D（资料性附录）　生命周期/风险管理矩阵 …… 44
附录 E（资料性附录）　安全用例 …… 47
参考文献 …… 48

定义术语的索引 …… 49

图 1　危险(源)、事件序列、危险情况和伤害之间的关系示意图—取自 YY/T 0316—2016 附录 E …… 15
图 2　风险控制措施阻止不正确软件输出引发伤害的 FTA 图示 …… 18
图 A.1　事件序列、伤害和危险(源)的关系 …… 29

表 1　除 YY/T 0316—2016 的要求外,宜包括在风险管理文档中的文件的要求 …… 9
表 A.1　危险(源)、可预见事件序列、危险情况和可能发生的伤害的关系 …… 29
表 B.1　软件功能性区域原因的示例 …… 31
表 B.2　带来副作用的软件原因示例 …… 35
表 B.3　有利于保证风险控制措施按预期进行的方法 …… 39
表 C.1　需要避免的软件相关的潜在隐患 …… 40
表 D.1　生命周期/风险管理关系表 …… 44

前　言

YY/T 1406《医疗器械软件》,由下列部分组成:

——第1部分:YY/T 0316 应用于医疗器械软件的指南;

——第2部分:医疗器械质量体系软件的确认;

——第3部分:医疗器械软件生存周期过程(YY/T 0664)的过程参考模型。

本部分为 YY/T 1406 的第1部分。

本部分按照 GB/T 1.1—2009 给出的规则起草。

本部分使用翻译法等同采用 IEC/TR 80002-1:2009《医疗器械软件　第1部分:ISO 14971 应用于医疗器械软件的指南》(英文版)。

本部分方框中的文本内容直接引用自 YY/T 0316—2016 标准,在文本的前面写明“YY/T 0316—2016 原文”。

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。

本部分由国家食品药品监督管理总局提出。

本部分由国家食品药品监督管理总局医疗器械标准管理中心归口。

本部分起草单位:北京国医械华光认证有限公司、上海市医疗器械检测所、沈阳东软医疗系统有限公司。

本部分主要起草人:王志强、由洪顺、米兰英、何骏、陆锷、郑一菡、陈志刚。

引　言

软件通常作为医疗器械技术的不可或缺的组成部分。对于包含软件的医疗器械建立其安全和有效性，需要知道软件的预期用途，同时要证明软件的实现满足预期用途而不引起任何不可接受的风险。

虽然软件本身不是一种危险(源)，但软件可能引发危险情况，理解这一点很重要。宜总是以系统观点来考虑软件，软件的风险管理不能脱离系统孤立地进行。

复杂的软件设计可能涉及复杂的事件序列，这些序列可能引发危险情况。软件风险管理的任务包含识别那些导致危险情况的事件序列，识别在这些事件序列中哪些位置可以中断序列，预防伤害或降低伤害概率。

引发危险情况的软件事件序列可分为两类：

a) 事件序列表现为软件对输入产生不可预见的响应(软件规范中的错误)；

b) 事件序列是由编码错误引起的(软件实施中的错误)。

由于正确地规范和实施复杂系统的难度以及完整验证复杂系统的难度，所以这些分类对软件来说是特有的。

因为很难估计会引发危险情况的软件异常的概率，并且因为软件在使用中不会因为损耗而随机失效，所以软件方面的风险分析，宜关注潜在软件功能的识别和会导致危险情况的异常的识别——而不是估计概率。软件异常引发的风险大多数情况下只需要评价伤害的严重度。

风险管理通常是有挑战性的，当包含软件时更是如此。下面的条包含了关于软件特性的补充细节，这为从软件层面理解 YY/T 0316—2016 提供了指南。

● **本部分的结构：**

本部分遵循了 YY/T 0316—2016 的结构，并且为与软件相关的每项风险管理活动提供了指南。

由于软件生命周期中风险管理活动的迭代特性，在提供的信息中存在一些有意的冗余。

医疗器械软件
第1部分:YY/T 0316应用于医疗器械软件的指南

1 总则

1.1 范围

本部分为YY/T 0316—2016《医疗器械 风险管理对医疗器械的应用》中包含的要求应用于有关YY/T 0664—2008《医疗器械软件 软件生存周期过程》中所指的医疗器械软件提供了指南,本部分并不增加或改变YY/T 0316—2016或YY/T 0664—2008的要求。

当软件作为医疗器械/系统时,本部分供需要实施风险管理的风险管理从业者以及需要理解如何满足YY/T 0316—2016中阐述的风险管理要求的软件工程师使用。

监管机构意识到ISO 14971在世界范围内被广泛认可作为实施医疗器械风险管理的重要标准。YY/T 0664—2008规范性引用了YY/T 0316—2016中的要求。这两个标准为本部分提供了基础。

宜说明的是,虽然YY/T 0316—2016和本部分关注的是医疗器械,但本部分还可用于为医疗卫生保健环境中的所有软件实施安全风险管理过程,无论该软件是否被归类为医疗器械。

本部分不涉及:

——已经由现有标准或计划中的标准覆盖的领域,如:报警、可用性工程、网络等;

——生产或质量管理体系软件;

——软件开发工具。

本部分预期不作为法规检查或认证评定活动的依据。

本部分中"宜"是用来表明,在满足要求的若干可能性中,推荐特别适合的一种,并未提及或排斥其他的可能性,或者用来表明某种做法更好但不是必须的要求。"宜"不应理解为要求。

1.2 规范性引用文件

下列文件对于本部分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(包括所有的修改单)适用于本部分。

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

YY/T 0664—2008 医疗器械软件 软件生存周期过程(IEC 62304:2006,IDT)

2 术语和定义

YY/T 0316—2016和YY/T 0664—2008界定的以及下列术语和定义适用于本文件。

注:定义术语的索引开始于49页。

2.1

多样性 diversity

一种冗余的形式,冗余要素用于不同的(多样的)组件、技术或方法以降低共同原因导致所有要素同时失效的概率。