**（产品名称）**

**软件架构设计规格书**

**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 引言 4](#_Toc187409128)

[1.1 目的 4](#_Toc187409129)

[1.2 适用范围 4](#_Toc187409130)

[1.3 术语与缩写 4](#_Toc187409131)

[1.4 参考文献 4](#_Toc187409132)

[1.5 文件的更新要求 4](#_Toc187409133)

[1.6 人员职责 4](#_Toc187409134)

[2 概述 5](#_Toc187409135)

[2.1 设计指导思想和原则 5](#_Toc187409136)

[2.2 产品概述 5](#_Toc187409137)

[3 网络安全 5](#_Toc187409138)

[3.1 数据架构 5](#_Toc187409139)

[3.2 网络安全能力评估 5](#_Toc187409140)

[4 软件体系结构设计 6](#_Toc187409141)

[4.1 XX 模块 6](#_Toc187409142)

[4.1.1 \*\*子模块 7](#_Toc187409143)

[4.1.2 \*\*子模块 7](#_Toc187409144)

[4.2 XX 模块 7](#_Toc187409145)

[附录A：自定义 7](#_Toc187409146)

# 引言

## 目的

## 适用范围

## 术语与缩写

| **序号** | **术语/缩写** | **英文全称** | **描述/解释** |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |

## 参考文献

1. 文件编号 用户需求管理制度（版本）（要求同上。若没有参考文件，此节应写“无”。文件名称前需有序号、文件编号（如有），如需标注版本，在文件名称后以括号形式增加。序号、编号、文件名称间留一个空格）。
2. 文件编号 文件名称（版本）
3. 文件编号 文件名称（版本）

## 文件的更新要求

## 人员职责

| **序号** | **姓名** | **职务** | **职责** |
| --- | --- | --- | --- |
| 1 |  |  |  |
| 2 |  |  |  |
| 3 |  |  |  |
| 4 |  |  |  |

# 概述

## 设计指导思想和原则

## 产品概述

从特定视角出发，专注于该视角系统的结构、模块划分、基本组件职责和主要控制流，可以从逻辑视图、开发视图、物理视图、运行视图和数据视图，完整的表达架构。

确定软件系统的主要结构、并确定每个模块的关键责任（功能），其外部可见特性、以及模块之间的关系。

# 网络安全

## 数据架构

提供医疗器械在每个使用场景（含远程维护）下的网络环境和数据流图，并依据图示描述医疗器械相关数据和电子接口的基本情况。

数据情况明确医疗器械相关数据的类型（敏感与非敏感医疗数据、设备数据），并依据数据类型明确每类数据的具体内容（如个人信息、医疗活动信息、设备运行信息）、功能（如单向、双向电子数据交换，实时、非实时远程控制）、用途（如医疗活动、设备维护）等。

电子接口情况逐项说明每个网口接口、电子数据交换接口的预期用户、使用场景、预期用途、数据类型、技术特征、使用限制。

## 网络安全能力评估

| **序号** | **网络安全能力评估项** | **是否适用** | **实现方式/不适用理由** |
| --- | --- | --- | --- |
| 1 | 自动注销：产品在使用闲置期间阻止非授权用户访问和使用的能力。 |  |  |
| 2 | 审核：产品提供用户活动可被审核的能力。 |  |  |
| 3 | 授权：产品确定用户已获授权的能力。 |  |  |
| 4 | 网络安全特征配置：产品根据用户需求配置网络安全特征的能力。 |  |  |
| 5 | 网络安全补丁升级：授权用户或服务人员安装/升级网络安全补丁的能力。 |  |  |
| 6 | 数据去标识化：产品直接去除或匿名化数据所含个人信息的能力。 |  |  |
| 7 | 数据备份与灾难恢复：产品的数据、硬件或软件受到损坏或破坏后恢复的能力。 |  |  |
| 8 | 紧急访问：产品在预期紧急情况下允许用户访问和使用的能力。 |  |  |
| 9 | 数据完整性与真实性：产品确保数据未以非授权方式更改且来自创建者或提供者的能力。 |  |  |
| 10 | 恶意软件探测与防护：产品有效探测、阻止恶意软件的能力。 |  |  |
| 11 | 节点鉴别：产品鉴别网络节点的能力。 |  |  |
| 12 | 人员鉴别：产品鉴别授权用户的能力。 |  |  |
| 13 | 物理防护：产品提供防止非授权用户访问和使用的物理防护措施的能力。 |  |  |
| 14 | 现成软件维护：产品在全生命周期中对现成软件提供网络安全维护的能力。 |  |  |
| 15 | 系统固化：产品通过固化措施对网络攻击和恶意软件的抵御能力。 |  |  |
| 16 | 网络安全指导：产品为用户提供网络安全指导的能力。 |  |  |
| 17 | 存储保密性与完整性：产品确保未授权访问不会损坏存储媒介所存数据保密性和完整性的能力。 |  |  |
| 18 | 传输保密性与完整性：产品确保数据传输保密性和完整性的能力。 |  |  |
| 19 | 远程访问与控制：产品确保用户远程访问与控制的网络安全的能力。 |  |  |
| 20 | 抗拒绝服务攻击：产品具有抗拒绝服务攻击的能力。 |  |  |

# 软件体系结构设计

结合软件体系结构设计中的模块，进行详细描述。

## XX 模块

1. 描述该模块实现功能。
2. 模块内部实现的逻辑图。
3. 以及模块相关的使用环境和条件等。

例如硬件环境、软件环境，详细描述相关设备参数、芯片参数。

芯片需描述如下相关参数：

1. 芯片厂家：
2. 芯片型号：
3. 开发平台：
4. 开发语言：

### \*\*子模块

正文（要求同正文要求）

模块编号（模块名称）

1. 实现功能
2. 输入参数
3. 输出参数
4. 返回值
5. 对其他模块的影响
6. 异常处理

若子模块复杂,以结构图的形式可进一步描述子模块内部的调用关系；并逐一描述最小模块（软件项）的外部特性并给予标识。

### \*\*子模块

## XX 模块

# 附录A：自定义