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〕;

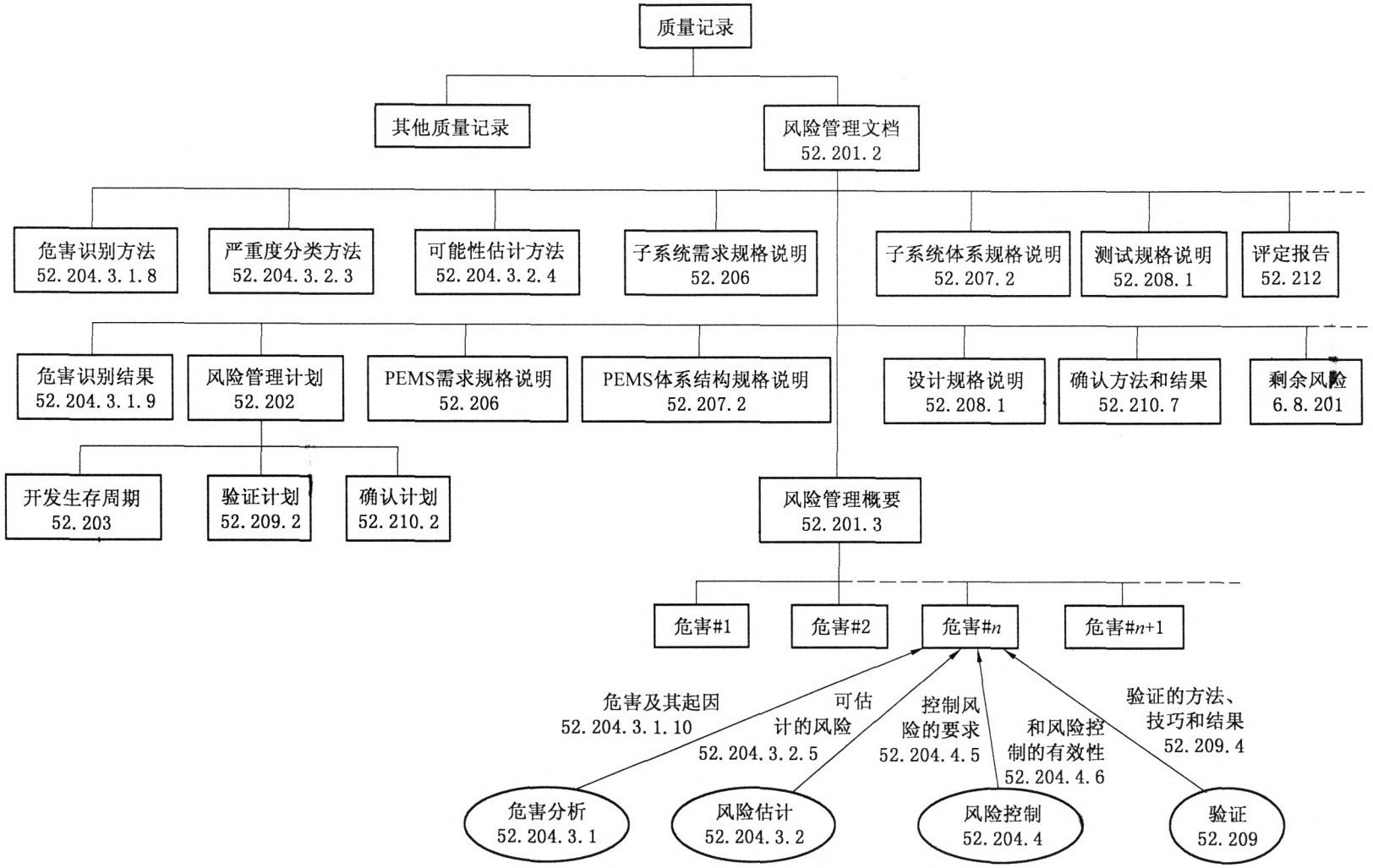

图 201　风险管理文件和风险管理概述的内容

——确定解决各种问题所采取的措施；

——确定每一种措施的确认方法；

——确定验证持续符合性的步骤。

52.204 **风险管理过程**

52.204.1 **要素**

应采用包括如下要素的**风险**管理过程：

——**风险**分析；

——**风险**控制。

52.204.2 **要求**

风险管理过程应贯穿于整个**开发生存周期**。

52.204.3 **风险分析**

52.204.3.1 **危害分析**

52.204.3.1.1 应按**风险**管理计划进行**危害**的识别，见52.202。

52.204.3.1.2 应对所有合理可预见的情况进行**危害**识别，包括：

——正常使用情况下；

——不正确使用情况下。

52.204.3.1.3 应考虑合适的**危害**状况，包括：

——对**患者**的**危害**；

——对**操作者**的**危害**；

——对维护人员的**危害**；

——对附近人员的**危害**；

——对环境的**危害**。

52.204.3.1.4 应考虑可能导致危害的合理可预见的事件序列。

52.204.3.1.5 应考虑导致**危害**的合适的原因，包括：

——人的因素，包括人体工程学方面的限制；

——硬件故障；

——软件故障；

——集成错误；

——环境条件。

52.204.3.1.6 应考虑合适的事项，包括：

——系统组件的兼容性，包括硬件和软件；

——用户界面，包括命令语言、警告以及出错信息；

——用户界面和使用说明书中使用的文本的翻译准确性；

——针对有意或无意的人为因素影响的数据保护；

——风险(受益)准则；

——第三方软件。

52.204.3.1.7 应采用与**开发生存周期**阶段相适应的**危害**识别方法。

52.204.3.1.8 所采用的方法(例：故障树分析法，失效模式和效应分析)应归档到**风险管理文档**中。

52.204.3.1.9 方法应用的结果应归档到**风险管理文档**中。

52.204.3.1.10 每个被识别的**危害**和引发的原因应记录在**风险管理概要**中。

通过检查**风险管理文档**核查符合性。

52.204.3.2 **风险估计**

52.204.3.2.1 对每一个被识别的**危害**，应估计其风险。

52.204.3.2.2 **风险**估计应基于对每个**危害**发生的可能性和(或)每个**危害**发生后果的**严重度**进行估计。

52.204.3.2.3 **严重度**级别分类方法应记录在**风险管理文档**中。

52.204.3.2.4 危害发生的可能性的估计方法既可以是定量的也可以是定性的，并应记录在**风险管理文档**中。

52.204.3.2.5 对每个**危害**，其估计的风险应记录在**风险管理概要**中。

通过检查**风险管理文档**核查符合性。

52.204.4 **风险控制**

52.204.4.1 应控制**风险**以使每个已识别的**危害**的经估计的**风险**降至可接受的程度。

52.204.4.2 如果**风险**低于或等于**最大可容许风险**，并且该**风险**已经尽可能合理可行地降低了，那么认为是可接受的。

52.204.4.3 **风险**控制方法应降低**危害**发生的可能性或**危害**的**严重度**，或两者均降低。

正确实施降低**风险**手段的可能性，应以定性或定量的方式说明；见附录 CCC(资料性附录)。

52.204.4.4 **风险**控制的方法应面向**危害**起因(例如，通过降低其可能性)或在**危害**的起因出现时采取保护措施，或者两者均采用，优先级如下：

——固有安全设计；

——保护措施包括警报；

——关于**剩余风险**的充分的用户信息。

52.204.4.5 控制风险的各种要求应直接在**风险管理概要**中文件化或引用。

52.204.4.6 **风险**控制有效性的评价应记录在**风险管理概要**中。

通过检查**风险管理文档**核查其符合性。

52.205 **人员资格**

根据 GB/T 19001—2000 中 6.2.2 的要求，**可编程医用电气系统**的设计和修改应视为一个指定的任务。

通过检查相关文件核查其符合性。

52.206 **需求规格说明**

52.206.1 对**可编程医用电气系统**和其对应的子系统(如可编程电子子系统)都应有需求规格说明。

注：附录 EEE(资料性附录)中给出了可编程医用电气系统体系结构的例子。

52.206.2 需求规格说明应详述与**风险**有关的功能。包括控制由下列原因产生的**风险**的功能：

a) 环境条件引起的原因；

b) **可编程医用电气系统**其他方面引起的原因；

c) 可能的故障。

52.206.3 需求规格说明中应包括确保**风险**控制措施圆满地降低了已识别**风险**的必要信息。

52.207 **体系结构**

52.207.1 体系结构应满足需求规格说明。

52.207.2 应规定**可编程医用电气系统**以及其子系统的体系结构。

52.207.3 有关**编程医用电气系统**及其子系统体系结构规格说明应在合适处通过降低相应的**危害**的可能性或**危害**发生的**严重度**，或二者均降低来实现**风险控制**要求。

52.207.4 为了降低**危害**发生的可能性，应在体系结构规格说明的合适处利用：

a) 高可靠性组件；

b) 失效防护功能；

c) 冗余；

d) 多样性；

e) 防护设计；

f) 潜在**危害**影响的限制，例如限制可获得输出能量和(或)通过采用限制执行机构行程的方法。

52.207.5 体系结构规格说明应考虑如下因素：

a) **风险**控制措施在**可编程医用电气系统**组件和子系统上的配置；

注：子系统和部件包括：传感器、执行机构、可编程电子子系统和接口。

b) 组件的失效模式及效应；

c) 一般原因的失效；

d) 系统性失效；

e) 测试时间间隔、测试持续时间和测试诊断范围；

f) 可维护性；

g) 有意或无意的人为因素的防护。

52.208 **设计和实现**

52.208.1 设计应在合适处适当分解成子系统，每个子系统都应有设计和测试规格说明。

52.208.2 有关设计环境的描述性数据应包括在**风险管理文档**中。

注：有关设计环境要素的示例见附录 DDD(资料性附录)。

52.209 **验证**

52.209.1 安全要求的实现应进行**验证**。

52.209.2 应制订**验证**计划，说明在**开发生存周期**的每个阶段的**安全性**要求如何验证。该计划应包括：

a) **验证**的策略、活动和技术的选择和归档；

b) **验证**工具的选择和运用；

c) **验证**的覆盖准则。

注：关于方法和技术的实例是：

——走查和检查；

——静态(动态)分析；

——白盒(黑盒)测试。

52.209.3 应根据**验证**计划进行**验证**。**验证**活动的结果应归档、分析和评定。

52.209.4 **风险管理概要**中应包含**验证**的方法、技术和结果的证明。

52.210 **确认**

52. 210.1 应进行**可编程医用电气系统**在预期使用条件下**安全性**的**确认**。

52.210.2 应制订**确认**计划，以表明实现了正确的**安全性**要求。

52.210.3 应根据**确认计划**实施确认。**确认**活动的结果应归档、分析和评定。

52.210.4 实施**确认**的小组负责人应独立于开发小组。

52.210.5 **确认**小组成员和设计小组成员的专业关联性应记录在**风险管理文档**中。

52.210.6 设计小组成员不能承担其设计的**确认**职责。

52.210.7 **风险管理文档**中应包括**确认**的方法和结果的证明。

通过检查**风险管理文档**核查其符合性。

52.211 **修改**

52.211.1 如果任何部分或全部设计是由对先前设计的修改产生，则该设计要么视为一个全新设计，则本标准的所有条款适用；要么任何先前设计文档的持续有效性应按照修改/更改程序进行评价。

52.211.2　在**开发生存周期**中所有的相关文件，应依照 GB/T 19001—2000 中 4.2.3 规定或等同规定的文件控制计划，进行校订、修正、复核和批准。

通过检查**风险管理文档**核对其符合性。

52.212　**评定**

为确保**可编程医用电气系统**按照本标准的要求开发完成并记录在**风险管理文档**中，应进行评定。它可由内部审核方式进行。

通过检查**风险管理文档**核查符合性。

附 录 AAA
（规范性附录）
术语 术语定义索引

附 录 BBB
（资料性附录）
基 本 原 理

概述

由于本标准涉及的学科技术不依从于对成品的通过(不通过)检验来判定，因此，本标准要求建立并遵循具有特定要素的过程。实现的方法为：规定要求，让本并列标准的用户决定如何达到这些要求。这与 GB/T 19001 系列中所采取的方法类似。由于期望使用者是具备资格的，因此对细节作了最少的规定。过程的某些部分预期会重复，但是没有给出要求，那是因为重复过程的需要对一个特定的项目而言是唯一的。重复也来自于在设计过程中形成的更深入的理解。

作为过程的部分，出于对过程控制的需要建立文档。此外，允许通过对文档核查以检查其与本标准的过程要求的符合性。**风险管理概要**是文档的一部分，以确保在过程中和过程结束时，**安全性**问题和措施都易于理解。

风险管理并非只针对 PEMS，为说明本标准学科技术的内在复杂性和确保**危害**的早期识别，强调风险管理。如果希望后续的严格性对**安全性**是有效的话，那么，**风险**的早期识别是必要的。

强调只有具备资格的人员才能使用本标准，这样做的目的是为了确保使用者具有熟知基本要素、识别软件保证和危害评定领域广泛而日益增长的文献的能力，因为在可编程医用电气系统开发中出现特定情况时，本并列标准的使用人员需要应用文献中的工具。在开发的早期，经常采用“自上而下”的工具，如故障树分析。当设计进入细节阶段，广泛采用“自下而上”的工具，比如失效模式和效应分析。

术语和定义

术语和定义是以方便读者并使文本简洁的方式给出。已尽力使正文中的要求清楚明了，以使定义不会被认为是要求。

识别、标记和文档

要求 PEMS 可识别，其目的是确保**用户**不会在疏忽时使用错误的或作废版本的软件。因为消除所有**危害**是不可能或不切实际的，所以识别内容要包含**剩余风险**的信息。在这种情况下，制造商最起码的职责是提示**用户**警惕这些**危害**，并提供用于帮助避免和消除**危害**的信息。

文件

要求**风险管理概要**以确保已识别的**危害**的风险得到控制。**风险管理概要**在**开发生存周期**结束时完成。

开发生存周期

要求**开发生存周期**以确保用系统性方式处理**安全性**问题，尤其在复杂系统中，能对**危害**做到早期识别。

需要一个确定的问题解决体系，因为临时方法会带来自身的问题。可以预见的问题包括诸如不一致和不明确的需求、缺少详细规格说明以及在评价过程中发现的缺陷。

风险管理过程

这些要求用于构成一个框架，在该框架中运用经验、见识和判断力进行成功地管理**风险**。

基本概念是：可预见的**风险**越大，要求分析越严格，**风险**控制措施的完整性越高。选择与本并列标准相适应的详细程度。考虑某一特定医疗应用，专用标准将提供更加具体的管理**风险**的方法，包括通过(不通过)要求。

当**危害**因素已经识别时，在**开发生存周期**中全程应用该过程以使合适的风险控制方法得以规定。

风险估计

软件和其他系统性失效本身作为事件可能性或概率的概念是不合适的。尽管如此，本标准的主要目标是减小系统性错误存在的可能性。另一相关关注点为在使用中碰到危害性错误的可能性。在不可量化情况下，负责任的设计过程都要仔细考虑与系统性错误相关的**风险**的因素。**风险**估计在确定设计侧重点和判定结果上都是必要的步骤。如何对系统性软件错误可能性进行定量和定性正在考虑中。

附 录 CCC
（资料性附录）
风 险 概 念

风险

风险概念有两个要素：

——**危害**事件的发生可能性；

——**危害**事件后果的**严重度**。

风险可分为三个区域：

——不容许区；

——合理可行区(ALARP)；

——广泛可接受区。

不容许区

某些**危害**风险的**严重度**是系统所不能容许的。通过降低**严重度**和(或)危害的发生可能性来减小该区域的**风险**。

合理可行区

介于广泛可接受区与不容许区之间称为合理可行区(ALARP)。在合理可行区，权衡接受风险的收益和进一步降低**风险**的代价，**风险**被降低至可行的最低水平。任何**风险**都应该降低至“合理可行区(ALARP)”。在不容许区极限处附近，即使需要相当大的代价通常也需要降低**风险**。

广泛可接受区

在某些情况下，某一**危害**的**严重度**和(或)可能性与其他可接受的**危害**风险相比较可以忽略，那么该**风险**是可接受的。对于这些**危害**，无需刻意追求降低**风险**。

三种**风险**区域概念见图 CCC.1。

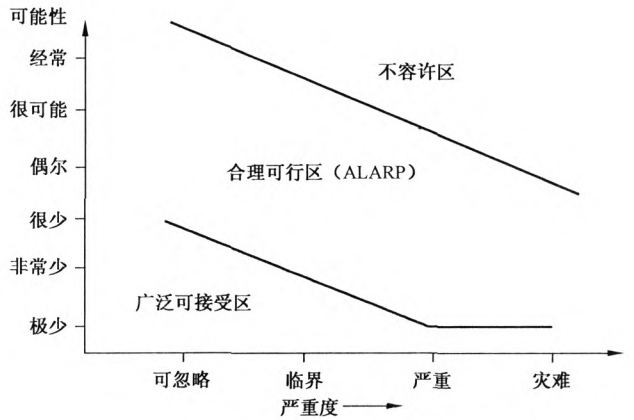

图 CCC.1 风险示意图

严重度等级

严重度是**风险**的要素之一。用于 PEMS 对危害所可能产生的后果定性度量的四种等级建议如下：

——灾难性：潜在的多种死亡或严重伤害；

——严重的：潜在的死亡或严重伤害；

——临界的：潜在的伤害；

——可忽略：较小的或无潜在的伤害。

可接受风险判定

本标准没有规定可接受**风险**。计划在专用标准中给出指南。通常，可接受**风险**是建立在个案基础上的。通过使用**单一故障状态**理论(在通用标准第 3 章)和(或)已在使用中的相似的**医用电气设备**的性

能中获得某些指南。

如果**患者**的预后得到改善，则与 PEMS 相关的风险也许可以接受，但这不能成为接受不必要风险的理由，应该始终应用 ALARP 原则。

风险管理

本标准要求风险管理过程始终贯穿**开发生存周期**。过程的目标是管理**风险**使其小于**最大可容许风险**以及尽可能小到合理可行程度。典型的**风险**管理过程见图 CCC.2。

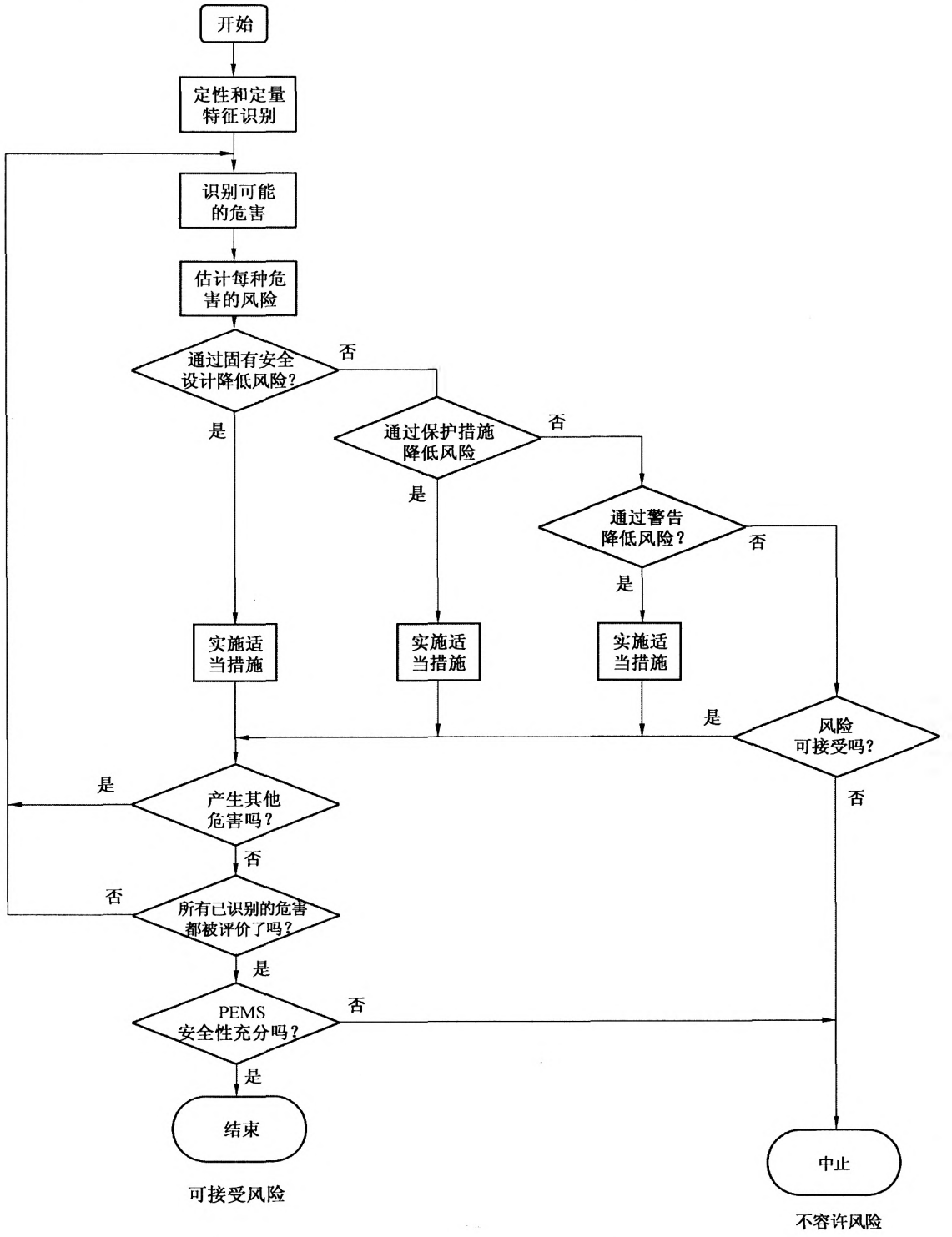

图 CCC.2 风险管理过程

失效原因

系统的失效能导致危害性事件。有两种可能类型的失效：

——随机失效；

——系统性失效。

随机失效

对许多事件而言，失效的统计概率是可以确定的；例如电子组件失效的概率通常可以通过组成零件的失效概率来估计。在这种情况下，失效概率能以数值形式给出。基本的假设为：失效是自然、随机发生的。硬件的失效表现形式既可以是随机方式也可以是系统性方式。软件失效表现为随机方式，然而，软件失效的原因总是系统性的。

系统性失效

系统性失效归因于在**开发生存周期**活动中的错误（包括过度和不足的错误），这些活动在某些特定的输入组合或环境条件下，将会产生一个失效。

系统性失效在硬件和软件上均可发生，并可能产生在产品**开发生存周期**中的任何时候。例如，系统性失效可以是数据库中一个不正确的危害条件的阈值设置。不正确的数据可能被错误地规定；在数据准备阶段被错误地复制，在使用中被错误地更改。此类事件发生的可能性是难于预测的。尽管如此，在开发生存周期中所用的过程的质量和被引入或未发觉而遗留的故障的可能性之间有一定的关系。

风险估计

估计风险可使用不同的方法，本并列标准给出了一个定性风险估计方法的例子。本并列标准并不要求采用某一特定方法，但强烈要求进行风险估计；见 52.204.3.2。当有适当的数据可资利用时，对其进行定量**风险**估计是可能的。定量**风险**估计方法包括定性方法或其他可选择的方法。用于**风险**估计的方法是风险管理过程的一部分，宜在**风险**管理计划中定义；见 52.202.2d）。

图 CCC.1 中的风险图可用来定义风险水平。

风险水平都能落在其中的某一风险区域内，即：不容许区、合理可行区、广泛可接受区。

图 CCC.1 是风险图例子；仅是一个方法示例，不意味它对可编程医用电气系统是通用的。如果风险图方法用于估计**风险**，那么，宜在该应用中对特定的风险图和使用的说明进行合理性论证。

正确性能的可能性

52.204.4.3 要求对概率进行定性或定量的规定。有关如何实现的建议如下。

定量可能性

当失效的概率可以计算或证明时（例如，对一个电子硬件统基于随机失效的计算），该数据可以用来说明正确性能的可能性。在要求时，它可以典型地以两次失效之间的平均时间或失效概率来表示。

定性可能性

当失效是系统性的，且原因与软件有关，通常要进行失效概率的计算或论证是不可行的。在该情况下，可以采用定性的方法规定和验证可能性。

本标准不要求任何确定系统性失效概率的定性度量的特定方法。仅是指导性的方法。

该方法的基本思想是：用于生产 PESS 的过程越严格质量越高，那么，PESS 就越可能执行其预期的功能。这些过程可包括：

——开发方法和技术；

——体系结构选择；

——质量保证；

——项目管理。

根据当前的技术，对特定情况，无法确定哪种方法适用那些过程。本标准的用户宜基于现实可行、并基于 ALARP 原则做出最佳的判断。

确定有关于所采用的过程和软件执行预期风险减小(措施)之间的关系的进一步指南，见附录 FFF 中的参考文献[5]和[7]。在参考文献[5]中的术语“安全完整性”用于规定 PESS 实现其预期功能的可能性。

附 录 DDD
（资料性附录）
开发生存周期

开发生存周期模型—设计和实现

在应用**开发生存周期**模型时，设计和实现包括选择：

a） 软件开发方法；

b） 电子组件；

c） 计算机辅助软件工程(CASE)工具；

d） 冗余硬件；

e） **可编程医用电气系统**人—机接口；

f） 能量源；

g） 环境条件；

h） 编程语言；

i） 第三方软件。

这些设计环境的要素在设计和实现过程中既可用通用的方式也可用它们在设计和实现过程中的特殊方式说明。

确认是设计用于确保生产正确的产品。在**开发生存周期**的最后阶段，对可编程医用电气系统整体的确认可包括大容量的数据测试、高负载或强度的测试、人为因素的测试、保密测试、性能测试、配置的兼容性测试、故障测试、用户文档和**安全性**要求实现情况的测试。

符合本并列标准，要求规定并遵循**开发生存周期**；虽然不要求采用特定**开发生存周期**，但的确要求开发生存周期在其中是有特定作用的。相关要求见 52.203。

图 DDD.1 图解说明了**开发生存周期**模型。在该模型中，集成过程跟随分解过程。由于设计是根据需求分解而来的，所以功能构建模块、体系结构、技术是确定的。当设计信息能使**可编程医用电气系统**组件构建时(如电路图和软件代码)，则分解过程结束。在完成分解后，组件将被集成在一起。当完成组件集成后，将通过**验证**确定该实现是否满足要求。在集成过程结束时，**确认可编程医用电气系统**是否按预期目的工作。

文档

本并列标准要求所应用的**开发生存周期**规定文档要求。尽管如此，但不规定文档和**开发生存周期**的关联性。表 DDD.1 建议了文档要求与**开发生存周期**各阶段的相互关系。

所要求的文档之一是**风险管理概要**，它有来自如下所有阶段的贡献：

——已识别的**危害**以及产生原因…… 52.204.3.1.10

——已估计的**风险** …… 52.204.3.2.5

——控制**风险**要求 …… 52.204.4.5

——**验证**方法和结果的证明 …… 52.209.4

——**风险**控制有效性评价 …… 52.204.4.6

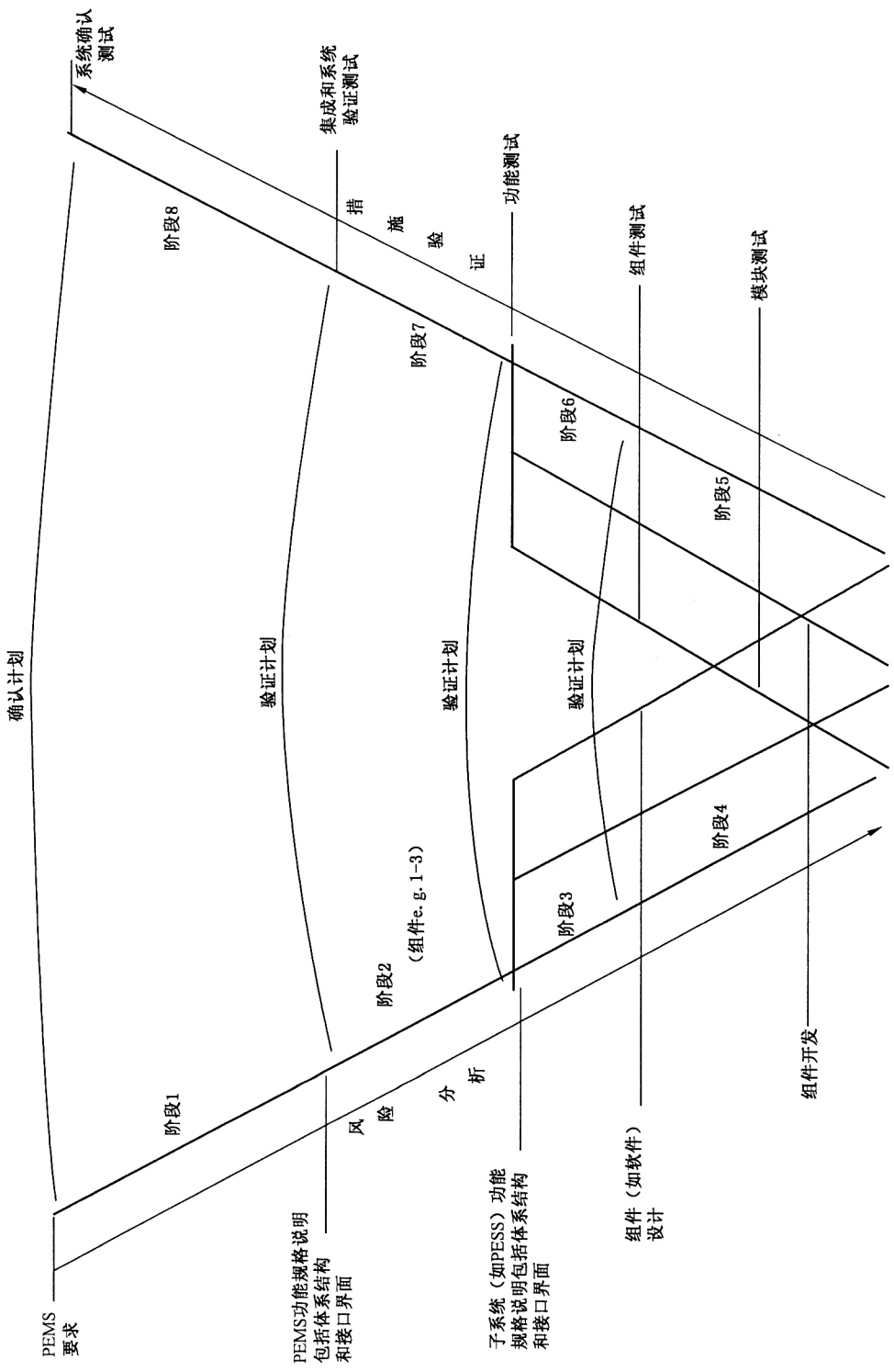

图 DDD.1 一个用于 PEMS 开发生存周期的模型

表 DDD.1 文档要求与开发生存周期各阶段相互关系建议

文档	阶段							
	1	2	3	4	5	6	7	8
已识别的危害以及产生原因 …… 52.204.3.1.10	*	*	*					
已估计的风险 …… 52.204.3.2.5	*	*	*					
控制风险要求 …… 52.204.4.5	*	*	*					
风险管理计划 …… 52.202	*							
开发生存周期 …… 52.203	*							
PEMS需求规格说明 …… 52.206	*							
验证计划 …… 52.209.2	*							
确认计划 …… 52.210.2	*							
子系统(例如PESS)需求规格说明 …… 52.206		*						
PEMS体系结构规格说明 …… 52.207.2		*						
PESS体系结构规格说明 …… 52.207.2			*					
子系统设计规格说明 …… 52.208.1			*					
子系统测试规格说明 …… 52.208.1			*	*				
验证方法和结果 …… 52.209.4				*	*	*	*	
确认方法和结果 …… 52.210.7								*
风险控制有效性评价 …… 52.204.4.6								*
剩余风险 …… 6.8.201								*
评价报告 …… 52.212								*
风险管理概要 …… 52.201.3	*	*	*	*	*	*	*	*
* 建议文档所对应的阶段。								

附 录 EEE
（资料性附录）
可编程医用电气系统(PEMS)/可编程电子子系统(PESS)体系结构例子

可编程医用电气系统可以是一个非常简单的医用电气设备或者是一个复杂的医用电气系统，或者介于二者之间。

图 EEE.1 给出了一些可编程医用电气系统(PEMS)可能的例子。

图 EEE.1 a)给出了一个复杂系统。可编程医用电气系统分解为若干个主要的子系统，而子系统由包含 PESS 的子系统组成。

图 EEE.1 b)给出了一个较简单的实现。在本例中没有中间层的主要子系统，PESS 是 PEMS 本身的子系统。

图 EEE.1 c)给出了一个最简单的可编程医用电气系统。其中可编程医用电气系统(PEMS)与可编程电子子系统(PESS)相同。

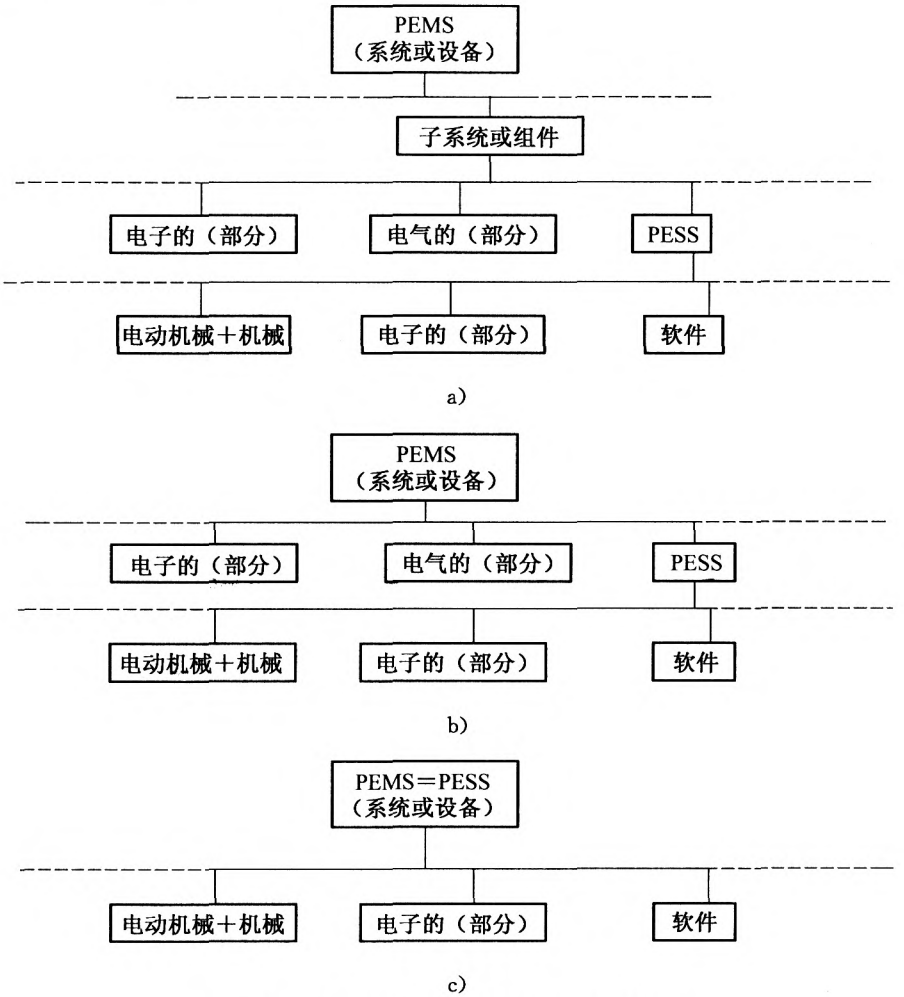

图 EEE.1 PEMS/PESS 体系结构例子

附 录 FFF
（资料性附录）
参 考 文 献

本附录所列的参考文献是为读者提供风险管理方法和过程方面的指导。

[1] IEC 60513:1994 医用电气设备安全标准基本方面

[2] IEC 60812:1985 系统可靠性分析技术 故障模式和影响分析程序(FMEA)

[3] IEC 60880:1986 核电站安全系统的计算机软件
IEC 60880 增补(45A(Sec)189CD 和 45(UK)98)

[4] IEC 61025:1990 故障树分析(FTA)

[5] GB/T 20438—2006 电气/电子/可编程电子安全相关系统的功能安全
——第 1 部分:一般要求
——第 2 部分:电气/电子/可编程电子安全相关系统的要求
——第 3 部分:软件要求
——第 4 部分:定义和缩略语
——第 5 部分:确定安全完整性等级的方法示例
——第 6 部分:GB/T 20438.2 和 GB/T 20438.3 的应用指南
——第 7 部分:技术和措施概述

[6] GB/T 17544—1998 信息技术软件包质量要求和测试

[7] GB/T 18492—2001 信息技术 系统和软件完整性级别

[8] prEN 1441:1994 医疗器械/风险分析

中华人民共和国医药
行业标准
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
YY/T 0708—2009/IEC 60601-1-4:2000
*
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 1.75 字数 41千字
2010年4月第一版 2010年4月第一次印刷
*
书号:155066·2-20718 定价 27.00元

YY/T 0708-2009