**XXXX软件**

**网络安全研究报告**

**DHF-XXX-XXX**

|  |  |  |  |
| --- | --- | --- | --- |
| **职责** | **职能** | **人员** | **签名** |
| **文件编制** |  |  |  |
| **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 |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

目录

[版本记录 2](#_Toc135236944)

[1 基本信息 4](#_Toc135236945)

[1.1软件信息 4](#_Toc135236946)

[1.2 数据架构 4](#_Toc135236947)

[1.3 网络安全能力 5](#_Toc135236948)

[1.4 网络安全补丁 6](#_Toc135236949)

[1.5 安全软件 6](#_Toc135236950)

[2 实现过程 6](#_Toc135236951)

[2.1风险管理 6](#_Toc135236952)

[2.2 需求规范 7](#_Toc135236953)

[2.3 验证与确认 7](#_Toc135236954)

[2.4 可追溯性分析 7](#_Toc135236955)

[2.5 维护计划 7](#_Toc135236956)

[2.5.1维护流程 7](#_Toc135236957)

[2.5.2流程说明 9](#_Toc135236958)

[2.5.3 网络安全事件应急响应的流程 9](#_Toc135236959)

[3 漏洞评估 11](#_Toc135236960)

[4 结论 11](#_Toc135236961)

# 1 基本信息

## 1.1软件信息

软件名称：

发布版本：

安全性级别：

依据《医疗器械软件注册审查指导原则（2022年修订版）》，按照软件对于病人、用户或其他相关人员的影响，脑电信号采集记录软件安全等级为轻微。

## 1.2 数据架构

1. 网络环境与数据流图
2. 数据输出接口
3. 数据情况

脑电数据以二进制格式存储，不含有敏感信息，用户敏感信息以加密数据库形式存储，检查导出后为加密ZIP格式。

设备数据，设备运行日志、配置参数等保存在配置文件中。

脑电信号处理器与脑电信号采集记录软件之间是双向数据传输，软件向脑电信号处理器发送设置参数，采集时，接收脑电信号处理器的采集的脑电信号数据。

放大器接口信号为单向数据，脑电信号放大器通SPI协议单向发送给脑电信号处理器。

## 1.3 网络安全能力

按实际情况撰写适用性

1.自动注销（ALOF）：适用，软件在设定时间无操作，会自动注销，跳转到登录界面。

2.审核（AUDT）：适用，软件通过日志记录用户活动。

3.授权（AUTH）：适用，用户登录以后才能访问设备功能，并通过用户角色进行权限控制。

4.节点鉴别（NAUT）：不适用，产品为单机使用，不连接网络。

5.人员鉴别（PAUT）：适用，通过用户名密码鉴别，密码要求大小写、数字、特殊符号其中两种。

6.连通性（CONN）：不适用，软件单机使用，连接网络和移动介质。

7.物理防护（PLOK）：不适用，软件安装在医生的专用电脑上，在专业场所使用。

8.系统加固（SAHD）：适用，安装部署时只安装所需的软件和服务组件，并告知客户不可安装跟产品无关软件，及时更新安装系统漏洞补丁。

9.数据去标识化与匿名化（DIDT）：不适用，软件安装在医生的专用电脑上，在专业场所使用,导出数据为加密Zip格式。

10.数据完整性与真实性（IGAU）：适用，只有登录用户才能访问数据。

11.数据备份与灾难恢复（DTBK）：适用，软件提供数据导入导出功能。

12.数据存储保密性与完整性（STCF）：适用，通过加密数据库控制访问，并保证数据完整性机制实现。

13.数据传输保密性（TXCF）：适用，软件单机使用，不连接网络，导出数据为加密Zip格式。

14.数据传输完整性（TXIG）：适用，导出数据为加密Zip格式，导入时进行完整性验证。

15.网络安全补丁升级（CSUP）：适用，操作系统授权用户可安装/升级网络安全补丁。

16.现成软件清单（SBOM）：不适用，产品不使用现成软件。

17.现成软件维护（RDMP）：不适用，产品不使用现成软件。

18.网络安全使用指导（SGUD）：不适用，产品由脑虎工程师进行安全维护。

19.网络安全特征配置（CNFS）：不适用，产品由脑虎工程师进行安全配置。

20.紧急访问（EMRG）：不适用，本系统根据软件安全级别定义，不支持紧急访问功能。

21.远程访问与控制（RMOT）：不适用，产品不支持远程访问。

22.恶意软件探测与防护（MLDP）：不适用，产品不接入网络，也不接入其他存储介质。

## 1.4 网络安全补丁

|  |  |  |
| --- | --- | --- |
| 名称 | 完整版本 | 发布日期 |
| Windows10 2023-05累积更新 | KB5026361 | 2023/5/9 |
| Windows10 2023-04累积更新 | KB4023057 | 2023/4/27 |
| Windows10 .Net累积更新预览 | KB5025367 | 2023/4/25 |

## 1.5 安全软件

**无**

# 2 实现过程

## 2.1风险管理

见《脑电信号采集记录软件网络安全风险管理报告》。

## 2.2 需求规范

见《数字脑电图机软件设计规格书》

## 2.3 验证与确认

医疗器械产品的网络安全需求（如保密性、完整性、可得性等特性）均已得到满足。详见附件《数字脑电图机网络安全测试计划》《数字脑电图机网络安全测试报告》。本公司质量体系基于ISO 13485体系流程，设计开发过程管理依据《设计和开发控制程序》（NH-COP-006）执行。网络安全追溯、设计规范、测试验证、风险管理关系如下图1所示。

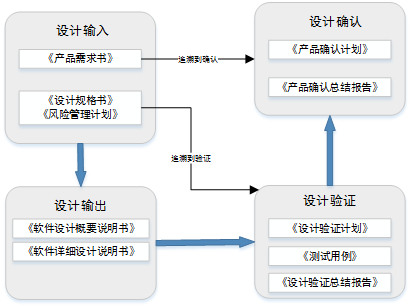


图1 产品设计追溯流程

## 2.4 可追溯性分析

见《数字脑电图机网络安全可追溯性分析报告》

## 2.5 维护计划

### 2.5.1维护流程

上市后产品反馈抱怨与维护流程依据公司程序文件，《顾客反馈投诉处理控制程序》（NH-COP-012）执行。工程部搜集客户抱怨反馈，将信息传递到质量部。质量部分析抱怨、投诉原因，跟踪上市后产品风险，并指定责任部门。相关责任部门根据问题进行具体原因分析及指定应对计划，并根据应对计划实施。

由于软件的复杂性，一个看似很小的地方的修正可能对全局系统产生重大影响。因此每次产品维护过程应按产品设计开发过程来执行、实施应对计划。每当软件修正后，验证分析不仅要对修正进行验证，还要确认此修正对整个软件系统的影响程度。同时涉及到该软件的修改、评审、验证和风险分析，软件修改前后的差别对比，新软件版本号，这些都将形成文字记录。

公司制定《设计开发控制程序》（NH-COP-006）中规定了上市后市场反馈和设计变更的管理流程。《变更控制程序》（NH-COP-020）中制定了软件变更事项分类、命名、配置管理流程。软件维护进行管理和控制，并按照《风险管理控制程序》(NH-COP-035)对软件维护可能产生的风险进行分析和控制，以确保软件维护可能造成的风险可接受。

软件网络安全更新的维护流程如下图2：

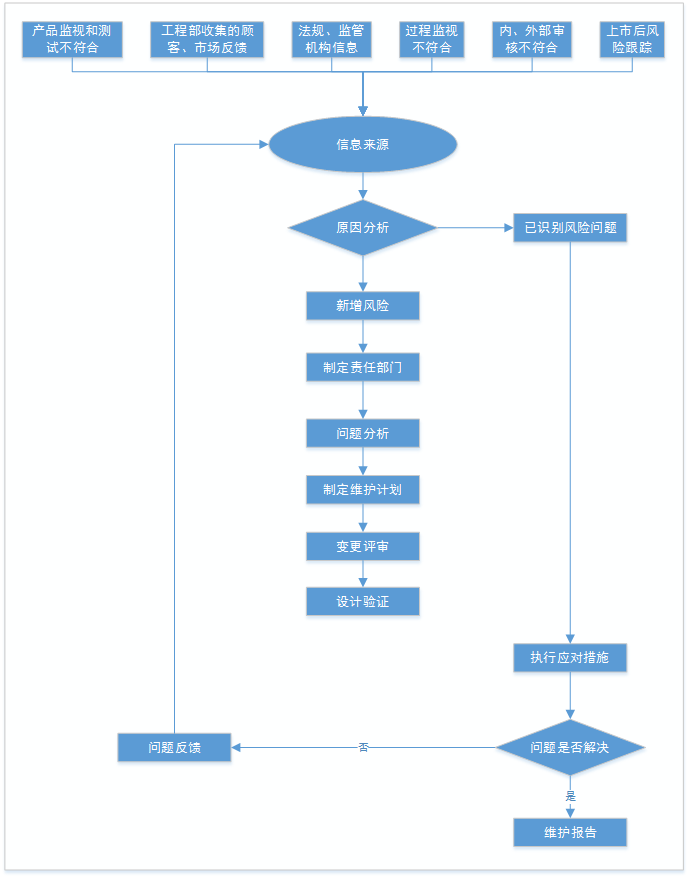


图2 网络安全软件更新流程

### 2.5.2流程说明

* 更新确认：

质量部门根据产品上市后的跟踪收集产品信息。反馈信息可能来源于：

工程部、售后投诉等接到的客户抱怨；

产品检测过程中的不合格报告；

法规机构提出的法规要求更新；

过程监控过程发现的产品缺陷；

内部、外部审核发现的产品缺陷；

产品风险管理计划中上市后跟踪检测的风险事件；

质量部搜集到以上反馈信息后需指定工程部、法规、研发、质量等相关人员核实确认反馈信息。

确认信息后质量部责任人将对问题分析、确认并指派责任部门。

研发部负责人制定维护计划、实施方案。系统工程师对方案进行审核，确保方案的安全性和正确性，并对可能产生的风险进行分析，必要时进行风险控制。根据维护所涉及产品的安全性和有效性的影响程度确定维护类型，确定软件维护符合法规要求。

如需要，对系统进行备份。（具体操作有方案确定）

如需要，对维护操作进行模拟验证。（具体操作由方案确定）

* 用户告知

现场工程师按照方案进行修改操作。完成维护后，如果需要对用户软件更新，应通知用户软件进行了维护以及维护的主要内容。

维护申请提出用户对维护结果进行反馈和评价。

### 2.5.3 网络安全事件应急响应的流程

在发生信息安全事件时，启动下列应急响应流程，应急响应流程下图所示：



**1、事件分析**

事件分析主要完成如下工作：

1）在发生信息安全事件后，应急响应工作小组对事件进行确认。

2）确认为信息安全事件后，根据应急处理事件分类规则对事件进行定性、定级和上报。

3）根据对事件的初步分析，确定应急处理方式，如果应急响应工作组以自身力量无法处理的事件，由应急工作小组向上级领导或上级机关提出应急支援请求。

**2、事件处理**

事件处理主要包括以下内容：

1）泄密安全事件发生时，要及时的用口头或书面的形式向保密工作部门如实报告并上报上级主管部门的保密机构，同时采取断开网络、改变或终止用户权限等措施切断泄密源头，控制泄密范围，并及时对系统隐患进行修补。在对系统的泄漏隐患或风险进行重新评估，确认安全后，系统方能重新运行，对事件类型、发生原因、影响范围、补救措施和最终结果进行详细纪录。

2）系统运行安全事件发生时，应分析是否存在针对该事件的特定系统预案，如果存在则启动特定系统应急预案，如果涉及多个特定系统预案，应同时启动所有涉及的特定系统预案。分析是否存在针对该事件的专题预案，如果存在则启动专题预案，如果事件涉及多个专题预案，应同时启动所有涉及的专题预案。

3）如果没有针对该事件的应急预案，应根据事件具体情况，采取抑制措施，抑制事件进一步扩散，并根除事件影响，恢复系统运行；

**3、结束响应**

系统恢复运行后，应急响应工作组对事件造成的损失、事件处理流程、应急预案进行评估，对响应流程、预案提出修改意见，撰写事件处理报告。应急响应工作组应根据《信息安全应急预案》要求，确定是否需要上报该事件及其处理过程，需要上报的应及时准备相关材料，上报上级机关。

对于蠕虫、病毒等易造成大范围传播的信息安全事件，应及时向应急工作小组提交预警信息。

应急响应流程结束。

# 3 漏洞评估

扫描工具：openvas 22.4.1 2023-01-09 供应商：[Greenbone Networks](https://www.openvas.org/)

漏洞库：CNNVD漏洞库 2023.4,中国信息安全测评中心

已知漏洞总体情况：

|  |  |  |
| --- | --- | --- |
| CVSS漏洞等级 | 已知漏洞总数 | 剩余漏洞数 |
| 超危险（9.0-10.0） | 2 | 0 |
| 高危（7.0-8.9） | 66 | 0 |
| 中危（4.0-6.9） | 29 | 0 |
| 低危（0.1-3.9） | 0 | 0 |

已知漏洞中，中高危级及以上等级的漏洞均已修复，在产品的使用场景中对产品的安全性不造成影响。

# 4 结论

产品的日常使用场景中不接入网络，在医院专业场所，由专业人员单机使用，只通过USB接口以USB线缆连接脑电信号处理器，数据为双向传输，不传输敏感信息，脑电信号处理器通过HDMI线缆连接脑电信号放大器，数据为单向传输；通过加密数据库保存管理敏感数据，导出数据为加密Zip格式。产品的网络安全实现过程按照轻微级别的要求规范研发活动，修复了所有CVSS中高危级及以上的网络安全漏洞，无已知剩余漏洞，对产品的使用不构成安全威胁。综上，产品的网络安全能够满足要求，受益大于风险。