ICS 11.040.60
CCS F 91

中华人民共和国国家标准

GB/T XXXXX—XXXX

医用轻离子治疗装置　远程控制与数据传输技术要求

Medical light ion therapy device—Technical requirements for remote control and data transmission

（工作组讨论稿）

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国医疗装备产业与应用标准化工作组（SAC/SWG26）提出并归口。

本文件起草单位：兰州泰基离子技术有限公司、国科离子（杭州）医疗科技有限公司、机械工业仪器仪表综合技术经济研究所。

本文件主要起草人：

医用轻离子治疗装置　远程控制与数据传输技术要求

1　范围

本文件给出了医用轻离子治疗装置远程控制与数据传输的总体框架，规定了远程控制与数据传输的总体要求、应用层要求、服务层要求、网络传输层要求、数据采集层要求、可靠性要求及安全保障体系要求。

本文件适用于医用轻离子治疗装置远程控制与数据传输的开发和应用。

2　规范性引用文件

本文件没有规范性引用文件。

3　术语和定义

下列术语和定义适用于本文件。

3.1

故障　fault

可能导致轻离子治疗装置或设备执行功能的能力降低或丧失的异常情况。

3.2

故障诊断　fault diagnose

分析轻离子治疗装置或设备状态信息，确定故障类型并判别其严重程度。

3.3

计划性维护　planned preventative maintenance

将设备计划性、周期性的维护任务纳入设备管理，到维护时间定时提醒运维工程师进行计划性维护和设备状态确认。

3.4

敏感信息　sensitive information

装置的关键参数、身份验证数据、密码、密钥、设备运行等。

3.5

平台　platform

能够按需提供应用程序部署、管理和运行的操作环境。

[来源：GB/T 39837—2021,2.11]

3.6

远程控制　remote control

利用网络或无线通信实现对医用轻离子治疗装置中设备或系统的远程操作、监控和管理的技术。

3.7

预测性维护　predictive maintenance

根据历史数据对轻离子治疗装置或设备未来状态进行预测，根据预测结果提出维护建议。通过设备参数的记录和数据分析来减少故障及其运行成本，通过基于条件的操作来预测未来故障的可能性。

4 缩略语

下列缩略语适用于本文件。

AR：增强现实（Augmented Reality）

HTTPS：超文本传输协议（Hypertext Transfer Protocol Secure）

IP：网际协议（Internet Protocol）

MQTT：消息队列遥测传输（Message Queuing Telemetry Transport）

MR：混合现实（Mixed Reality）

OPC：用于过程控制的OLE（对象连接与嵌入）（OLE for Process Control）

OPC UA OPC：统一架构（OPC Unified Architecture）

VPN：虚拟专用网（Virtual Private Network）

VR：虚拟现实（Virtual Reality）

5 系统概述

医用轻离子治疗装置远程控制与数据传输框架模型见图1。

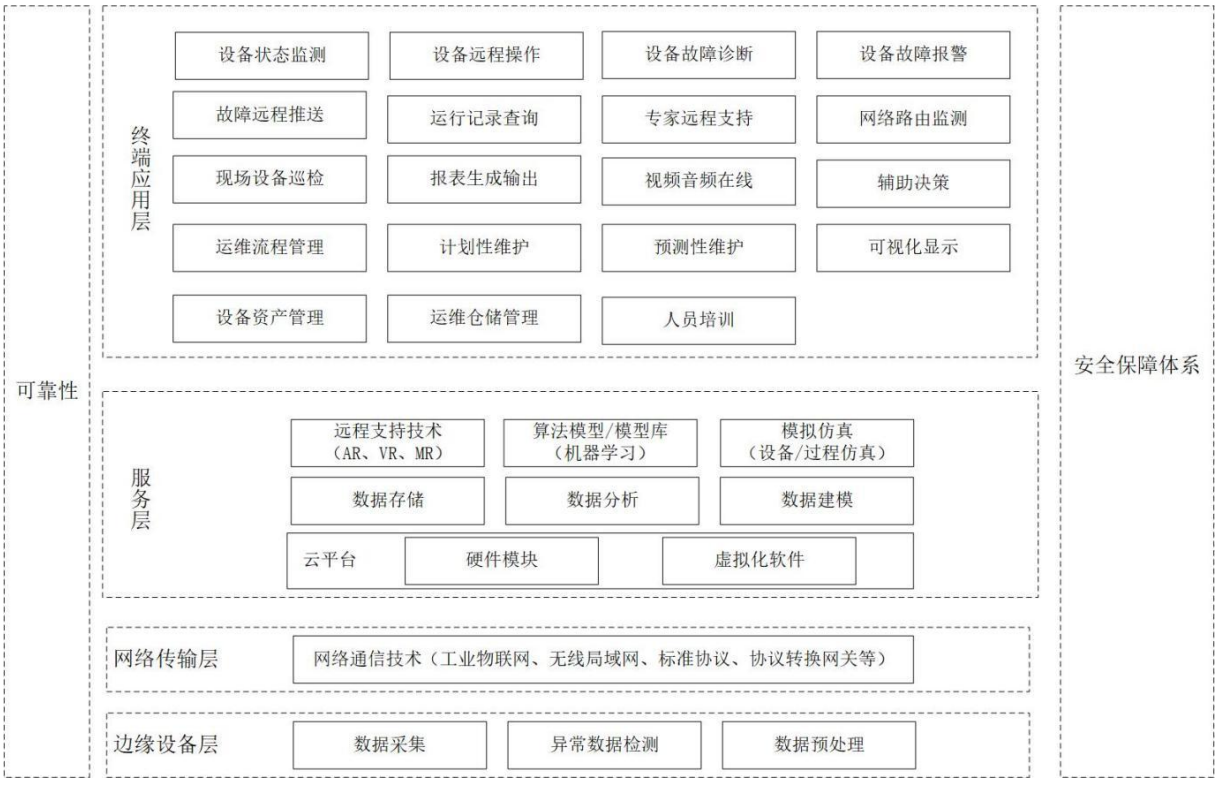

图1 远程控制与数据传输框架模型

6 总体要求

医用轻离子治疗装置远程控制与数据传输设计应当充分考虑被控设备分布范围广，种类多，接口繁杂的特性，围绕高实时性、高安全性、高可靠性和可扩展性等控制需求展开，在系统设计中的总体要求如下。

a) 应采用分布式分层架构设计，确保远程控制系统的高可用性和扩展性。
b) 在系统设计中，应采用模块化与微服务化模式，实现独立可替换的微服务单元，确保远程控制系统的高可靠性。
c) 应采用安全可靠的数据传输协议、先进的加密技术和认证机制，确保数据在公网或专用网络上的安全传输，防止数据在传输过程中被窃取或篡改，且不泄露敏感信息，符合医疗数据安全与隐私保护法规要求。
d) 应采用成熟的网络架构，网络传输设备应满足设计的数据传输速率要求，确保所有涉及设备的关键数据能得到实时、有效、全面、精准地采集。
e) 应实施严格的数据权限管理，按照最小授权原则分配数据访问权限，确保不同角色的用户仅能访问与其职责相对应的数据和功能，防止非授权访问和滥用，降低因误操作或恶意行为带来的安全风险。

7 应用层要求

7.1 设备状态监测

设备状态监测功能应满足如下要求。

a) 支持设备运行状态的监测，监测数据应实时、准确、全面，包括但不限于设备工作状态、运行参数、能量输出、环境参数等信息。
b) 支持设置设备运行状态的监测周期，监测频率应满足设备运行特性需求。
c) 支持设备运行状态实时曲线绘制功能。

7.2 设备远程操作

设备远程操作功能应满足如下要求。

a) 支持设备远程登录。
b) 支持设备远程控制操作并反馈操作结果，关键设备远程操作应支持二次确认。
c) 支持设备运行参数远程调试、自动上传和手动批量导入功能。
d) 设备参数调节精度满足产品技术要求。

7.3 设备故障诊断

设备故障诊断功能应满足如下要求。

a) 支持设备故障类型识别。
b) 支持设置设备故障告警的触发条件或阈值。
c) 支持识别故障告警的诊断结果。

7.4 设备故障报警

设备故障报警功能应满足如下要求。

a) 支持故障等级评判和识别并将故障分级，如严重、一般和轻微分级。
b) 支持设置故障告警触发条件修改功能。
c) 支持故障显示，设备故障进行前置显示和告警。
d) 支持故障报警紧急屏蔽功能。
e) 设备出现故障、偏离预设参数范围、偏离正常运行允许阈值或其他异常情况时，系统应能即时发出报警。

f） 报警阈值应根据设备性能和技术规范合理设定，并支持用户自定义调整。
g） 报警信息应详细记录异常类型、发生时间、持续状态等信息，便于追溯分析。

7.5 故障远程推送

支持通过短信、邮件、微信等形式将故障告警信息及时推送至运维工程师。

7.6 运行记录查询

运行记录查询功能应满足如下要求。
a） 提供简便快捷的查询功能，如允许用户按照时间、设备、操作人员等维度搜索和浏览历史记录。
b） 查询结果应以易于理解的形式呈现，支持既定格式导出和打印功能，方便进行分析和问题追溯。

7.7 专家远程支持

专家远程支持功能应满足如下要求。
a） 支持设备故障诊断、设备维修的远程专家在线指导。
b） 支持远程可视对讲功能。

7.8 网络路由监测

网络路由监测功能应满足如下要求。
a） 支持网络链路状态监测，实时监测网络通信路径，确保数据传输畅通无阻。
b） 支持设置网络状态监测指标、网络故障报警机制和网络恢复策略。
c） 网络路由应进行冗余设计，确保远程控制服务的连续性。

7.9 现场设备巡检

现场设备巡检功能应满足如下要求。
a） 支持现场运维工程师通过移动端完成设备检查、数据录入和异常上报。
b） 支持根据设备特性及维护计划，生成详细的巡检任务清单和检查标准。
c） 支持在线帮助，如设备操作规程、故障处理提示等。

7.10 报表生成输出

报表生成功能应满足如下要求。
a） 可定时自动生成指定数据内容的报表。
b） 支持报表的自定义、预览、打印输出，或以其他格式导出保存或转发的功能。

7.11 视频音频在线

视频音频在线功能应满足如下要求。
a） 支持视频音频监控，能实时获取设备运行画面和声音信息。
b） 支持视频音频数据压缩和加密传输，确保画质清晰、音质良好且数据安全。
c） 支持视频音频监控系统故障检测与报警，确保设备异常时能及时通知运维工程师。

7.12 远程运维流程管理

远程运维流程管理功能应满足如下要求。
a） 制定远程运维作业流程，如日常巡检、故障排查、紧急维修等环节的流程管理。
b） 远程运维作业流程可视化，确保远程运维流程易于理解与操作，流程流转清晰明确。

c） 可引入电子签名，识别远程运维流程各节点的执行者身份并记录操作详情。
d） 支持跨部门协作功能，当远程运维流程涉及多个团队时，能够无缝对接，协同完成运维任务。
e） 制定远程运维流程和结果的反馈机制和改进流程，持续优化设备性能和运维服务。

7.13 计划性维护

计划性维护功能应满足如下要求。

a） 根据设备的状态，设置计划性的周期性维护任务。
b） 支持运维工程师定期维护的提醒功能。
c） 支持维护信息的录入、确认、记录和维护状态的更新功能。
d） 支持设备运行参数的定期记录、统计、进一步分析和给出预测性维护建议。

7.14 预测性维护

预测性维护功能应满足如下要求。

a） 支持根据设备的状态监测数据、故障数据等分析设备运行关键指标，并设置预测性维护策略。
b） 支持对设备的使用寿命、保养时间或优化备件时间等进行预测。
c） 支持运维工程师远程查看或确认设备的预测性维护信息。

7.15 可视化显示

可视化显示功能应满足如下要求。

a） 支持显示设备的实时运行状态及故障告警信息。
b） 支持使用常规图表显示设备的历史数据。
c） 支持通过显示屏、个人计算机（PC）、移动终端等设备进行可视化显示。

7.16 设备资产管理

设备资产管理功能应满足如下要求。

a） 支持建立设备的台账信息。
b） 支持浏览和查询设备的历史数据。
c） 支持设备备件信息的管理。
d） 支持设备历史数据的导出或打印。
e） 支持基于设备台账信息、故障记录、维修记录生成设备检修及保养计划。

7.17 仓储管理

仓储管理应满足如下要求。

a） 应根据需求做好物料的分类标准，设计规范的物料编码规则，并制定相应的储备、使用与回收策略，便于快速查询其技术说明及更换维护流程。
b） 支持物料入库、出库等流程管理和设置。
c） 支持物料库存管理，如库存量、库存位置、质保期监控等。
d） 支持物料安全库存预警线设置和低库存预警等功能。
e） 记录物料的领用、安装、退库、报废等全生命周期信息。
f） 及时更新物料消耗情况，剩余物料使用寿命等信息，确保账物相符。

7.18 人员培训

人员培训应满足如下要求。

a) 应建立完善的在线培训体系，提供在线培训资源，及时更新维护最新的设备操作手册和技术指南。
b) 可借助 VR 技术提供虚拟仿真环境，模拟故障发生情境，运维工程师能够在不影响设备运行的情况下熟悉设备操作、故障排查等流程。

8 服务层要求

8.1 远程支持技术

远程控制与数据传输宜支持VR、AR、MR等技术，辅助现场进行故障处理。

8.2 算法模型/模型库（机器学习）

远程控制与数据传输宜支持数据统计分析、异常诊断、故障识别、预测评估等远程控制所需的算法模型，为设备运行决策提供可靠的数据支持和智能辅助，具体要求如下。

a) 统计分析模型
   1) 根据关键数据定义统计指标，并规定统计周期、统计粒度和统计方法；
   2) 确保输入模型的数据经过清洗、去噪和预处理，满足统计分析的准确性和可靠性的质量要求；
   3) 根据业务需求，选择合适的统计模型，用于分析设备性能、故障规律等。
b) 异常诊断算法
   1) 确定设备运行状态的正常范围，并设定设备参数偏离正常范围的阈值，以识别异常情况；
   2) 开发或选择适用于医疗设备的异常检测算法，并制定算法性能评估指标和阈值标准；
   3) 建立异常诊断结果的实时反馈机制，并提供异常原因初步分析。
c) 故障识别算法
   1) 构建基于设备原理、历史故障记录的故障模式库，为故障识别提供基础。
   2) 制定故障识别算法的标准，确保故障识别的准确性和时效性。
   3) 故障识别算法应与设备维护手册、行业标准和实践经验相吻合，确保故障诊断结果的一致性和权威性。
d) 预测评估模型
   1) 根据设备运行特性和控制需求，选择恰当的预测模型。
   2) 制定预测模型的性能评估指标，确保模型在实际应用中有较高的预测精度。
   3) 基于预测评估结果，制定前瞻性维护策略，以延长设备使用寿命、降低故障发生概率。

8.3 模拟仿真（设备/过程仿真）

远程控制与数据传输宜支持关键设备运行过程模拟仿真。

8.4 数据存储

数据存储功能应满足如下要求。

a) 支持多种类型数据的存储。
b) 支持集中式或分布式的存储方式。
c) 系统具备冗余的数据存储能力。
d) 明确存储的数据类型与结构。
e) 制定数据存储策略和安全标准。

f） 建立定期备份制度、规划灾难恢复方案。
g） 制定数据加密策略，建立严格的访问控制机制，采用多层身份验证和权限划分，确保仅授权人员可以访问相关数据。

8.5 数据分析

数据分析功能应满足如下要求。

a） 支持设备历史数据统计分析功能。
b） 支持设备运行数据与目标数据的比对分析，支持设备运行状态的评估。
c） 支持设备运行数据手动校准，支持异常数据过滤功能。

8.6 云平台

8.6.1 硬件模块

应提供满足远程控制与数据传输运行的硬件，包括计算资源、存储资源、网络资源。
远程控制与数据传输应支持计算、存储等资源的弹性扩容，并根据业务负载情况进行调整。

8.6.2 虚拟化软件

远程控制与数据传输应支持云端部署，支持数据云存储协议并采取可行的虚拟化方案。

9 网络传输层要求

9.1 网络支撑

网络支撑应满足如下要求。

a） 保证网络的连通性，远程控制系统跨互联网部署，网络通过专用网络接入。
b） 支持已授权移动终端、个人电脑、服务器访问远程控制与数据传输。
c） 网络带宽、速率、时延、优先级等能够保证连接设备的正常接入。

9.2 数据传输

数据传输功能应满足如下要求。

a） 支持通过专用网络进行数据传输。
b） 支持通过有线或无线的方式进行数据传输。
c） 已修改为“支持工业以太网不同通信协议的适配转换，支持 HTTP、OPC/OPC UA 、MQTT 等通信协议。
d） 支持数据传输过程中的加密算法，采用必要的数据加密技术，确保数据在传输过程中的安全。

9.3 接口协议

接口协议应满足如下要求。

a） 选择高效且适合大规模数据传输的接口协议规范，保证大量实时数据的交互，确保本地设备与远程控制系统的软件无缝对接。
b） 根据实际数据的类型，选择符合统一标准的协议数据交换格式。
c） 接口协议应采用模块化设计，并具备良好的版本控制机制，保证新的版本升级不影响旧版本的正常使用，同时提供向前兼容和向后兼容的支持。

10 数据采集层要求

10.1 概述

数据采集层通过智能控制器、PLC等采集设备对现场数据进行采集，包括数据采集、异常数据检测、数据预处理。

10.2 数据采集

数据采集功能应满足如下要求。

a) 应制定可行的数据采集方案，确保数据来源可靠、完整。
b) 应明确符合远程控制业务需求的数据采集对象和类型，可按动态数据和静态数据来规划要求。
c) 应根据设备运行特点和控制需求，设定合理的数据采集频率，确保数据更新的实时性。
d) 应针对不同数据类型设定相应的采集精度要求，确保数据的准确性。
e) 应定义统一规范的数据采集接口标准，确保数据采集的兼容性和便捷性。
f) 应制定数据封装格式，并有确保数据完整性的机制。
g) 应采用统一的时钟信号，所采集的数据应具有时间戳标记。

10.3 异常数据检测

应支持数据质量自动监测，建立异常数据检测机制，及时发现并处理异常数据，以满足远程控制需求的数据质量要求。

10.4 数据预处理

应支持数据的边缘预处理，数据预处理应满足如下要求。

a) 应提供原始数据的抽取功能。
b) 应支持不同设备、系统产生的异构数据转换成统一标准格式整合功能。
c) 应支持对数据进行脱敏处理。

11 可靠性要求

可靠性应满足如下要求。

a) 系统正常运行时，对设备本身的正常运行无任何影响。
b) 系统发生故障时，应不影响被控设备的正常运行。
c) 系统需要支持网络容灾保护，组网方案中的关键业务部件不存在单点故障。
d) 故障恢复切换：

系统在存在备份点的设备发生故障，短时间（小于切换时间）内无法恢复时能够快速切换，切换后保证数据完整和一致，保证7×24小时不间断运行。

e) 恢复策略：

系统应有良好的备份和恢复策略，系统数据和业务数据可在线备份和恢复，恢复的数据应保持其完整性和一致性。

f) 恢复措施：

系统应具备自动或手动恢复措施，以便在发生错误时能够快速地恢复正常运行。

g) 系统恢复时间：

要求系统发生影响业务的故障后能够在1小时之内恢复。

12 安全保障体系要求

应遵循现有且适用于远程控制与数据传输规划、设计、建设等各个环节的国家和行业安全技术和安全管理的相关标准。包括病毒防护、权限管理、数据安全、安全审计、数据备份恢复等。

12.1 网络安全

网络安全应满足如下要求。

a) 应部署必要的网络安全设备，保障网络链路的安全性，如 VPN、智能安全网关等。
b) 互联网与局域网之间应采用必要的物理隔离手段，如防火墙、网关等。
c) 应支持对病毒查杀、入侵防护等具备自定义规则的能力。
d) 建立对未知安全威胁的发现，通过将已发现的异常行为与原始日志进行关联，用于探测未知安全威胁。
e) 应支持漏洞扫描和补丁升级功能。
f) 应具备安全告警功能。

12.2 防病毒

防病毒功能应满足如下要求。

a) 应提供对网络病毒、恶意软件的检测、告警、消除的手段。
b) 应提供防病毒软件，且具有全面查杀病毒和恶意软件的能力。
c) 应提供系统漏洞扫描和补丁升级的能力。

12.3 防入侵

应具备对入侵监测、记录、告警、阻断等方面的安全能力。

12.4 接口安全

接口安全应满足如下要求。

a) 应提供外部接口，可与其他安全系统集成。
b) 系统的部署和使用，应避免带来新的安全漏洞。

12.5 权限管理

权限管理应满足如下要求。

a) 支持用户类型的设置，如管理人员、运维工程师、审计人员等。
b) 支持根据用户类型设置不同的权限，如浏览信息的范围，操作的范围等。
c) 支持对远程控制系统的用户进行身份鉴别、证书鉴别或双因子认证等。
d) 支持对远程访问主机的申请和审批，如申请访问时间，访问端口，访问事由等。
e) 支持用户通过 HTTPS 或第三方认证体系方式登录。
f) 支持用户自动注销功能，在无人值守期间阻止非授权用户访问和使用。
g) 支持详细记录用户权限操作日志功能。

12.6 系统安全

系统安全应满足如下要求。

a) 应提供必要的物理防护（如非授权人员无法进入控制区域）。
b) 应支持登录节点鉴别功能，如非授权地区禁止登录，非授权 IP 禁止访问等。

c） 对暴力破解等访问攻击，应具有登录验证码，或多次访问失败后账户锁定或客户端锁定功能。

12.7 数据安全

数据安全应满足如下要求。

a） 系统应支持数据加密技术，确保数据存储和传输的保密性。
b） 系统应提供必要的手段，确保数据存储和传输的完整性。
c） 系统应支持去除、匿名化包含个人信息的数据的能力。
d） 对数据的访问应设置必要的访问认证机制和权限管理。
e） 系统应确保系统数据的真伪性，具有辨别数据伪造的能力。
f） 系统控制指令应通过安全加密通道传输，确保指令不被篡改或拦截。

12.8 安全审计

安全审计应满足如下要求。

a） 所有用户的操作应被记录并可被审核。
b） 审计范围应支持覆盖远程控制系统的所有用户。
c） 审计范围应包括重要用户行为、系统操作异常和重要系统命令等重要安全事件。
d） 审计记录应得到保护，避免受到非系统授权的修改或删除等。
e） 审计记录可根据系统使用的实际需求，按照指定的有效期保存。

12.9 数据备份恢复

数据备份恢复功能应满足如下要求。

a） 应具备海量数据存储功能，保证信息的保存。
b） 支持数据的手动备份和自动备份。
c） 支持数据的全量备份和自增量备份。
d） 支持数据的异步备份和同步备份。
e） 支持数据的本地备份和异地备份。

参 考 文 献

[1] GB 17859—1999 计算机信息系统安全保护等级划分准则

[2] GB/T 25069—2022 信息安全技术术语

[3] GB/T 28827.4—2019 信息技术服务 运行维护 第4部分：数据中心服务要求

[4] GB/T 39837—2021 信息技术远程运维技术参考模型

[5] GB/T 42136—2022 智能制造 远程运维系统通用要求

[6] YD/T 1478—2006 电信管理网安全技术要求

[7] YY 9706.264—2022 医用电气设备 第2-64部分：轻离子束医用电气设备的基本安全和基本性能专用要求