附录3:

控制系统检查要点

1. 加速器控制系统

（征求意见稿）

1. 产品介绍
2. 预期用途

加速器控制系统软件通过与控制设备的协同作用，实现磁铁电源监控、真空系统状态监控、定时触发、联锁保护和中央监控等功能，并为操作人员提供可视化的人机交互界面。

1. 工作原理

加速器控制系统软件是作为加速器的可视化软件，实时显示加速器各子系统设备运行参数、运行状态、故障报警信息等，实现加速器设备参数、状态、历史信息的存储、查找及分析，为物理人员提供在线监测、分析手段，提供设备运行状态。操作人员通过加速器控制系统软件的人机界面对加速器运行状态进行监控，按照加速器运行的需求，实现加速器内束流的产生、注入、加速、累积、引出，同时通过调整磁铁电源的电流来控制束流轨道，实现加速器的调试。

1. 结构组成

加速器控制系统软件结构模块包括：中央定时系统、电源系统监控、联锁系统、真空系统监控、冷却水监测、系统管理等，各模块之间能够基于中央监控系统的集成进行数据交互，进而实现对加速器被控设备的集成调试与监测功能。

1. 主要技术指标

表1 加速器控制系统主要技术指标

| **序号** | **检验项目** | **主要控制指标** | **检验方法** |
| --- | --- | --- | --- |
|  | 软件环境 | 技术文件中应提供加速器控制系统运行环境，包括：服务端、客户端的软件环境和硬件环境及网络环境 | 按照企业制定的规程 |
|  | 使用限制 | 技术文件中应提供加速器控制系统用户使用限制 | 按照企业制定的规程 |
|  | 数据接口 | 技术文件中应提供加速器控制系统数据交互接口 | 按照企业制定的规程 |
|  | 用户访问控制 | 技术文件中应提供加速器控制系统软件登录用户名和密码，以及用户权限区分 | 按照企业制定的规程 |
|  | 功能、性能 | 技术文件中应提供加速器控制系统软件功能、易用性、可靠性、兼容性、性能效率、维护性、可移植性、信息安全性等 | 按照企业制定的规程 |

1. 生产工艺和质量关键控制点
2. 生产环节风险点

加速器控制系统软件生产环节风险点主要包括人员、仪器设备、配置管理、软件设计、软件验证、数据安全、安装等。

1. 生产质量管理关键控制措施

|  |  |  |
| --- | --- | --- |
| **序号** | **风险点** | **控制措施** |
|  | 人员 | ①企业应配备软件架构师、算法工程师、软件开发工程师、软件测试工程师、UI工程师等技术人员；  ②软件开发、测试、维护人员应当具备与岗位职责要求相适宜的专业知识、实践经验和工作能力，应当保证黑盒测试同一软件项的开发人员和测试人员不得互相兼任；  ③企业应在设计开发周期内关注团队人员的状态，建立人才储备；  ④企业应对软件开发人员和测试人员进行需求规范、设计规范、使用说明书、标准等的培训。 |
|  | 仪器设备及开发环境 | 检测仪器和设备：  ①企业应建立监视测量设备相关管理程序文件，对设备的采购、检定、校准、维护保养等方面进行规定；  ②企业应配置与加速器控制系统相匹配的检测设备，主要仪器设备应建立操作规程；  ③企业应制定设备校准周期和年度检定/校准计划。 |
| 开发环境：  ①企业应配备软件开发测试环境，建立软件开发测试环境维护文件及相应的维护记录（定期验证、更新升级、病毒查杀记录等）；  ➁企业应制定计算机软件确认程序文件，依据文件要求对软件开发工具（如配置管理工具和自研或第三方软件测试工具等）、安装在检测设备中的计算机软件进行确认，当软件更改、受计算机病毒侵害等情况发生时，企业应进行再确认；  ③软件研发负责人或软件架构师应对开发团队使用的工具及版本等进行统一规范、管理，并进行确认。 |
|  | 配置管理 | ①企业应建立软件配置管理程序文件；  ➁企业应依据配置管理程序文件要求对软件版本、源代码、文件、工具、现成软件等进行控制；  ③企业应对软件配置项进行识别、标识，QA对配置项进行检查，记录检查结果；  ④QA根据软件开发阶段检查配置状态，并对配置状态进行记录及更新；  ➄企业应对软件版本变更（涵盖软件、现成软件、网络安全的全部更新）进行控制，并保留变更记录、验证记录。 |
|  | 软件设计 | ①企业应建立软件设计开发程序文件；  ➁企业应依据软件设计开发程序文件的要求进行软件策划、需求分析及设计；  ③软件设计开发输入的用户需求、自身需求、预期用途的功能、性能、安全要求、法规/标准要求、风险管理要求等输入信息应充分；  ④软件设计开发输出的技术要求应满足输入的国家和行业标准等要求；  ➄软件设计变更应进行识别、提出、验证和评审等，发布版本变更的，应进行注册变更；  ➅软件开发过程应建立可追溯性机制，形成可追溯性记录，如从测试追溯到源代码，从源代码追溯到设计，从设计追溯到需求；  ⑦企业应对现成软件（尤其是未知来源软件）的风险进行评估，并采取安全措施确保软件安全。 |
|  | 软件验证 | ①企业应建立软件测试计划（单元测试、集成测试、系统测试、网络安全测试），并对其进行评审；  ➁企业应制定软件测试用例，并对其进行评审，检查测试用例覆盖情况；  ③企业应选择成熟稳定可靠的测试工具；  ④企业应依据软件测试用例对软件进行单元测试、集成测试、系统测试、网络安全测试，测试记录、测试报告、自检记录、自检报告应满足真实、完整性要求；  ➄软件标识应满足可追溯性要求，如软件名称、规格型号、完整版本、发布版本、HASH值等。 |
|  | 数据安全 | ①企业应对软件系统电子接口（网络接口、电子数据交换接口）的访问、防护等进行控制，防止非预期的使用；  ➁企业应对软件网络安全威胁进行识别、保护、探测、响应、恢复等，如采用防火墙、堡垒机、漏洞扫描系统、终端用户管理系统等硬件防护措施，网络安全具体参照《医疗器械网络安全注册审查指导原则》；  ③企业应对软件系统漏洞进行扫描，如根据软件安全性级别进行网络安全漏洞自评或第三方漏洞评估检测，且两者不能使用同一工具进行漏洞扫描；  ④企业应对软件系统重要数据进行灾备，灾备方案设计合理，如异地增量备份，便于数据的备份与恢复等。 |
|  | 安装 | ①现场调试人员根据当前软件系统的技术要求，核对现场的运行环境是否与技术要求一致；  ➁由版本管理人员或配置管理人员对发行的每个软件版本进行跟踪检查，确保能追踪到当前版本所对应的源码备份；  ③现场安装的软件版本出口必须统一：统一由版本管理人员或配置管理人员从受控库检出再转交给软件安装人员；  ④现场软件安装完成后须进行确认及测试，形成安装记录。 |

1. 检查要点

（一）机构与人员

企业应对从事影响产品质量的工作人员，特别是产品设计开发人员、测试人员等制定考核评价制度，培训内容包含相关法律法规、基础理论知识、专业操作技能、过程质量控制及质量检验等，并保留相关培训记录。如：软件设计开发人员和测试人员需进行强制性标准及行业标准IEC 62304（YY/T 0664）等培训。

（二）厂房与设施

不涉及。

（三）设备

不涉及。

（四）文件管理

企业应根据实际情况及产品特点采用信息化管理手段，实现文件和记录电子化，便于管理、使用与知识共享。

1.企业应建立与相适应的质量管理体系文件，包括质量手册、程序文件、规范制度、技术文件和记录等。技术文件应当包括产品技术要求及相关标准、生产工艺规程、作业指导书、检验作业规程和运维操作规程等相关文件。记录应当确保产品设计开发、物料采购、生产、质量控制、运维管理等活动可追溯。

2.企业应建立文件控制程序，系统地设计、制定、审核、批准和发放质量管理体系文件。文件更新或修订时，应按规定评审和批准，应能识别文件的更改和修订状态。分发和使用的文件应当为适宜的文本。

3.企业应建立记录控制程序，包括记录的标识、保管、检索、保存期限和处置要求等。记录应当保证产品生产、质量控制等活动的可追溯。记录应当清晰、完整，易于识别和检索，防止破损和丢失。记录不得随意涂改或销毁。

4.加速器控制系统软件设计开发、采购、安装、检验、运维等过程相关的记录应永久保存；对于受控文件/记录应根据企业的规定处置。

（五）设计开发

1.企业应当依据风险管理控制程序实施软件风险管理活动，结合软件功能、接口、用户界面、现成软件、网络安全等进行风险识别、分析、评价、控制和验证，并贯穿于软件生存周期全过程。

（1）企业应在加速器控制系统软件设计开发策划阶段制定软件风险管理计划，包括风险管理活动的范围、职责和权限的分配、风险管理方针、风险可接受性准则、风险管理活动计划、验证活动、生产和生产后信息的收集等。

（2）企业应建立软件缺陷管理制度，对软件开发及使用过程中发现的各类缺陷进行记录、评估、修复、回归测试、风险管理、评审等，形成软件缺陷分析报告，例如：非预期输入数据的响应，使用的外部组件的错误（比如数据库、操作系统和IT环境），网络安全风险/威胁、人机界面和人为错误等。

2.企业应根据软件产品特点、质量管理体系要求、合规性等因素制定软件版本命名规则并予以记录，各字段含义明确且无歧义无矛盾。例如，软件版本命名规则为X.Y.Z.B，其中X表示重大增强类更新，Y表示轻微增强类更新，Z表示纠正类更新，B表示内部构建，则软件完整版本为X.Y.Z.B，而软件发布版本为X，此时X发生变化应进行许可事项变更，而Y、Z和B发生变化无需进行许可事项变更。

3.企业应建立软件可追溯性分析控制程序并形成文件，涵盖现成软件、网络安全的控制要求，软件可追溯性分析能够追踪到软件需求、软件设计、源代码、测试及风险管理之间的关系，相互之间满足正确性、一致性和完整性的要求。

4.企业应对软件需求进行分析，包括法规、标准、用户、产品、功能、性能、接口、用户界面、网络安全、警示提示等软件需求，确定风险管理、可追溯性分析、现成软件使用评估、软件确认测试计划创建、评审等活动要求，形成软件需求规范和评审记录并经批准，适时更新并经批准。

5.企业应依据软件需求规范实施软件体系架构、功能、性能、算法、接口、用户界面、单元、网络安全等设计，确定风险管理、可追溯性分析、现成软件使用评估、软件验证测试计划创建、评审等活动要求，形成软件设计规范和评审记录并经批准，适时更新并经批准。

6.企业应制定软件测试计划，依据软件测试计划进行单元测试、集成测试、系统测试，涵盖现成软件、网络安全的测试要求，形成相应软件测试记录、测试报告以及评审记录，并适时更新。

7.企业应制定软件确认制度，确认内容包含用户测试、评审等活动要求，涵盖现成软件、网络安全的确认要求，并保持相关记录。能够保证软件满足用户需求和预期目的，且软件已知剩余缺陷的风险均可接受。

8.企业软件更新应形成文件，涵盖现成软件、网络安全的变更控制要求，确定软件更新请求评估、软件更新策划、软件更新实施、风险管理、验证与确认、缺陷管理、可追溯性分析、配置管理、文件与记录控制、评审、用户告知等活动要求，形成相关文件和记录并经批准，适时更新并经批准。软件版本变更应当与软件更新情况相匹配。验证与确认应当根据软件更新的类型、内容和程度实施相适宜的回归测试、用户测试等活动。

（六）采购

对于加速器控制系统软件，企业应在质量协议或采购合同中明确主要技术参数、规格型号、质量要求及验收标准等内容，必要时提供供方出厂检验报告。

#### 1.采购流程

企业应建立采购程序文件，包括采购流程，应满足以下要求：

（1）对不同的采购部件或原材料应规定不同的控制方式，并对采购文件的制定、评审、批准作出明确的规定；

（2）对合格供方的选择、评价和再评价应予以明确规定；

（3）对采购产品符合性的验证方法进行规定；

（4）对采购过程的记录应进行保持的规定；

（5）实施采购和采购管理应进行规定。

#### 2.物料分类

（1）企业应根据采购物料对整个产品的影响程度将物料进行分类，通常分为A、B、C三类，包括：

A类物料（关键物料），对最终产品的主要功能或构成产品关键性能指标和重要安全性指标起决定性作用的材料、器件等。

B类物料（重要物料），对实现产品功能、性能和安全指标起重要作用的材料、器件等。

C类物料（一般物料），对产品的功能、性能和安全性指标有轻微影响，或生产过程所用的辅助性物料，主要指除A、B类之外的采购物料或服务。

（2）物料具体分类应在物料明细表或物料清单（BOM）中明确，至少包含产品名称、规格型号、技术指标或质量要求、分类等级等内容。还应根据产品分类情况，对供方提出相应的控制要求。

（3）企业采购的原材料应满足设计输出的要求，采购部件应遵守相应的采购合同规定、合同附件技术要求、质量协议等，采购产品的要求应不低于国家/行业标准规定的最低要求。

#### 3.供应商管理

（1）企业应依据《医疗器械生产企业供应商审核指南》及物料分类，通常将供方分为A、B、C三类。企业应制定对供方进行选择、评价和再评价的准则，评价范围一般包括：质量、服务、人员能力、供货能力、企业资信等。企业还应保存供方评价的结果和评价过程的记录，对于首次选择的供方应关注其资质及其样品试用情况的评价，对于非首次选择的供方应关注生产、检验和采购部门对其产品使用情况的评价。

（2）企业应与合格供方签订较为固定的供需合同或技术协议，以确保物料的质量和稳定性。对于涉及最终产品的安全、性能的采购物料，应保存对供方实施控制的记录。采购文件中（可以在与供方的协议中形成）的表述应符合采购信息的要求，确保采购信息的可追溯。

#### 4.采购记录

（1）企业应保存所有采购过程活动记录，如采购合同、入库单等信息，应保证关键物料的正向及逆向可追溯。

（2）在采购方面：

①企业关键物料供应商的资质、质量协议及采购合同应完整，应满足可追溯性要求，应明确物料名称、规格型号、主要技术指标、验收规范等内容。

②企业关键物料的随机资料如说明书、认证证书、检验报告、安装记录、调试测试记录等应满足要求。

③若需供应商提供出厂检验报告的，应在采购合同或质量协议中明确且应确认检验报告中的检验内容是否满足要求；若供应商提供物料的规格型号、性能指标、核心功能等发生变更的，应予以说明、且甲乙双方须进行确认，必要时，生产企业应对采购技术要求等文件进行同步变更。

④企业关键物料的来料检验规范、检验记录应完整，应满足技术要求及可追溯性要求。

⑤企业关键物料供应商定期评价或再评价记录应完整、充分，应按照供应商管理制度进行筛选。

⑥当采购的关键物料不合格时，企业应按照不合格品控制要求进行评审、处置，若发生严重不合格时，应进行退换货等处理。

#### 5.采购物料的验证

企业应按规定的采购控制程序和供应商审核指南等要求实施采购验证。应具有采购产品的进货检验规范，明确检验项目、检验方法（包括检验设备）、抽样方法、判定准则等。

（七）生产管理

不涉及。

（八）质量控制

企业应建立质量控制程序，规定检验部门、人员、操作等要求，并规定检验仪器设备的使用、校准等要求。

#### 1.控制程序

（1）企业应建立相应质量控制程序文件，如：检验控制程序、不合格品控制程序、监视测量设备管理控制程序等。

（2）企业建立的质量控制文件应包含：来料检验、过程检验、委托检验、不合格品的来源、分类、处置流程及方式，监视测量设备的检定/校准、使用和维护等。

#### 2.来料、过程控制

（1）企业应根据物料的管理类别建立相应的来料、过程检验规程。

（2）来料检验规程一般包含通用物料检验规程和专用物料检验规程。外购设备验收应包含出厂合格资料和现场验收报告。

（3）过程检验规程一般应包含单元测试、集成测试、系统测试、网络安全测试、回归测试等。

3.检验过程

（1）企业应根据产品的特性建立检验相关程序文件，包含来料检验、过程检验规范，并出具相应的检验报告或证书。

（2）企业进行常规控制的来料检验、过程检验项目，原则上不得进行委托检验。对于检验条件和设备要求较高，确需委托检验的项目，可委托具有资质的机构进行检验，以证明产品符合强制性标准和经注册或者备案的产品技术要求。

（3）企业对加速器控制系统来料检验、过程检验部分内容应按照相关检验规程要求在项目现场开展，并对合格品、不合格品进行标识，便于检查和监控。

#### 4.不合格品控制

（1）企业应建立不合格品控制程序，规定不合格品控制的部门和人员的职责与权限。

（2）企业应明确不合格物料的识别、记录、隔离和评审流程，根据评审结果，对不合格物料采取相应的处置措施。

（3）企业应按程序文件要求对不合格物料进行分门归类、原因分析，纠正预防措施应合理、有效。必要时，应进行评审，且保留评审记录。

（4）企业应对可以返工的不合格物料作出规定，应按照返工文件要求进行返工活动，并记录。

（5）企业应建立不合格物料处置记录，记录内容应完整且能有效反映处置的过程，满足可追溯要求。

5.记录要求

质量控制过程中产生的记录应完整、可追溯。