PEMS自查表

**一、填表说明：**

1、PEMS检查表由三部分组成。

2、内容所在文档位置，**应填写该部分内容在哪个文档的哪个章节第几页第几段**。

3、以下两种情况不需填写此表中第二部分：

1）可编程电子子系统不提供基本安全或基本性能所必需的功能；

2）通过风险管理表明任何可编程电子子系统的失效不会导致不可接受的风险。

4、预期接入IT-网络的任何PEMS不管是否需要填写此表第一部分和第二部分，均要填写此表的第三部分，第三部分的内容应查看随附文件。

5、“是否适用”统一填写“√”；“内容所在文档位置”统一填写所在“文档名称+页码+条款号”。

**二、PEMS检查表（第一部分）**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 标准条款号 | 文档中应包含的内容 | 是否适用 | 内容所在文档位置或不适用理由 |
| 是 | 否 |
| 1 | YY/T 0664-2020中4.3 | 软件安全分级 |  |  |  |
| 2 | YY/T 0664-2020中5 | 软件开发过程 | 软件开发策划 |  |  |  |
| 软件需求分析 |  |  |  |
| 软件体系结构设计 |  |  |  |
| 软件详细设计 |  |  |  |
| 软件单元的实现 |  |  |  |
| 软件集成和集成测试 |  |  |  |
| 软件系统测试 |  |  |  |
| 软件在系统级别应用的发布 |  |  |  |
| 3 | YY/T 0664-2020中7 | 软件风险管理过程 | 促成危险情况的软件分析 |  |  |  |
| 风险控制措施 |  |  |  |
| 风险控制措施的验证 |  |  |  |
| 软件变更的风险管理 |  |  |  |
| 4 | YY/T 0664-2020中8 | 软件配置管理过程 | 配置标识 |  |  |  |
| 变更控制 |  |  |  |
| 配置状态报告 |  |  |  |
| 5 | YY/T 0664-2020中9 | 软件问题解决过程 |  |  |  |

**三、PEMS检查表（第二部分）**

| 序号 | 标准条款号 | 文档中应有的内容 | 是否适用 | 内容所在文档位置或不适用理由 |
| --- | --- | --- | --- | --- |
| 是 | 否 |
| 1 | GB 9706.1-2020中14.2 | 14章要求的文档进行评审、批准、发布和更改的记录 |  |  |  |
| 2 | GB 9706.1-2020中14.3 | 风险管理计划对PEMS确认计划的引用 |  |  |  |
| 3 | GB 9706.1-2020中14.4 | PEMS开发生命周期 | 包含一组已定义的里程碑 |  |  |  |
| 在每个里程碑，应确定将要完成的活动和验证这些活动的方法 |  |  |  |
| 应确定每个活动，包括其输入和输出 |  |  |  |
| 每个里程碑应识别在此里程碑结束前一定有完成的风险管理活动 |  |  |  |
| 详细的活动、里程碑和进度表计划 |  |  |  |
| 对文档的要求 |  |  |  |
| 4 | GB 9706.1-2020中14.5 | 问题解决 | 影响基本安全或基本性能的潜在的或现存的问题 |  |  |  |
| 对每个涉及风险问题的评估 |  |  |  |
| 确定将问题解决一定要满足的准则 |  |  |  |
| 确定解决每个问题所采取的措施 |  |  |  |
| 5 | GB 9706.1-2020中14.6 | 风险管理过程中对已知和可预见危险的识别 |  |  |  |
| 为实现每个风险控制措施，应选择和确定合适的已确认的工具和程序 |  |  |  |
| 6 | GB 9706.1-2020中14.7 | PEMS及其各子系统的需求规格说明，应包含并区分由其自身实施的任何基本性能和任何风险控制措施 |  |  |  |
| 7 | GB 9706.1-2020中14.8 | 体系结构 | a) 高完善性元器件 |  |  |  |
| b）失效安全功能 |  |  |  |
| c）冗余设计 |  |  |  |
| d）多样性 |  |  |  |
| e）功能划分 |  |  |  |
| f）防护性设计,例如通过限制可得到的输出能量或采用限制执行机构的行程的方法来限制潜在危险的影响 |  |  |  |
| g）对PEMS子系统及其组件的风险控制措施的配置 |  |  |  |
| h）组件失效模式及其效应 |  |  |  |
| i）共同原因的失效 |  |  |  |
| j）系统性失效 |  |  |  |
| k）测试的间隔持续时间和诊断覆盖范围 |  |  |  |
| l）可维护性 |  |  |  |
| m）合理可预见误用的防护 |  |  |  |
| n）如适用, IT-网络规格说明 |  |  |  |
| 8 | GB 9706.1-2020中14.9 | 设计和实现 | 每个子系统的设计和测试规格说明 |  |  |  |
| 关于设计环境的描述数据应形成文档 |  |  |  |
| 9 | GB 9706.1-2020中14.10 | 验证计划 | 在每个里程碑，对实现基本安全、基本性能或风险控制措施的各个功能进行验证 |  |  |  |
| 验证策略、活动、技术及执行验证人员的适当独立程度的选择和形成文档 |  |  |  |
| 验证工具的选择和运用 |  |  |  |
| 验证的覆盖准则 |  |  |  |
| 10 | GB 9706.1-2020中14.11 | PEMS确认 | PEMS确认计划应当包含基本安全和基本性能的确认 |  |  |  |
| PEMS确认采用的方法 |  |  |  |
| PEMS确认活动的结果 |  |  |  |
| 全面负责PEMS确认的人员，其独立于设计组的独立性程度的解释说明 |  |  |  |
| 设计组成员不应承担其自己设计部分的确认工作 |  |  |  |
| 风险管理文档中应记录PEMS确认组成员和设计组成员之间的所有专业关系 |  |  |  |
| 11 | GB 9706.1-2020中14.12 | 修改 | PEMS检查表三部分的所有内容 |  |  |  |

**四、EMS检查表（第三部分）**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 标准条款号 | 文档中应包含的内容 | 是否适用 | 内容所在随附文件位置或不适用理由 |
| 是 | 否 |
| 1 | GB 9706.1-2020中14.13 | 如果PEMS预期接入未经PEMS制造商确认过的IT-网络 | a）PEMS连接到IT-网络的目的 |  |  |  |
| b）与PEMS相连的IT-网络所要求的特性 |  |  |  |
| c）与PEMS相连的IT-网络所需的配置 |  |  |  |
| d）PEMS网络连接的技术规格说明，包括数据安全规格说明 |  |  |  |
| e）在PEMS，IT-网络和IT-网络上的其它设备间的预期信息流，以及预期通过IT-网络的路由；和 |  |  |  |
| f）为达到PEMS与IT-网络连接目的所需特性的IT-网络失效时的危险状况清单 |  |  |  |
| 应告知责任方 | PEMS与包含其他设备的IT-网络的连接可能导致对患者、操作者、第三方带来以往没有识别的风险 |  |  |  |
| 责任方宜识别、分析、评价和控制这些风险 |  |  |  |
| 对IT-网络的后续修改可能引入新的风险,需要进行补充分析 |  |  |  |
| IT-网络的更改包括：●IT-网络配置的更改●与IT-网络连接的新增项●与IT-网络连接中断的项●与IT-网络连接的设备的更新●与IT-网络连接的设备的升级 |  |  |  |