**医疗器械软件描述文档**

1. **基本信息**
	1. **产品标识**

软件名称：

软件型号：

软件版本号：

软件制造商：

软件生产地址：

* 1. **安全性级别**

软件的安全性级别为A/B/C级。理由如下：

1. 软件的预期用途为：
2. 软件的功能包括：
3. 如果软件失效，可能导致以下后果（按软件各功能失效逐条描述，如果软件失效的时候由硬件降低失效后果或危害发生概率，可以做说明，并由此降低安全性级别）：
4. ……
5. ……
6. ……
	1. **结构功能**
		1. **组成模块、各模块功能及模块相互关系**

依据软件设计规格给出体系结构图（如图1.3-1所示）。

嵌入式软件（SDS）体系结构图——示例1



独立式软件（SDS）体系结构图——示例2



图1.3-1 XXX体系结构图

* + 1. **各模块功能说明**

 系统主要由XXXXXX模块组成。各模块功能简介如下：

|  |  |  |  |
| --- | --- | --- | --- |
| 产品名称 |  | 版本号 |  |
| 模块名称 |  |
| 软件功能项目 | 功能说明 |
| 一级功能 | 二级功能 | 三级功能 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
| 模块名称 |  |
| 软件功能项目 | 功能说明 |
| 一级功能 | 二级功能 | 三级功能 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

注：1、**每个软件模块一份表单**。

 2、软件功能项目列表需列出与测试相关的所有功能（包括各级子功能）。

 3、功能说明栏目应填写：功能项目概述、**边界值规定（数据有效性）**、安全说明等信息。

 4、功能列表上所列出来的功能必须是可以实现或演示的。

 5、功能名称与软件、文档保持一致。

 6、**软件功能项目列表根据需要列出**（可增加或删减子功能列）。

* + 1. **用户界面设计**

 采用广泛应用的图形用户界面（GUI），即诸如窗口、菜单、对话框、滚动条等。用户主界面见图1.3-2。

图1.3-2 XXX用户主界面

* + 1. **外部接口**

 XXX可使用VISUAL C++ 提供的对 SQL SERVER 的接口，进行对数据库的所有访问。

 XXX可使用SQL SERVER 的对数据库的备分命令，以做到对数据的保存。

 在网络软件接口方面，使用一种无差错的传输协议，采用滑动窗口方式对数据进行网络传输及接收。

* 1. **硬件关系**
		1. **物理拓扑图**

嵌入式软件物理拓扑关系表格形式——示例1

|  |  |
| --- | --- |
| 硬件 | 软件 |
| 分类 | 零件 | 种类 | 功能 |
| 显示部分 | 血压显示7工具LED | 血压值显示 | 最高血压・最低血压、脈拍を表示 |
| 时刻显示7工具LED | 時刻显示 | 显示现在时刻 |
| 压力单位显示LED  | mmHg / kPa 显示 | 显示血压值以及压力值的单位 |
| 开关部分 | 开始/关闭开关 | 开始/关闭开关读取控制 | 开始测量血压测量时停止测量 |
|  | 背面功能设定开关 | 背面功能设定开关读取控制 | 时刻的设定等、主机功能设定的更改 |
| 打印部分 | 打印切纸 | 打印控制 | 测量结果的打印、打印后切纸 |
| 血压测量部分 | 泵、电磁阀、压力传感器 | 血压测定控制 | 测量时加压、减压控制、脉搏信号处理以及测量值的确定 |
|  | 安全监视用压力传感器 | 压力安全检测控制 | 压力监测、急排控制 |
| 袖带驱动部分 | 袖带驱动用马达 | 袖带控制 | 袖带的卷曲、固定、开放 |
| 语音部分 | 扬声器 | 语音控制 | 测量通知 |
| 外部进出力部 | 串行通信 | 串行进出力 | 测量结果出力、指令输入 |
| 记忆存储 | U盘 | 设定值记忆存储控制 | 功能设定内容的保持 |

嵌入式软件物理拓扑关系表格形式——示例2

独立式软件物理拓扑关系表格形式——示例3

图1.4-1物理拓扑图

* + 1. **连接关系描述**

与PC连接

与医疗器械硬件连接

* 1. **运行环境**
		1. **硬件配置**

处理器:

储存器

外设器件

输入/输出设备

……

* + 1. **软件环境**

系统软件：

支持软件：

必备软件：

选配软件：

杀毒软件：

……

* + 1. **网络条件**

 网卡：

网络类型:

网络架构：

* 1. **适用范围**

独立软件：软件的适用范围和适用人群。

软件组件：同医疗器械产品的适用范围和适用人群。

* 1. **禁忌症**

独立软件：软件的禁忌症和不适用人群。

软件组件：同医疗器械产品的禁忌症和不适用人群。

* 1. **上市历史（软件组件写医疗器械的上市历史）(表格形式)**

国产首次注册示例：

该医疗器械，产品名称为XXXXX，据产品结构及预期用途，按《医疗器械分类目录》分为6870类软件，按照二/三类医疗器械进行首次注册。

**进口**（首次/重新）

该医疗器械作为XXX的组件，在中国（首次/重新）申请上市。依据产品结构及预期用途，按《医疗器械分类目录》分为68xx-xx类。上市历史详情见下表：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 上市国家 | 管理类别 | 上市时间 | 版本号 | 现版本号 |
| 原产国 |  |  |  |  |
| （中国） |  |  |  |  |
| 欧洲（如有） |  |  |  |  |
| 美国（如有） |  |  |  |  |
| … |  |  |  |  |

1. **实现过程**

**2.1 开发综述**

我司于XXXX年XX月开始XX软件的开发工作。整个开发过程包括可行性研究和项目开发计划、需求分析、概要设计、详细设计、编码、集成、测试等6个阶段，并编制相应开发文档。本软件开发采用XXXX模型。在开发过程中，采用的语言、工具和方法分别为：

1. 语言：本软件开发采用XX语言；
2. 工具：
* 软件需求工具：XXXXX，版本：XXXXXX，来源（制造商）：XXXXXX；
* 设计工具：
* 构造工具：
* 测试工具：
* 维护工具：
* 配制管理工具：
* 缺陷管理工具：
* ……
1. 开发方法：本软件采用XXXXX方法；

在开发过程中，开发人员为XXX人，开发时间为XX月，工作量为XXXX人月。

代码行共XXXX行，控制文档XXXX个。

**2.2 风险管理**

风险管理报告全文，见附件1。XXX风险管理报告（文件号：xxx 版本：xxx）

**2.3需求规格 (SRS)**

《需求规格说明书》（SRS）全文，见附件2。《需求规格说明书》（文件号：xxx 版本：xxx）

**2.4生存周期**

《软件开发计划》（SDP）摘要见附件3。

《软件配制管理计划》（SCMP）摘要见附件4。

《软件维护计划》摘要见附件5。

《生存周期实施情况核查表》见附件6。

**2.5验证与确认**

《软件验证与确认计划》见附件7。

在软件开发过程中，进行了以下测试：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 测试 | 测试文档 | 编号 |
|  | XXX单元测试 | XXX单元测试计划 |  |
| XXX单元测试报告 |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

各测试文档详见附件8

**2.6缺陷管理**

**2.6.1缺陷管理的流程**

缺陷管理流程为：

|  |  |  |  |
| --- | --- | --- | --- |
| 步骤 | 工作 | 主要内容 | 负责人 |
| 1 | 缺陷报告 |  |  |
| 2 |  |  |  |
| **……** |  |  |  |

**2.6.2缺陷总数和剩余数**

开发过程中发现缺陷xx个，上市后剩余缺陷数为xx个。

剩余缺陷描述、严重度、整改计划为：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 缺陷描述 | 严重度 | 整改计划 | 计划完成时间 |
|  |  |  |  |  |
|  |  |  |  |  |

**2.7修订历史**

软件版本的命名规则：软件的版本号为 XX.XX.XXXXX的形式，版本号中，第一位是xx，代表：XXXX，第二位是xx，代表……。

本软件修订历史

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 软件版本 | 修订日期 | 修订类型 | 变更内容描述 |
| 1 |  |  |  |  |
| 2 |  |  |  |  |
| 3 |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**2.8临床评价**

参考医疗器械软件描述文档 附件9

“《临床评价报告》（文件号：**xxx** 版本号**xxx**）”。

 ——与注册资料7临床评价资料一致。

**3核心算法概述**

算法类型：

公认成熟算法：公开文献专利标准、原理简单明确、上市超过四年且无不良事件。公认成熟算法列明名称、原理、用途，全新算法列明名称、原理、用途，并提供验证资料。

全新算法：源自科学研究和临床数据

内容：

实质首次注册：所有核心算法

实质重新注册：新增核心算法

附件1

**XXX风险管理报告**

附件2

**XXX需求规格说明书（SRS）**

1. 引言
	1. 编写目的

为了明确“XXXXX”项目的需求，为用户和分析设计人员之间的交流提供方便，更好地安排项目规划与进度，组织软件开发与测试，减少项目风险，撰写本需求规格规格说明书。

本需求规格说明书的读者为项目经理、分析设计人员、程序员、质量保证人员、维护人员以及客户方的相关人员。

* 1. 项目背景
	2. 定义

GB/T 11457所列术语和下列定义适用于本指南。

合同：指XXXX共同签署的关于本项目的合同。

客户：指XXXX公司。

语言：是指具有语法和语义的通信工具，包括一组表达式、惯例和传递信息的有关规则。

编程语言：是指用于编写源程序的高级语言和汇编语言。

用户：XXXXXX

……

* 1. 参考资料
1. GB/T 11457 软件工程术语
2. GB 8566 计算机软件开发规范
3. GB 8567 计算机软件产品开发文件编制指南
4. GB/T 12504 计算机软件质量保证计划规范
5. GB/T 12505 计算机软件配置管理计划规范
6. GB/T 19001 质量管理体系
7. ISO9001 质量管理体系
8. ISO9000-3质量管理体系
9. ISO/IEC 12207软件生命周期过程标准
10. ISO/IEC TR 15504软件过程评估标准
11. IEEE1058.1软件项目管理计划标准
12. CMM 2.0 能力成熟度模型
13. PMBOK项目管理知识体系
14. 项目计划任务书
15. 项目开发计划
16. 设备用户手册

……

1. 总体描述
	1. 目标
		1. 开发意图、应用目标
2. 开发意图：

XXXX。

1. 应用目标：

XXXX

* + 1. 产品描述

（描述产品的基本要求、主要部分、外部接口等可使用框图展示较大系统的主要部分、相互关系、外部接口等））

* + - 1. 软件系统总体结构图

采用基于采用 MVC 模式架构的开发方式，实现的系统具有界面美观、操作简单、开发系统容易升级、系统开发周期短、成本低等优点。在项目的研发中，从体系结构上将本系统设计为4层结构：

系统结构图

（结构图说明）

* + - 1. 软件系统总体数据流图 （图示及说明）
			2. 系统功能的总体用况图 （图示及说明）
			3. 约束：
	1. 系统接口；

（列出每个系统接口，识别完成系统需求的软件功能以及与系统匹配的接口描述。）

* 1. 用户界面；

（如要求的屏幕显示格式、页面、版式、报告内容、菜单内容等）

* 1. 硬件接口；

（如支持的设备，采用的协议等）

* 1. 软件接口；

（与其他软件的接口，软件应提供名称、助记符、规格说明编号、版本号、来源，接口软件的目的等）

* 1. 通信接口；

（如局域网协议等）

* 1. 内存约束；

（对主存、辅存的任何使用特征和限制）

* 1. 运行；

（如用户引发的操作、交互操作的周期、无人值守操作的周期、数据处理支持能力、备份和回复操作）

* 1. 现场适应性需求

（给定现场、任务和运行模式的需求）

* 1. 产品功能

描述软件的将执行主要功能的概要。（可用文本或图示的方法，显示不同功能及其之间的关系，显示变量之间的逻辑关系）

* 1. 用户的特点
1. 管理员：。
2. 用户1：
3. 用户2：
	1. 约束条件

经费限制：

时间限制：

硬件局限：

方法、技术、环境：

法规：

标准：

并行操作：

审核功能：

……

1. 具体需求
	1. 外部接口

各接口描述包括以下内容：

* + - * 1. 项的名称；
				2. 目的描述；
				3. 输入源和输出目的地；
				4. 有效范围、准确度和容限；
				5. 测量单位；
				6. 定时；
				7. 与其他输入/输出的关系；
				8. 屏显格式；
				9. 窗口格式；
				10. 数据格式；
				11. 命令格式；
				12. 结束消息。
			1. 用户接口

* + - 1. 硬件接口

* + - 1. 软件接口

* + - 1. 通信接口
	1. 功能需求
		1. 用户注册功能

系统应能完成用户注册功能

* 主参加者：用户
* 环境目标：
* 前置条件：数据库有足够的空间。
* 触发器：用户进入注册界面。
* 场景：
1. 用户进入注册界面。
2. 用户输入会员名。
3. 用户输入登录密码。
4. 用户输入确认密码。
5. 用户输入其他个人基本信息。
6. 用户输入验证码。
7. 点击确认按钮，提交注册信息。
* 异常：
1. 用户注册的会员名已在系统中存在时，给出提示信息，让其更改所输入的会员名。
2. 用户输入的确认密码与登录密码不一致时，给出提示信息，让其重新输入密码。
3. 用户输入的验证码错误时，给出提示信息，随机更换验证码的图片后，让其重新输入验证码。
* 优先级：必须被实现。
* 何时可用：首次开发。
* 使用频率：每天多次。
* 后置条件：用户完成操作后显示注册成功信息。
* 活动图

* + 1. …………

* 1. 性能需求
		1. 支持的终端数：
		2. 支持同时运行的用户数量；
		3. 要处理的信息量和类型：
		4. 精度
		5. 速度：
		6. 人身和环境安全性需求
	2. 数据库逻辑需求

（规定将置于数据库的任何信息的逻辑需求，可包括：）

不同功能使用的信息类型；

使用频度；

访问能力；

数据实体及其之间的关系；

完整性约束；

数据保存要求

* 1. 设计约束

（描述由可能由其他标准、硬件局限等引发的设计约束）

* 1. 软件系统属性
		1. 可靠性
		2. 可用性
		3. 保密性需求
1. 对注册过的用户个人信息的严格保密，除用户自己以及管理员之外，其他人不能查阅用户信息。
2. 对数据传输过程需有严格的保密机制，防止用户数据的泄露。
3. 对于管理员要分发给管理数据库的权限。
	* 1. 可维护性
		2. 可移植性

附件3

**XXX软件开发计划（SDP）摘要**

1. 引言

本条应简述本文档适用的系统和软件的用途，它应描述系统和软件的一般特性；概述系统开发、运行和维护的历史；标识项目的投资方、需方、用户、开发方和支持机构；标识当前和计划的运行现场；列出其他有关的文档。

1. 实施整个软件开发活动的计划
	1. 软件开发过程

本条应描述要采用的软件开发过程。计划应覆盖论及它的所有合同条款，确定已计划的开发阶段（适用的话）、目标和各阶段要执行的软件开发活动。

* 1. 软件开发总体计划
		1. 软件生存周期

描述预期采用的生存周期模型，并进行说明

* + 1. 软件开发方法

本条应描述或引用要使用的软件开发方法，包括为支持这些方法所使用的手工、自动工具和过程的描述。该方法应覆盖论及它的所有合同条款。

* + 1. 可重用的软件产品

本条应描述标识、评估和吸纳可重用软件产品要遵循的方法，包括搜寻这些产品的范围和进行评估的准则。描述应覆盖合同中论及它的所有条款。在制定或更新计划时对已选定的或候选的可重用的软件产品应加以标识和说明，（若适用）同时应给出与使用有关的优点、缺陷和限制。

* + 1. 处理关键性需求

本条应分以下若干条描述为处理指定关键性需求应遵循的方法。描述应覆盖合同中论及它的所有条款。

1. 进度表和活动网络图

本章应给出：

a． 进度表，标识每个开发阶段中的活动，给出每个活动的初始点、提交的草稿和最终结果的可用性、其他的里程碑及每个活动的完成点；

b． 活动网络图，描述项目活动之间的顺序关系和依赖关系，标出完成项目中有最严格时间限制的活动。

1. 项目组织和资源
	1. 项目组织

本条应描述本项目要采用的组织结构，包括涉及的组织机构、机构之间的关系、执行所需活动的每个机构的权限和职责。

* 1. 项目资源

 本条应描述适用于本项目的资源。（若适用）应包括：

 a．人力资源，包括：

 1) 估计此项目应投入的人力（人员／时间数）；

 2) 按职责（如：管理，软件工程，软件测试，软件配置管理，软件产品评估，软件质量保证和软件文档编制等）分解所投入的入力；

 3) 履行每个职责人员的技术级别、地理位置和涉密程度的划分；

 b．开发人员要使用的设施，包括执行工作的地理位置、要使用的设施、保密区域和运用合同项目的设施的其他特性；

 c．为满足合同需要，需方应提高的设备、软件、服务、文档、资料及设施，给出一张何时需要上述各项的进度表；

 d．其他所需的资源，包括：获得资源的计划、需要的日期和每项资源的可用性。

附件4

**XXX软件配置管理计划（SCMP）摘要**

1. 软件配置管理活动

本章描述配置标识、配置控制，配置状态记录与报告以及配置检查与评审等四方面的软件配置管理活动的需求。

* 1. 配置标识
		1. 本条必须详细说明软件项目的基线（即最初批准的配置标识）

 在软件生存周期中，主要有三种基线，它们是功能基线、分配基线和产品基线。对于每个基线，必须描述下列内容：

 a． 每个基线的项（包括应交付的文档和程序）；

 b． 与每个基线有关的评审与批准事项以及验收标准；

 c． 在建立基线的过程中用户和开发者参与情况。

 例如，在产品基线中，要定义的元素可以包括：

 a． 产品的名字和命名规则；

 b． 产品标识编号；

 c． 对每一个新交付的版本，要给出版本交付号、新修改的描述、修改交付的方法、对支持软件的修改要求以及对有关文档的修改要求；

 d． 安装说明；

 e． 已知的缺陷和故障；

f． 软件媒体和媒体标识。

* + 1. 本条必须描述本项目所有软件代码和文档的标题、代号、编号以及分类规程

例如，对代码来说：

 a． 编译日期可以作为每个交付模块标识的一部分；

b． 在构造模块源代码的顺序行号时，应使它适合于模块作进一步的修改。

* 1. 配置控制
		1. 本条必须描述软件生存周期中各个阶段使用的修改批准权限的级别
		2. 本条必须定义对已有配置的修改申请进行处理的方法

 其中包括：

 a． 详细说明在本计划第3.2条描述的软件生存周期各个阶段中提出修改申请的程序（可以用注上自然语言的流程图来表达）；

 b． 描述实现已批准的修改申请（包括源代码、目标代码和文档的修改）的方法；

 c． 描述软件库控制的规程，其中包括库存软件控制、对于适用基线的读写保护、成员保护、成员标识、档案维护、修改历史以及故障恢复等七项规程；

d． 如果有必要修补目标代码，则要描述其标识和控制的方法。

1. 工具、技术和方法

 本章必须指明为支持特定项目的软件配置管理所使用的软件工具、技术和方法，指明它们的目的，并在开发者所有权的范围内描述其用法。例如，可以包括用于下列任务的工具，技术和方法：

 a． 软件媒体和媒体文档的标识。

 b． 把文档和媒体置于软件配置管理的控制之下，并把它正式地交付给用户。例如，要给出对软件库内的源代码和目标代码进行控制的工具、技术和方法的描述；如果用到数据库管理系统，则还要对该系统进行描述。又如，要指明怎样使用软件库工具、技术和方法来处理软件产品的交付。

 c． 编制关于程序及其有关文档的修改状态的文档。因此必须进一步定义用于准备多种级别（如项目负责人、配置控制小组、软件配置管理人员和用户）的管理报告的工具、技术方法。

附件5

**XXX软件维护计划摘要**

1. 维护范围
	* 1. 改正性维护
		2. 适应性维护
		3. 完善性维护
		4. 预防性维护
2. 维护工作流程

附件6

**XXX软件生存周期实施情况核查表（YY/T 0708）**

|  |  |  |  |
| --- | --- | --- | --- |
|  | 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241。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/T19001-2000中的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 |  |
|  | e) | 验证证明 |  |
|  |  | 通过检查风险管理文档核查其符合性 |  |
|  | 52.202.1 | 制造商应制定风险管理计划。 |  |
|  | 52.202. 2 | 计划应包括以下内容: |  |
|  | a) | 计划的范围，确定项目或产品以及该计划适用的开发和生存周期的各阶段； |  |
|  | b) | 使用的开发生存周期（见52.203），包括验证计划的开发生存周期的各阶段； |  |
|  | 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 |  |
|  |  | 通过检查风险管文档核查其符合性 |  |
|  | 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.根据间题，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〕; |  |
|  |  | —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; |  |
|  |  | 一确定验证持续符合性的步骤。 |  |
|  | 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; |  |
|  |  | 一对维护人员的危害; |  |
|  |  | —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，包括入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、溅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)侧试。 |  |
|  | 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。 |  |
|  | 5.2.11.2 | 在开发生存周期中所有的相关文件，应依照GB/T 19001一2000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。 |  |
|  | 52.2 1 | 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。 |  |

附件7

**XXX软件****验证与确认计划（SVVP）**

* + - 1. 目的
			2. 引用文件
			3. 术语和定义
			4. V&V综述
	1. 组织
	2. 主进度
	3. 资源摘要
	4. 职责
	5. 工具、技术和方法
		+ 1. V&V过程
	6. 活动：概念V&V

（标识要执行的V&V的任务，描述每个V&V任务要求的输入、输出、进度、进度、资源等）

* 1. 活动：需求V&V
	2. 活动：设计V&V
	3. 活动：实现V&V
	4. 活动：测试V&V
	5. 活动：安装和检验V&V
	6. 活动：运行V&V
		+ 1. V&V报告

附件8

**XXX软件测试文档**

**XXXX测试计划**

1 测试计划标识符

AP05-0103

1. 引言

2.1 目标

 公司XX系统的系统测试计划应该支持以下目标：

 (1) 细化准备和进行系统测试所需要的活动。

 (2) 与所有负责方沟通有关他们要执行的任务以及执行任务时所安排的进度。

 (3) 确定用来准备计划的信息源。

(4) 确定进行系统测试所需要的测试工具和环境。

2.2背景

 去年，XYZ公司系统和程序开发部门应公司会计部门的要求开发了一个新的通用总帐系统。与此同时，还提出要求要开发一个与该通用总帐系统接口的新的公司工资系统。

管理层系统评估委员会在19\*\*年9月批准了开发工资系统的请求，并且指定一个工资系统顾问组来确定系统需求。顾问组于19\*\*年12月完成了一份需求陈述(AP01-01)和一份初步开发计划。

2.3范围

该测试计划覆盖了公司工资系统的全部系统测试，包括操作者和用户规程、以及程序和作业控制。除了综合性多程序功能性测试外，还应评估外部接口、安全、恢复和性能。

2.4 引用文件

 下列文档用作该测试计划的信息源：

 公司工资系统初步开发计划(AP01-02)

 公司工资系统授权(AP01-03)

 公司工资系统最终开发计划(AP01-06)

 公司工资系统质量倮证计划(AP01-08)

 公司工资系统配置管理计划(AP01-09)

 XYZ公司系统开发标准及规程(XYZ01-0100)

 公司通用总帐系统设计描述(AG01-04)

公司通用总帐系统测试计划(AG05-01)

3测试项

 组成公司工资系统的所有项在系统测试期间应予测试。待测试的版本应由配置管理员放在合适的库中。管理员还应控制对受试版本的更改，并且将可提供新版本的时间通知测试组。

 以下文档为规定正确的操作建立基础：

 公司工资系统需求规格说明(AP01-01)

 公司工资系统设计描述(AP01-04)

 公司工资系统参考手册(AP02-01)

公司工资系统模块参考手册(AP02-03)

GB/T 9386-2008

要测试的各项列出如下：

3.1 程序模块

要测试的程序模块按以下规则来标识：

类型 库 成员名称

源代码 SOURLIB1 AP0302

AP0305

可执行代码 MACLIBI AP0301

AP0302

AP0305

3.2 作业控制规程

 应用程序、分类和实用程序的控制规程标识如下：

 类型 库 成员名称

 应用程序 PROCLIBl AP0401

分类 PROCLIB1 AP0402

实用程序 PROCLIBI AP0403

3.3用户规程

公司工资系统用户事务参考手册(AP02-04)中规定的在线规程应予测试。

3.4操作者规程

系统测试包括公司工资系统操作参考手册(AP02-02)中规定的规程。

4要测试的特征

 以下清单列出待测试的特征：

测试设计

说明编号 描述

AP06-01 数据库转换

AP06-02 月薪雇员全面的工资处理

AP06-03 计时雇员全面的工资处理

AP06-04 所有雇员全面的工资处理

AP06-05 定期报告

AP06-06 通用总帐事务的建立

AP06-07 安全

AP06-08 恢复

AP06-09 性能

5不要测试的特征

 下列特征不应包括在系统测试中，因为它们在系统初始安装时不会使用。

 平等就业机会委员会符合性报告

内部培训进度报告

工资／业绩审查报告

 二期开发阶段文档集应包含关于这些特征的一个测试计划。

 测试用例将不会覆盖正在受试的事务或者报告中所有可能的选项组合。只有目前XYZ公司工资处理明确需求的组合应予测试。

6 方法

 测试人员应根据系统文档集准备所有的测试设计、用例以及规程说明。这种方法应验证测试所覆盖那些领域的文档集信息的准确性和综合性。

 公司工资和会计部门的人员应协助开发测试设计和测试用例，这样做有助于确保测试能体现系统的实际使用。

 为了确保保密性，从会计文件中选取的所有测试数据应含有已更改的保密敏感字段。

6.1 转换测试

 除了计算输入和输出的记录外，转换数据库的有效性应以两种方式进行验证。第一种验证方法涉及到使用必须由开发组建立的“数据库审核员”功能。当针对被转换数据库运行时，数据库审核员应核对一条记录内的数值范围，以及要求的各条记录之间的关系。

 第二种验证方法涉及到随机选取旧记录的一个小的子集，然后直接与新记录的相对应子集进行比较。直接比较的数目“c”和旧记录的数目“r”必须加以规定。从1到r的范围内产生由随机数字组成的c集合。在转换过程中，该集合应予以分类和应用，以驱动对宣接比较记录的选择。

 注：同样的两种验证方法在实际的转换期间应予采用。

6.2作业流测试

 月薪雇员和计时雇员的记录综合集以及这两种记录的合并集应用于测试工资处理。标准的作业流测试方法应予采用。

 每种定期报告作业流至少运行一次。

6.3接口测试

 为了测试工资系统与通用总帐系统之间的接口，工资系统应建立一个通用总帐事务综合集。这些事务应输入到通用总帐测试系统。生成的通用总帐条目必须加以选取、打印并与由工资系统准备的通用总帐事务的打印输出相比较。

6.4安全测试

 无妥当口令但又试图访问在线数据条目并显示事务的情况应予测试。

6.5恢复测试

 在可单独运行的时间内，通过停机且随后依照恢复规程进行恢复测试。

6.6性能测试

 依据性能要求(AP01-01)，通过利用产生的数据量测量若干作业的运行时间，以此来评估性能。

6.7 回归测试

 假设为了测试在系统测试期间做过的程序修改，则应对系统进行若干次重复测试。对系统的每一新版本应做一次回归测试，从而检测由于程序修改所导致的意想不到的影响。

 应通过对新版本执行前一版本曾执行的那些所有测试来完成回归测试，然后对由此得到的结果文件进行比较。标准的比较器程序(UT08-0100)应予采用，以便比较所有的系统输出。

6.8综合性

 公司工资系统参考手册( AP02-01)中描述的每个系统特征至少应有一份相关联的测试设计说明。公司工资系统用户事务参考手册(AP02-04)中所规定的每个用户规程至少应予测试一次。公司工资系统操作手册(AP02-02)中规定的每个操作规程至少也应予测试一次。另外，每个作业控制规程至少应予执行一次。

 对于关联到上述每个领域的测试设计说明，应采用覆盖矩阵予以核查。

6.9约束

 公司工资系统的最终执行日期定于19\*\*年8月31号。必须符合这个日期，因为新的ABC部门将于9月1日开始全面运行，必须拥有这个系统方能向其雇员发放工资。

7 测试项通过准则

该系统必须符合XYZ公司系统开发标准和规程(XYZ01-0100)中陈述的系统通过／失败的标准需求。该系统还必须满足下列需求：

——内存需求一定不要大于真实存储量64k。

——用户规程与其他会计系统的一致性必须使工资主管满意。

8暂停准则和恢复要求

8.1暂停准则

 不能转换雇员信息数据库会导致所有测试活动的暂停。

8.2恢复要求

 出现测试暂停后，当系统的新版本向测试组传递时，6.7条中描述的回归测试应予执行。

9测试交付项

1. 系统测试组应形成下列文档，这些文档在测试结束后交付给配置管理组。

 测试文档

 系统测试计划；

 系统测试设计说明；

 系统测试用例说明；

 系统测试规程说明；

 系统测试日志；

 系统测试事件报告日志；

 系统测试事件报告；

 系统测试总结报告。

 测试数据：

 所有数据录入、查询屏幕和回答屏幕的拷贝都应附在相关的测试用例文档中。

(2) 输入和输出测试文件的拷贝应交付给配置管理组。

(3) 最终执行每个测试规程的打印输出的缩微胶片拷贝，应与测试文档集一起交付给配置管理组。

1 0测试任务

 见附件A的任务列表。

1 1 环境要求

11.1 硬件

 测试应在XYZ公司的硬件配置下进行。

鉴于大多数测试必须在主要的操作时间内开展，在此期间内应向测试组提供3个在线终端。

11.2软件

11.2.1 操作系统

该业务操作系统应用于执行这些测试。

11.2.2通信软件

所有在线程序应在测试通信软件的控制下加以测试。

11.3安全性

 安全性应限于现有的各种控制器。

11.4工具

开发和评估系统测试需要下列测试工具：

(1) 测试数据生成器（UT09-0200）。该程序用于生成绝大多数的测试数据。它位于标准系统库SYSLIBA。

 (2) 比较器程序(UT08-0100)。该程序用于在回归测试期间比较系统结果。它位于标准系统库SYSLIBA中。

(3)数据库审核器。该程序用于审核数据库中的数值范围及记录之间的相互关系。它须由开发组提供。

11.5出版物

需要下列文档支持系统测试：

——公司工资系统需求陈述(AP01-01)

——公司工资系统设计描述（AP01-04）

～—公司工资系统参考手册（AP02-01）

——公司工资系统操作手册(AP02-02)

 ——公司工资系统模块参考手册（AP02-03）

——公司工资系统用户事务参考手册(AP02-04)

12职责

下列各组对测试各部分负有责任。

12.1 系统测试组

该组对测试及技术测试业务进行全面管理。

12.2公司工资部门

该组是公司工资系统的终端用户，在下列各项活动中应协助系统测试组工作。

——审查测试设计说明；

——执行在线测试；

——校验输出屏幕和报告。

12.3项目开发组

该组传递要测试的系统，并响应系统测试事件报告。该组对需要排错的任何程序进行调试，并提供数据库审核器。

13人员和培训要求

13.1 人员配备

需要下列人员开展该测试项目：

13.1.1 测试组

 测试经理 1

 高级测试分析员 1

测试分析员 2

测试技术员 1

13.1.2 工资部门

工资监管人员 1

13.2培训

公司工资部门的人员必须经过培训，以便对数据录入事务进行处理。用户事务参考手册(AP02-04)应作为该培训的基础。

14进度

见附录A的任务列表。

硬件，软件和测试工具应用于从19\*\*年6月1日到19\*\*年8月1日期间的测试。

15风险和应急

如果系统故障严重地影响测试进度，开发经理已同意分派一名全职人员到测试组做调试工作。

如果一位工资监管人员对于测试工作不够用，工资经理已同意确定第二位监管人员。

如果硬件出现的问题影响系统在白天的应用，则测试组应安排其夜晚的活动。

公司工资系统的第一次运行使用，在分发工资支票前必须详细地加以核查，并对住何出错的支票须用手工进行修正。

16批准

测试经理： 日期：

开发项目经理： 日期：

质量保证经理： 日期：

附加A 任务列表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 任务 | 前期任务 | 特殊技能 | 责任 | 投入 | 完成日期 |
| （1）准备测试计划 | 结束工资系统设计描述（AP01-04）和初步的开发计划（AP01-02） | — | 测试经理；高级测试分析员 | 4（人日） | ××-01-21 |
| （2）准备测试设计说明 | 任务1 | 通晓公司的工资规程 | 高级测试分析员 | 9 | ××-04-01 |
| （3）准备测试用例说明 | 结束相应的测试设计（任务2） | — | 测试分析员 | 4 | ××-04-15 |
| （4）准备测试规程说明 | 结束相应的测试用例（任务3） | — | 测试分析员 | 6 | ××-05-15 |
| （5）建立最初的雇员信息数据库 | 任务4 | — | 测试分析员 | 6 | ××-06-01 |
| （6）结束测试项传递并向测试组传递该公司的工资系统 | 结束集成测试 | — | 开发项目经理 | — | ××-06-01 |
| （7）检查执行该系统需要的所有工作控制规程 | 任务6 | 工作控制经验 | 测试分析员 | 1 | ××-06-08 |
| （8）组装并链接该公司工资系统 | 任务6 | — | 测试分析员 | 1 | ××-06-08 |
| （9）执行数据录入测试规程 | 任务5任务8 | — | 测试分析员 | 1 | ××-06-22 |
| （10）执行批测试规程 | 任务5任务8 | — | 测试分析员 | 3 | ××-06-30 |
| （11）检查批测试规程 | 任务10 | 通晓工资报告需求 | 测试分析员 | 1 | ××-07-02 |
| （12）解决测试事件报告 | 任务9任务11 | — | 开发组经理；系统测试组经理；公司的工资部门经理 | 2 | ××-07-16 |
| （13）重复任务（6）~（12）直到所有测试规程成功运行 | 任务12 | — | — | 2 | ××-07-30 |
| （14）撰写系统测试总结报告 | 任务13 | — | 系统测试组经理；公司工资部门经理 | 1 | ××-08-06 |
| （15）将所有测试文档集和测试数据传输给配置管理组 | 任务14 | — | 系统测试组 | 1 | ××-08-06 |

**XXX测试报告**

1. 引言
	1. 标识
	2. 系统概述
	3. 文档概述
2. 引用文件
3. 测试结果概述
	1. 对被测试软件的总体评估
	2. 测试环境的影响
	3. 改进建议
4. 详细的测试结果
	1. XXX项目
		1. 测试结果小结
		2. 遇到的问题
			1. 测试用例的项目唯一性标识符
			2. （逐个标识……）
		3. 与测试用例/测试过程的偏差
			1. 测试用例的项目唯一性标识符
			2. （逐个标识……）
5. 测试记录

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 日期时间 | 地点 | 硬件配置 | 软件配置 | 测试活动 | 测试结果 | 测试人 |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

1. 评价
	1. 能力
	2. 缺陷和限制
	3. 建议
	4. 结论
2. 测试活动总结

附件9

**XXX软件临床评价**

