**（产品名称）**

**软件开发计划书**

**DHF-XXX**

|  |  |  |  |
| --- | --- | --- | --- |
| **职责** | **职能** | **人员** | **签名** |
| **文件编制** |  |  |  |
| **文件审核** |  |  |  |
| **文件审核** |  |  |  |
| **文件审核** |  |  |  |
| **…** |  |  |  |
| **文件批准** |  |  |  |

**版本记录**

| **序号** | **更改日期** | **版本** | **编制人** | **修改说明** |
| --- | --- | --- | --- | --- |
| 01 |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**目录**

[1 目的 5](#_Toc186454082)

[2 适用范围 5](#_Toc186454083)

[3 参考文件 5](#_Toc186454084)

[4 术语与缩写 5](#_Toc186454085)

[5 软件开发概览 5](#_Toc186454086)

[5.1 软件产品概述 5](#_Toc186454087)

[5.2 软件安全性级别分类 5](#_Toc186454088)

[5.2.1 软件安全性级别分类依据 5](#_Toc186454089)

[5.2.2 软件安全性级别分类列表 5](#_Toc186454090)

[5.2.3 软件风险分析和评估 5](#_Toc186454091)

[5.3 软件开发标准及方法 6](#_Toc186454092)

[5.3.1 软件开发标准 6](#_Toc186454093)

[5.3.2 软件开发方法 6](#_Toc186454094)

[5.4 软件开发过程 6](#_Toc186454095)

[5.5 软件评审计划 6](#_Toc186454096)

[5.6 软件配置管理 6](#_Toc186454097)

[5.6.1 人员与职责 6](#_Toc186454098)

[5.6.2 配置管理工具 6](#_Toc186454099)

[5.6.3 配置项定义 7](#_Toc186454100)

[5.6.4 配置基线库 7](#_Toc186454101)

[5.6.5 软件版本定义 7](#_Toc186454102)

[5.6.6 软件版本升级方案 8](#_Toc186454103)

[5.6.7 软件版本控制 8](#_Toc186454104)

[5.7 软件开发测试环境及维护 8](#_Toc186454105)

[5.7.1 软件开发测试工具清单 8](#_Toc186454106)

[5.7.2 软件开发测试环境维护 8](#_Toc186454107)

[5.8 人员与职责 8](#_Toc186454108)

[6 软件开发计划 8](#_Toc186454109)

[6.1 软件开发计划概述 8](#_Toc186454110)

[6.2 交付件 9](#_Toc186454111)

[7 软件需求分析 9](#_Toc186454112)

[7.1 需求分析过程 9](#_Toc186454113)

[7.2 兼容性 9](#_Toc186454114)

[7.3 需求规范评审 9](#_Toc186454115)

[7.4 交付件 9](#_Toc186454116)

[8 软件架构设计 9](#_Toc186454117)

[8.1 软件架构设计过程 9](#_Toc186454118)

[8.2 软件架构设计评审 9](#_Toc186454119)

[8.3 交付件 9](#_Toc186454120)

[9 软件详细设计 10](#_Toc186454121)

[9.1 软件详细设计过程 10](#_Toc186454122)

[9.2 软件详细设计评审 10](#_Toc186454123)

[9.3 交付件 10](#_Toc186454124)

[10 软件单元实现和测试 10](#_Toc186454125)

[10.1 软件单元实现和测试过程 10](#_Toc186454126)

[10.2 软件单元实现相关检查测试任务 10](#_Toc186454127)

[10.2.1 语法检查 10](#_Toc186454128)

[10.2.2 代码规范及编译检查 10](#_Toc186454129)

[10.2.3 关键模块单元测试 10](#_Toc186454130)

[10.3 交付件 10](#_Toc186454131)

[11 软件集成和测试 11](#_Toc186454132)

[11.1 软件集成过程 11](#_Toc186454133)

[11.2 软件集成测试 11](#_Toc186454134)

[11.3 交付件 11](#_Toc186454135)

[12 软件系统测试 11](#_Toc186454136)

[12.1 测试标准 11](#_Toc186454137)

[12.2 软件缺陷处理 11](#_Toc186454138)

[12.3 交付件 11](#_Toc186454139)

[13 软件发布 12](#_Toc186454140)

[13.1 软件发布过程 12](#_Toc186454141)

[13.2 交付件 12](#_Toc186454142)

[14 软件上市后维护阶段 12](#_Toc186454143)

[15 软件变更控制 12](#_Toc186454144)

[16 网络安全管理计划 12](#_Toc186454145)

[16.1 网络安全开发管理计划 12](#_Toc186454146)

[16.1.1 网络安全小组 12](#_Toc186454147)

[16.1.2 网络安全活动的评审要求 13](#_Toc186454148)

[16.1.3 网络安全可接受标准 13](#_Toc186454149)

[16.1.4 网络安全测试活动 13](#_Toc186454150)

[16.1.5 上市后信息的收集和评审 13](#_Toc186454151)

[16.2 网络安全维护计划 13](#_Toc186454152)

[16.2.1 网络安全的维护组织 13](#_Toc186454153)

[16.2.2 网络安全更新流程 13](#_Toc186454154)

[16.2.3 网络安全事件应急响应预案 15](#_Toc186454155)

[16.2.4 远程维护流程 16](#_Toc186454156)

[17 文档计划 16](#_Toc186454157)

# 目的

# 适用范围

# 参考文件

| **序号** | **文件名称** | **文件编号** |
| --- | --- | --- |
|  |  |  |
|  |  |  |

# 术语与缩写

| **序号** | **术语/缩写** | **描述/解释** |
| --- | --- | --- |
|  |  |  |
|  |  |  |

# 软件开发概览

## 软件产品概述

## 软件安全性级别分类

### 软件安全性级别分类依据

### 软件安全性级别分类列表

### 软件风险分析和评估

软件风险管理贯穿整个软件开发周期，遵循（文件编号）《产品风险管理控制程序》的要求，包括议题的提出，分析评估及措施执行。

软件需求分析、设计等阶段对软件系统、软件项及涉及的未知来源软件进行相应的风险分析和评估，且可以根据需要重新对产品需求规范和失效模式与影响分析进行相应的升级。软件系统测试阶段需要回顾，确认软件风险控制措施的执行情况。

## 软件开发标准及方法

### 软件开发标准

### 软件开发方法

软件代码规范遵循公司内部《软件编码规范》文档，嵌入式软件采用 C/C++语言作为主要开发语言，PC应用软件采用C#语言作为主要开发语言

## 软件开发过程

软件生命周期各阶段介绍。

## 软件评审计划

相关评审活动：

1. 需求文档评审
2. 设计文档评审
3. 代码评审
4. 设计验证方案评审
5. 剩余问题评审
6. 软件发布评审

## 软件配置管理

### 人员与职责

| **序号** | **姓名** | **职责** |
| --- | --- | --- |
|  |  |  |
|  |  |  |

### 配置管理工具

| **环境** | **名称** | **规格/型号版本** | **说明** |
| --- | --- | --- | --- |
| 硬件环境 | 配置库服务器 |  |  |
| 操作系统 | 配置库服务器 |  |  |
| 开发服务器 |  |  |
| 数据库服务器 |  |  |
| 开发工具 |  |  |  |
| 测试工具 |  |  |  |
| 配置管理工具 |  |  |  |
| 缺陷管理工具 |  |  |  |
| 未知来源软件 |  |  |  |

### 配置项定义

### 配置基线库

定义将要被建立的基线：

1. 包括基线的内容
2. 基线建立原则及发布时间
3. 基线变更原则
4. 基线库的访问权限

### 软件版本定义

软件版本格式为：X.Y.Z.B

软件完整版本为 X.Y.Z.B，软件发布版本为 X。

X-主版本号，该版本号变更时表示软件有重大增强类软件更新；

Y-辅版本号，轻微增强类软件更新；

Z-修正编号，纠正类软件更新；

B-编译号，构建，

主版本号.辅版本号[.修正编号[.编译号]]。

主版本号：产品重大升级或重要确认，如多种型号的增加，产品涉及的网络安全重大变架构变更。格式：0~99，增量为1。申，

辅版本号：每次的特征升级或应用修正，包括产品涉及的网络安全轻微变更。辅版本号需要做相应调整。格式：0~99，增量为1。

修正编号：用于跟踪漏洞的修复，发行数月后的补丁发布，需要调整此码。格式：0~99，增量为 1。

编译号：内部编译号。

### 软件版本升级方案

例如：

主板本号增加：2.5.6->3.0.0

辅版本号增加：1.00.12.678-> 1.01.00.999

修正号增加：1.0.0.678->1.0.1.999

编译号增加：1.5.0.678->1.5.0.1020

### 软件版本控制

软件开发相关的代码、文档、工具配置文件全部使用VSN进行版本管理。

## 软件开发测试环境及维护

### 软件开发测试工具清单

应当在软件生存周期过程持续提供充分、适宜、有效的软件开发和测试环境，包括软硬件设备、开发测试工具、网络等资源以及病毒防护、数据备份与恢复等保证措施。

### 软件开发测试环境维护

软件开发和测试环境维护方案，确定软件开发和测试环境定期验证、更新升级、病毒防护等活动要求，并保持相关记录。

## 人员与职责

项目组织结构图及人员分工表

# 软件开发计划

## 软件开发计划概述

## 交付件

| **序号** | **文档标题** | **文档编号** |
| --- | --- | --- |
|  |  |  |
|  |  |  |

# 软件需求分析

## 需求分析过程

## 兼容性

## 需求规范评审

## 交付件

| **序号** | **文档标题** | **文档编号** |
| --- | --- | --- |
|  |  |  |
|  |  |  |

# 软件架构设计

## 软件架构设计过程

## 软件架构设计评审

## 交付件

| **序号** | **文档标题** | **文档编号** |
| --- | --- | --- |
|  |  |  |
|  |  |  |

# 软件详细设计

## 软件详细设计过程

## 软件详细设计评审

## 交付件

| **序号** | **文档标题** | **文档编号** |
| --- | --- | --- |
|  |  |  |
|  |  |  |

# 软件单元实现和测试

## 软件单元实现和测试过程

## 软件单元实现相关检查测试任务

### 语法检查

### 代码规范及编译检查

代码编译工具

评审方式

### 关键模块单元测试

## 交付件

| **序号** | **文档标题** | **文档编号** |
| --- | --- | --- |
|  |  |  |
|  |  |  |

# 软件集成和测试

## 软件集成过程

## 软件集成测试

## 交付件

| **序号** | **文档标题** | **文档编号** |
| --- | --- | --- |
|  |  |  |
|  |  |  |

# 软件系统测试

## 测试标准

系统测试阶段测试人员需要至少遵循如下测试标准执行系统测试：

1. 遵循软件系统测试用例原则，严格按照测试用例描述步骤执行测试；
2. 测试用例没有办法覆盖所有可能的情况，测试工程师力求在每个测试用例之外发挥想象进行扩展，以便在有限的操作中覆盖更多的测试可能；
3. 同一测试用例由不同的测试人员在不同样机上的测试结果应一致。

## 软件缺陷处理

软件正式发布前和发布后发现的软件问题需进入软件更改流程并提出报告，软件问题的处理需要依据 （文件编号）《缺陷管理制度》进行处理。

## 交付件

| **序号** | **文档标题** | **文档编号** |
| --- | --- | --- |
|  |  |  |
|  |  |  |

# 软件发布

## 软件发布过程

发布过程需要准备发布日志、发布评审、发布方式、发布后软件位置说明。

## 交付件

| **序号** | **文档标题** | **文档编号** |
| --- | --- | --- |
|  |  |  |
|  |  |  |

# 软件上市后维护阶段

# 软件变更控制

软件正式发布后如果软件存在问题或者需求存在偏差导致需要进行修正软件，应遵循（文件编号）《缺陷管理制度》和 文件编号《变更控制程序》要求。

# 网络安全管理计划

## 网络安全开发管理计划

### 网络安全小组

网络安全开发小组由软件安全技术代表(主导)、项目经理、相关部门专家、服务代表、质量代表、法规代表、IT 共同参与的技术组织，主要有以下职责：

1. 分析和落实公司产品涉及的网络安全法规。
2. 制定和维护公司产品的网络安全策略，选择和变更网络安全技术。
3. 分析 IT 部门发布的网络安全通报。
4. 对产品上市后识别的网络安全事件进行评估，并给出应对措施和计划。
5. 上市后网络安全的主动监测与常规更新。
6. 对网络安全的发展规划提出指导，例如培训。
7. 监控相关策略、标准和任务的推进，完成相关活动。

| **角色** | **姓名** | **职责&权限** |
| --- | --- | --- |
| 软件安全技术代表 |  | 网络安全小组主导人 |
| 项目经理 |  |  |
| XX专家 |  |  |
| XX专家 |  |  |
| 服务代表 |  |  |
| 质量代表 |  | 上市后识别网络安全相关的投诉 |
| 法规代表 |  | 医疗器械网络安全相关的不良事件信息的收集 |
| IT |  | 识别网络安全检测部门发布的网络安全通报  关注各杀毒服务商及产品中现成软件是否停止售后服务 |
|  |  |  |
|  |  |  |
|  |  |  |

### 网络安全活动的评审要求

### 网络安全可接受标准

### 网络安全测试活动

### 上市后信息的收集和评审

## 网络安全维护计划

### 网络安全的维护组织

由网络安全小组负责网络安全的日常维护工作，并成立网络安全应急响应小组。

### 网络安全更新流程

明确日常网络安全的流程，形成网络安全更新的流程图。若适用，建立现成软件网络安全更新维护过程，及时将现成软件网络安全相关信息以及应对措施告知用户。

网络安全小组对识别的信息进行评估，给出评估意见，并给出需要应对的措施和计划，必要时，启用应急响应预案。

基于对网络安全信息的风险评估，应满足以下时限要求：

| **网络安全事件的严重度** | **相应组织和权限** |
| --- | --- |
| 1-无  2-很低  3-低 | 网络安全小组每月定期评估网络安全信息 |
| 4-中 | 网络安全小组应在收到相关信息后72H内响应并给出评估意见 |
| 5-高  6-很高 | 网路安全小组应在收到相关信息后48H内响应并给出评估意见 |

可能采取以下几种类型的措施：

| **类型** | **控制措施类型** | **描述** |
| --- | --- | --- |
| 潜在网络安全风险 | 消减风险 | 通过适当的控制措施降低风险发生的可能性 |
| 规避风险 | 决定不进行引起风险的活动 |
| 接受风险 | 风险值不高或者处理的代价高于风险引起的损失，公司决定接受该风险/剩余风险 |
| 已发生的网络安全事件 | 资产恢复 | 依据具体情况制定资产恢复措施 |

若为已发生的网络安全事件，除风险控制措施外，还应考虑对受损资产的恢复。

若需采取措施，应进一步给出以下信息，并判定是否需要启动应急相应预案：

1. 受到紧急情况影响的范围，如受影响客户、经销商、库存。
2. 潜在的影响或损失。
3. 问题原因。若无法立刻分析到原因，可先解决问题随后再分析事故起因。
4. 被更换的项目(如硬件、软件、固件或支持材料)。
5. 估计恢复正常服务所需的时间。

### 网络安全事件应急响应预案

中等、严重级别：提供网络安全事件应急响应的流程图，并依据图示描述相关活动。

#### 网络安全应急响应小组

网络安全应急响应小组由软件安全技术代表（主导）、服务代表、质量代表、法规代表、IT代表共同参与的领导组织，负责预案的准备、编制和实践。

网络安全应急响应小组联络表

| **角色** | **姓名** | **职责&权限** | **电话号码** | **邮箱地址** | **备用联系人** | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **关系** | **姓名** | **电话号码** |
| 软件安全技术代表 |  |  |  |  |  |  |  |
| 服务代表 |  |  |  |  |  |  |  |
| 质量代表 |  |  |  |  |  |  |  |
| 法规代表 |  |  |  |  |  |  |  |
| IT |  |  |  |  |  |  |  |

#### 网络安全事件应急响应流程

提供网络安全事件应急响应的流程图，并依据图示描述相关活动。

### 远程维护流程

若适用，全部级别均应提供远程维护的流程图，并依据图示描述相关活动。

# 文档计划

开发过程中的文档应遵循（文件编号）《文件控制程序》和（文件编号）《软件设计开发管理制度》要求。

| **序号** | **阶段** | **文档标题** | **文档编号** | **期望完成日期** |
| --- | --- | --- | --- | --- |
|
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |