ICS 11.040.01
C 30

YY

中华人民共和国医药行业标准

YY/T 0708—2009/IEC 60601-1-4:2000

医用电气设备　第1-4部分:安全通用要求并列标准:可编程医用电气系统

Medical electrical equipment—Part 1-4:General requirements for safety—collateral standard:programmable electrical medical systems

(IEC 60601-1-4:2000,IDT)

2009-11-15 发布　　2010-12-01 实施

国家食品药品监督管理局　发布

前　言

本并列标准等同采用 IEC 60601-1-4:2000《医用电气设备　第 1-4 部分:安全通用要求 并列标准:可编程医用电气系统》。

本并列标准是 GB 9706.1—2007《医用电气设备　第 1 部分:安全通用要求》(IEC 60601-1:1988,IDT)通用标准的并列标准。

本并列标准的附录 AAA 为规范性附录,附录 BBB、附录 CCC、附录 DDD、附录 EEE、附录 FFF 均为资料性附录。

本并列标准由全国医用电器设备标准化技术委员会(SAC/TC 10)归口。

本并列标准起草单位:国家食品药品监督管理局杭州医疗器械质量监督检验中心、国家武汉医用超声波仪器质量监督检测中心。

本并列标准主要起草人:杜堃、马莉、忙安石、郑建。

引　言

计算机在医用电气设备中的使用日益增多，常常起着与安全密切相关的作用。计算机应用技术在医用电气设备的运用使系统的复杂程度仅次于医疗设备的诊断和(或)治疗的对象——患者的生理系统。这种复杂性意味着系统性失效可能超出通过实际可以接受的测试限来判定的能力。相应地，本安全标准超出了对已有医用电气设备的传统测试和评定；本安全标准包括对医疗器械开发过程的要求。成品测试本身不能充分说明复杂医用电气设备的安全性。

本文件是通用标准的并列标准。它要求遵循某一过程，并产生该过程的记录来支持带有可编程电子子系统的医用电气设备的安全。风险管理和开发生存周期的概念是标准的基础，而这些概念对于开发那些不带有可编程电子子系统的医用电气设备同样是具有价值的。

针对要处理的任务，本标准的有效应用要求如下的能力：

——特定的医用电气设备应用中应着重考虑的安全因素；

——医用电气设备的开发过程；

——安全性保证方法；

——风险分析和风险控制的技能。

医用电气设备　第1-4部分:安全通用要求
并列标准:可编程医用电气系统

第一篇　概述

1　适用范围、目的及与其他标准的关系

1.201　范围

本并列标准适用于带有可编程电子子系统(PESS)的医用电气设备和医用电气系统[以下简称为可编程医用电气系统(PEMS)]的安全要求。

注:某些带有软件并用于医用目的的系统超出了本并列标准的范围,例如:许多医用信息系统。识别要素(准则)为:该系统是否满足GB 9706.1—2007中2.2.15关于医用电气设备的定义或GB 9706.15—2008中2.201中关于医用电气系统的定义。

1.202　目的

本并列标准规定了可编程医用电气系统设计过程中的要求。本并列标准也作为专用标准要求的基础,包括作为降低和管理风险目的的安全要求指南。本并列标准面向:

a)　认证机构;

b)　制造商;

c)　专用标准编制人员。

本标准涵盖:

d)　需求规格说明;

e)　体系结构;

f)　详细设计与实现,包括软件开发;

g)　修改;

h)　验证和确认;

i)　标记和随机文件。

本标准没有涵盖部分:

j)　硬件制造;

k)　软件复制;

l)　安装与交付使用;

m)　操作和维护;

n)　退出使用。

1.203　与其他标准的关系

1.203.1　GB 9706.1

对于医用电气设备而言,本并列标准是对GB 9706.1的补充。

当单独或联合引用GB 9706.1标准或本并列标准时,明确如下说法:

——"本通用标准"仅指GB 9706.1;

——"本并列标准"仅指YY/T 0708—2009;

——"本标准"合指通用标准和本并列标准。

1.203.2 专用标准

专用标准中的要求优先于本并列标准中的对应要求。

1.203.3 规范性引用文件

下列文件中的条款通过本并列标准的引用而成为本并列标准的条款。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并列标准，然而，鼓励根据本并列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并列标准。

GB 9706.1—2007 医用电气设备 第1部分：安全通用要求(IEC 60601-1:1988,IDT)

GB 9706.15—2008 医用电气设备 第1-1部分：安全通用要求 并列标准：医用电气系统的安全要求(IEC 60601-1-1:2000,IDT)

GB/T 19001—2000 质量管理体系 要求(idt ISO 9001:2000)

IEC 60788:1984 医用放射学术语

2.201 术语和定义

下列术语和定义适用于本并列标准。在本并列标准中，采用五号黑体字表示的术语与通用标准、GB 9706.15及本并列标准或IEC 60788:1984中的定义一致。

本并列标准在附录AAA(规范性附录)中给出了术语索引。

2.201.1

开发生存周期 development life-cycle

从项目概念设计阶段开始至可编程医用电气系统(PEMS)的确认完成期间进行的必要的活动。

2.201.2

危害分析 hazard analysis

危害及发生原因的识别。

注：危害的量化不是危害分析的一部分。

2.201.3

最大可容许风险 maximum tolerable risk

规定可以接受的最大风险量。

注：该风险量既可以是对可编程医用电气系统整个危害的规定，也可以是对特定危害作规定。

2.201.4

可编程医用电气系统(PEMS) programmable electrical medical system

包含有一个或多个可编程电子子系统的医用电气设备或医用电气系统。

2.201.5

可编程电子子系统(PESS) programmable electronic subsystem

基于一个或多个中央处理单元的系统，包括它们的软件和接口。

2.201.6

剩余风险 residual risk

实施风险管理后，由危害分析得出还剩余的风险。

2.201.7

风险 risk

危害导致损害发生的概率和损害的严重度程度。

2.201.8

风险管理文档 risk management file

本标准要求的那部分质量记录。

2.201.9

风险管理概要 risk management summary

为危害和风险分析中每个危害的原因以及风险已经受控的验证提供追溯的文件。

注：文件可保存在纸质或电子媒介中。

2.201.10

安全性 safety

免除于不可接受的风险。

2.201.11

安全危害(以下简称为危害) safety hazard

直接由医用电气设备引起的，对患者、其他人员、动物或环境产生的潜在有害影响。

2.201.12

不采用。

2.201.13

严重度 severity

危害可能产生后果的定性度量。

2.201.14

确认 validation

在开发过程期间或结束时，对可编程医用电气系统或其组件进行评价的过程，以确定是否满足预期用途的要求。

2.201.15

验证 verification

对可编程医用电气系统或其组件进行评价的过程，以确定在开发阶段的产品是否满足在该阶段开始时所提出的特定要求。

2.202 要求的程度和其他术语

在本并列标准中，某些词汇有如下特别的含义：

——“应(shall)”表示必须达到的强制性要求。

——“宜(should)”表示强烈建议但不是必须达到的。

——“可(may)”表示为了符合要求或可避免需要符合的内容而采用的容许的方式。

——“特定(specific)”用于表明在本并列标准或其他标准中引用的确定的信息，通常是有关特定的操作条件、测试安排，或与符合性相关的准则。

——“规定(specified)”由制造商在随机文件或正在考虑的与 PEMS 相关的其他文件中陈述的限定性信息，通常涉及它的预期目的或参数，或其使用相关的条件或用于确定符合性的测试。

6 识别、标记和文件

6.8 随机文件

6.8.201 所有涉及与重要的剩余风险相关的信息，包括对危害的描述以及操作者或用户为避免(减低)危害而应采取的措施，都应在使用说明书和风险管理文档中记载。

6.8.202 可编程医用电气系统的随机文件至少应标识制造商及唯一的识别符，如文件的版本号、发布(出版)日期。

注：适用于某些预期与软件一起使用的特定设备的信息，以及制造商的联系方式，应位于外包装或者用户说明书中，以便于用户独立于软件操作。

第九篇　不正常的运行和故障状态;环境试验

52　不正常的运行和故障状态

52.201　文件

52.201.1　应维护应用本标准形成的文件并应使其成为质量记录的一部分;见图 201。宜依照 GB/T 19001—2000 中 4.2 的要求实施。

52.201.2　这些文件(以下简称为**风险管理文档**),应根据规定的配置管理机制进行批准、发布和更改。宜依照 GB/T 19001—2000 中 4.2.3 的要求实施。

52.201.3　在整个**开发生存周期**中,应形成**风险管理概要**,并将其作为**风险管理文档**的一部分。其内容应包括:

a)　已识别的危害以及其起因;

b)　风险估计;

c)　用于消除或控制危害的风险所采取的安全性措施的证明;

d)　风险控制的有效性的评价;

e)　验证证明;

通过检查**风险管理文档**核查其符合性。

52.202　风险管理计划

52.202.1　制造商应制定风险管理计划。

52.202.2　计划应包括下列内容:

a)　计划的范围,确定项目或产品以及该计划适用的**开发生存周期**的各阶段;

b)　适用的**开发生存周期**(见 52.203),包括验证计划和确认计划;

c)　依照 GB/T 19001—2000 中 5.1 的管理职责;

d)　**风险管理过程**;

e)　审核要求。

52.202.3　如果在开发过程中计划改变,应保留更改的记录。

通过检查**风险管理文档**核查其符合性。

52.203　开发生存周期

52.203.1　应为**可编程医用电气系统**的设计和开发定义**开发生存周期**。

52.203.2　**开发生存周期**应分解为各个阶段和任务,对每一个阶段和任务都应明确定义输入和输出以及活动。

52.203.3　**开发生存周期**应包括**风险管理**的整个过程。

52.203.4　**开发生存周期**应包括对文档的要求。

52.203.5　风险管理活动应合适地贯穿于**开发生存周期**中,见 52.204。

注:在附录 DDD(资料性附录)给出了一个**开发生存周期**的示例。

通过检查**风险管理文档**核查其符合性。

52.203.6　应在**开发生存周期**的所有阶段和任务之内或之间的适用处,建立和维护一套明确的问题解决体系,并作为**风险管理文档**的一部分。根据问题,该体系可具有如下特征:

——定义作为**开发生存周期**的一部分;

——允许报告潜在的或现存**安全性**和(或)性能方面的问题;

——包括对每个问题的相关风险的评估;

——确定问题分析结束的准则〔安全性和(或)性能方面〕;

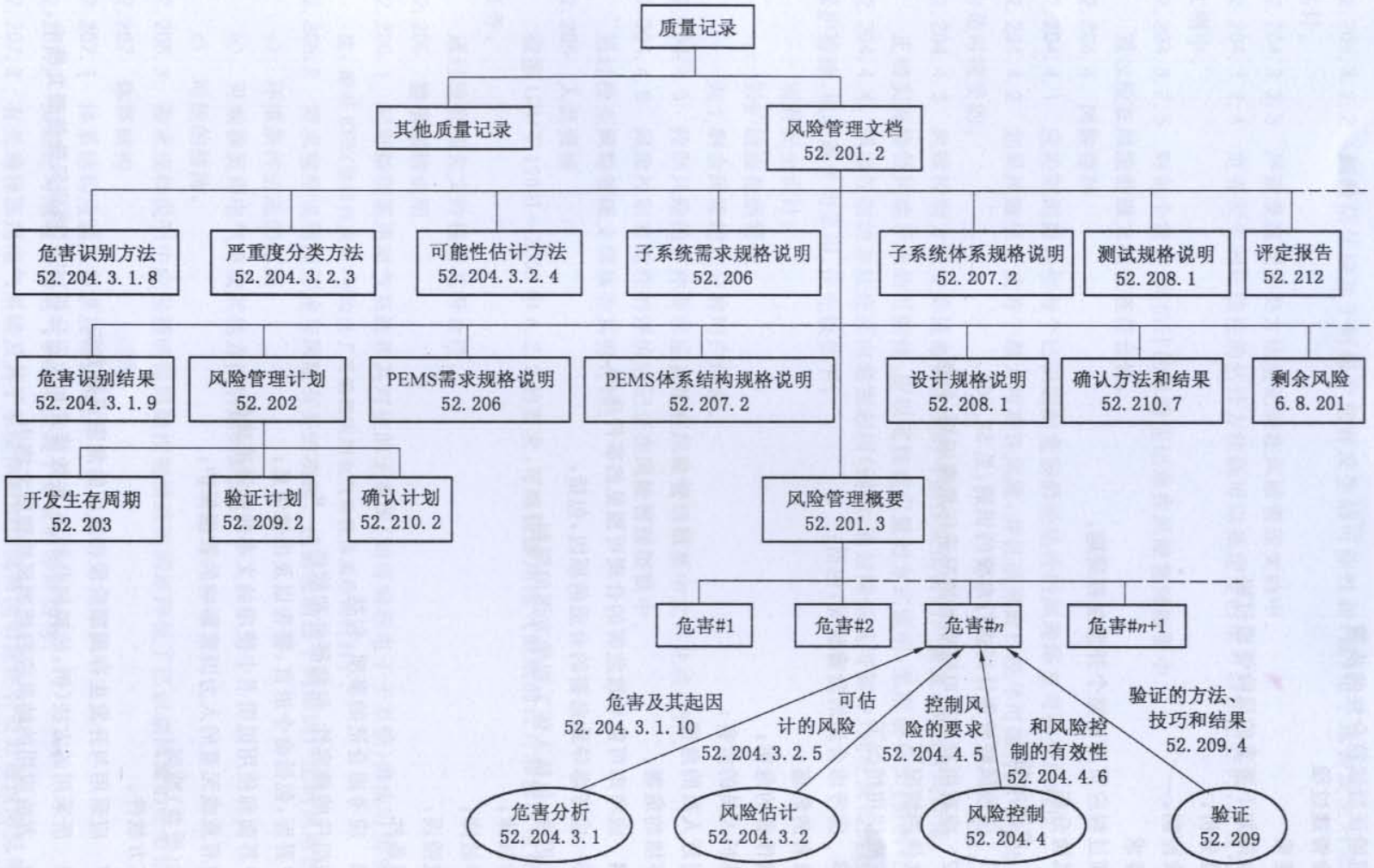

图 201　风险管理文件和风险管理概述的内容