



中华人民共和国国家标准

GB/T XXXXX—XXXX

采用机器人技术的医用电气设备 远程传输 通用要求

Medical electrical equipment employing robotic technology General requirements for
remote transmission

(点击此处添加与国际标准一致性程度的标识)

草案版次选择

(本草案完成时间：)

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX – XX – XX 发布

XXXX – XX – XX 实施

国家市场监督管理总局 发布
国家标准化管理委员会

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。

本文件由国家药品监督管理局提出。

本文件由国家药品监督管理局归口。

本文件起草单位：

本文件主要起草人：

采用机器人技术的医用电气设备 远程传输通用要求

1 范围

本文件规定了借助远程通信实现其预期使用目的的全部或部分操作的采用机器人技术医用电气设备/系统的远程传输通用要求和测试方法，其中，技术要求包括功能要求、性能要求和安全要求，测试方法包括测试环境、测试工具和测试内容。

本文件适用于具有远程通信能力，并且借助远程通信能力实现其预期使用目的的全部或部分操作的采用机器人技术的医用电气设备/系统。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB 4943.1-2022 音视频、信息技术和通信技术设备 第1部分：安全要求

GB 9706.1-2020 医用电气设备 第1部分：基本安全和基本性能的通用要求

YY/T 1686-2020 采用机器人技术的医用电气设备 分类

GB/T 25000.51-2016 系统与软件工程 系统与软件质量要求和评价（SQuaRE） 第51部分：就绪可用软件产品（RUSP）的质量要求和测试细则

YY 9706.102-2021 医用电气设备 第1-2部分：基本安全和基本性能的通用要求 并列标准：电磁兼容要求和试验

YY 9706.277-2023 医用电气设备第2-77部分：采用机器人技术的辅助手术设备的基本安全和基本性能专用要求

YY 9706.278-2023 医用电气设备 第2-78部分：康复、评定、代偿或缓解用医用机器人的基本安全和基本性能专用要求

YY/T 1843-2022 医用电气设备网络安全基本要求

YY/T 1712-2021 采用机器人技术的辅助手术设备和辅助手术系统

YY/T 1901-2023 采用机器人技术的骨科手术导航设备要求及试验方法

YY/T 1941-2024 采用机器人技术的腹腔内窥镜手术系统

3 术语和定义

下列术语和定义适用于本文件。

3.1.1

远程通信 Telecommunication

在连接的系统间，通过使用模拟或数字信号调制技术进行的语音、数据、传真、图像、音频、视频和其他信息的电子传输。

在医疗领域，专业医疗人员或患者应用远程通信技术交换信息，用于诊断、治疗和预防疾病，研究和评估，以及对医疗健康服务人员的指导和培训等。

3.1.2

采用机器人技术的医用电气设备 / 系统 Medical electrical equipment/system employing

robotic technology

一种基于机器人技术开发的医用电气设备或医用电气系统，包含由可编程医用电气系统(PEMS)驱动的装置，模仿、辅助或代替医护人员/患者执行移动、操纵或定位。

[来源 YY/T 1686-2024,3.1.6]

3.1.3

传输延时 Transmission Latency

传输延时 (Transmission Latency)：是指业务相关完整数据包从源端发出到目的端接收完成所需的时间。

3.1.4

双线路故障转移 Dual WAN Failover, DWF

双线路故障转移 (Dual WAN Failover, DWF) 是一种网络冗余配置，旨在通过使用两个独立的广域网 (WAN) 连接来提高网络的可靠性和可用性。当一个 WAN 连接出现故障时，网络流量可以自动切换到另一个可用的 WAN 连接，以确保持续的互联网访问。

3.1.5

本地端 Local End

指远程医疗应用场景中靠近患者的一端。

3.1.6

远程端 Remote End

远程医疗应用场景中远离患者的一端。

3.1.7

双控制台热备 Dual Console Hot-Standby

双控制台热备 (Dual Console Hot-Standby) 是指在本地端和远程端分别配置医生控制台并处于热备状态，当网络出现中断或远程控制台发生故障时，本地端医生可继续操作已保证医疗操作的连续性和安全性。

来源：“双医生控制台”这一术语起源于手术机器人领域的协作和培训需求，随着技术的发展和行业实践的积累逐渐形成并普及。达芬奇手术系统等机器人手术系统的推出和普及，推动了这一术语在医疗和手术机器人领域的广泛应用。

3.1.8

网络性能监测

网络性能监测 (Network Performance Monitoring, NPM) 的定义通常涉及对网络的各种性能指标进行测量和分析，以确保网络的正常运行和优化。这些性能指标可以包括延迟、抖动、吞吐量、丢包率等，以确保网络的正常通信和系统正常运行并有效执行操作。网络实时监测的目的是在网络发生异常或故障时，能够立即发现并采取相应措施，将风险控制在接受水平。

3.1.9

局域网

局域网 (Local Area Network, 简称 LAN) 是指在相对较小的地理范围内 (如医院、办公室、校园或建筑物内) 连接计算机、服务器、打印机和其他网络设备的网络。局域网通过有线或无线方式实现设备之间的数据传输和资源共享，具有高数据传输速率、低延迟和较高的可靠性。

3.1.10

广域网

广域网 (Wide Area Network, 简称 WAN) 是指在广泛的地理范围内 (如城市、国家或跨国) 连接

多个局域网（LAN）的网络。广域网通过公共或私有通信设施（如电话线、光纤、卫星链路等）实现远距离的数据传输，支持跨地域的通信和资源共享。

3.1.11

以太网

以太网（Ethernet）是一种广泛使用的局域网（LAN）技术，用于连接计算机和其他设备以形成网络。它定义了物理层和数据链路层的规范，允许设备通过共享介质进行通信。

3.1.12

传输层安全协议

传输层安全协议（TLS, Transport Layer Security）是一种用于在计算机网络上提供安全通信的协议。TLS 通过加密数据、验证通信双方的身份以及确保数据完整性来保护传输中的数据不被窃听、篡改或伪造。TLS 广泛应用于保护互联网通信，如 HTTPS、电子邮件和即时消息等。

3.1.13

网络安全能力

基于风险管理使产品数据和/或功能具有可接受水平的保密性、完整性、可得性等网络安全特性的技术措施。

4 要求

4.1 远程功能要求

4.1.1 远程通信

4.1.1.1 通信方式

制造商应明确建立远程端与本地端的网络通信方式。（支持有线（如互联网、数据专线等）、无线（如5G等）传输。）

4.1.1.2 组网方式

制造商应明确建立远程端与本地端网络通信的网络拓扑结构、通信协议和通信端口，并通过体系结构图和物理拓扑图来表示这些连接方式。

4.1.1.3 网络性能要求

制造商应给出远程环境下设备运行所需的最低网络性能要求。

注：制造商应通过研究资料证明为保证系统性能应满足的网络条件参数，可能包括：带宽、网络时延、网络抖动、丢包率、误码率等。

4.1.1.4 网络性能监测

- a) 网络性能参数监控：如果网络参数的波动或超出范围要求会对患者安全产生风险，MEE/S ERT 应对些网络性能参数进行监控。
- b) 设备状态监控：系统应能监控手术机器人的运行状态（如机械臂的位置、操作指令反馈），并确保远程端操作者获得必要的设备状态信息。
- c) 实时画面与音频监控：必要时，系统应确保操作端能持续获取清晰的远程画面和音频。

4.1.1.5 远程端与本地端的提示信息

MEE/S ERT 监控到的网络状态应在用户界面显示；在网络条件下降至一定程度时给出相应的提示信息或报警，必要时应给出操作提示信息。

应确保远程端医生获得安全有效操作的必要的提示信息，一般情况，该提示信息应与本地端医生相同。

如远程医疗场景中远程端的医生需要获得MEE/S ERT以外的信息，这些信息有本地端患者或医生提供，则MEE/S ERT应具备远程视讯功能，实现两地的音视频通话。

4.1.1.6 远程图像延时

如远程操作依赖于或者为了获得医疗器械生成的图像信息，制造商应给出在规定的网络条件下的图像传输延时。

4.1.1.7 远程图像质量

如远程操作依赖于或者为了获得医疗器械生成的图像信息，制造商应给出在规定的网络条件下的图像质量要求。

4.1.1.8 与联合使用器械通信的延时

如MEE/S ERT用于控制其他医疗器械，如电能量激发、内窥镜控制，制造商应明确给出在规定的网络条件下的远程控制、交互操作时允许的延时。

4.1.1.9 操作数据存储要求

如MEE/S ERT具备数据存储能力，应明确相应数据的存储位置以及数据在远程端和本地端的同步方式。应明确数据的查看、读取、导出的权限。

4.1.1.10 审计能力

MEE/S ERT应具备审计能力，包括保存必要的操作信息用于后续审计。

4.1.1.11 应急功能

如果网络参数的波动或超出范围要求时远程操作会对患者安全产生风险，MEE/S ERT应具备DCHS，并应提供紧急情况下的应急功能：

- a) 应具备控制权强制切换功能，当本地端医生或患者认为不宜远程操作或需本地医生干预时，本地医生可强制切换控制权至本地端；
- b) 应具备控制权自动切换功能，在网络条件不佳时，可自动中止远程操作并将控制权切换至本地端；
- c) 远程端和本地端应分别具备急停功能。

4.1.2 远程音视频通信

4.1.2.1 远程音视频通信方式

制造商应提供远程端与本地端之间的远程会议功能，使得两端人员之间能够进行实时的音（视）频通话。并应在说明书中给出备用的音视频通信方式。

4.1.2.2 音画同步

音频信号与视频信号的同步偏差应满足制造商规定的要求。

4.1.2.3 音画延时

制造商应明确远程会议音频、视频传输延时。

4.1.2.4 视频帧率与分辨率

制造商应明确远程会议视频帧率与分辨率。

4.1.2.5 视频与执行装置同步

如果远程端操作者需要通过视频观察MEE/S ERT执行装置，制造商应明确其远程端看到的视频和执行装置的时间差。

4.1.3 双控制台热备及切换

如果网络参数的波动或超出范围要求时远程操作会对患者安全产生风险，MEE/S ERT应具备远程端与本地端双医生控制台热备，制造商应明确控制权切换机制。

4.2 软件功能

4.2.1 设备连接

- a) 远程端具有支持查看本地端设备在线列表和管理功能；
- b) 远程端支持选择指定本地端建立远程网络连接，连接成功后给出提示；
- c) 远程端/本地端支持自行断开与现有病人端/医生端的连接；
- d) 通过网络让本地端与远程端设备进行配对连接，能实现机械臂实时运动控制，动态图像传输，实时参数调节和/或音视频交流。

4.2.2 数据管理

- a) 本地端可以新建、浏览、发送病人信息；
- b) 远程端可以编辑、预览、查看和发送报告；
- c) 数据管理和传输应符合医院关于数据授权和敏感数据保护的要求。

4.2.3 使用限制

制造商应在随附文件中明确在使用远程通信技术时，产品的技术限制与用户使用限制。

4.2.4 应急措施

制造商应在随附文件中明确在使用远程通信技术时，由于网络不稳定可能导致的风险，并制定应急措施要求。

4.2.5 访问控制

产品技术文档中应指明在进行远程通信时，鉴别通信双方的身份(包括设备的身份与操作者的身份)方式，以及基于身份认证基础上的临时密钥协商以及数据传输加密的方式。

a) 身份验证

多因素认证(MFA)：操作者必须使用强密码进行登录，密码应符合复杂性要求(如长度、字符种

类等)并定期更新;还需要通过动态多因素认证(如验证码、TOTP 应用程序、硬件令牌等)来进一步验证操作者身份。

设备证书:每个远程访问设备(如手术控制台)应配备唯一的设备证书,由可信任的认证机构签发。设备证书用于设备身份验证,确保只有授权设备能够连接到手术机器人系统,并且避免单一机器的密钥泄露所产生大规模安全问题。

b) 通信加密

使用协商生成的临时对称密钥,对所有传输的数据进行加密(如 AES-256)。确保数据在传输过程中不会被窃听或篡改。

c) 审计和日志记录

记录所有远程访问活动,包括登录尝试、操作命令、数据传输等。日志应包含时间戳、操作者ID、设备ID、操作类型等信息。

4.3 接口

制造商应给出支持接入外部网络的类型(包括但不限于:外部具有 RJ45 等网络端口、外部具有 USB 等能够转换为网络接口的端口、支持 wifi 或移动通信技术等),应有方法保障远程运动控制信息的可得性:

——有 QoS 机制确保远程运动控制信息的优先级,或

——远程运动控制信息使用独立的传输与处理链路,不与外部网络信息共用。

应当有方法保障手术运动控制信息的完整性:

——远程运动控制信息应有时序,且该时序不依赖于远程端或本地端时钟的绝对值(即当控制过程中,主端或从端时钟由于 NTP 服务等原因发生变化时,不会影响手术运动控制信息的时序);

——远程运动控制信息应具有应用层完整性校验机制(即独立于 TCP/IP 完整性校验以外的机制)。

应当有方法保障远程运动控制信息的保密性:

——远程连接的建立应当具有身份鉴别机制,本地端仅接受身份鉴别通过的手术运动控制信息;

——身份鉴别信息的数据包应被加密,或携带数字签名。

4.4 运行环境

产品技术文档中应指明远程通信的软硬件环境要求,及外部网络环境要求,包括网络适配器、网络架构、网络类型、带宽、时延、丢包率等。

4.5 采用机器人技术的医用电气设备/系统在远程条件下性能要求

在4.1.1.1要求的条件下,产品性能应符合制造商的规定,产品性能的要求应参考本地临床应用场景下的要求来制定,应满足采用机器人技术的医用电气设备适用标准或制造商宣称的性能要求。可能包括控制精度、操作延时、映射频率、图像质量要求等。

注:性能举例见附录B。

4.6 安全要求

4.6.1 网络安全

4.6.1.1 网络报警

制造商应明确对远程通信影响的因素的报警方式。当超过预警值时应采取有效的安全防护措施(包括但不限于自动停止机械臂和远程控制,并通过有效方式输出告警信息)。

4.6.1.2 网络异常安全管控

制造商应明确以下远程安全措施：

- a) 远程设备安全接入和授权方式，避免出现远程非法接入和非法操作；
- b) 系统安全防护措施（包括安全检测和防御措施等）、应急手段、响应周期以及升级方式；
- c) 对使用人员的安全使用要求。

4.6.2 数据安全

4.6.2.1 数据去标识化功能

- a) 远程机器人系统应具备数据去标识化功能，应使用数据加密技术对敏感数据进行保护；
- b) 应在安全网络环境下开展去标识化服务。

4.6.2.2 数据完整性与真实性保障功能

- a) 应采用校验或密码等技术手段，保证重要数据和个人信息来源可靠且未经篡改与破坏；
- b) 应具备对重要数据和个人信息在采集、传输、存储过程中的完整性和真实性的监测能力，当数据受到破坏时，能够及时发现并恢复原始数据。

4.6.2.3 数据存储加密/保密功能

- a) 应采用加密技术以保证重要数据和个人信息存储保密性，包括但不限于用户身份数据、个人健康医疗数据、重要业务数据等；
- b) 应采用经国家密码主管部门认证核准的评估密码产品；
- c) 应根据数据分级分类原则，对达到一定量级和敏感性程度高的数据选择相应的加密方法和强度。

4.6.2.4 数据传输保密功能

- a) 应采用加密技术保证重要数据和个人信息传输的保密性，包括但不限于用户身份数据、个人健康医疗数据和重要业务数据等；
- b) 应采用经国家密码主管部门认证核准的评估密码产品；
- c) 应使用专用网络或数据传输保密性策略。

4.6.2.5 数据传输完整性保障功能

- a) 应采用消息摘要等技术手段保证通信过程中的数据完整性，避免数据在传输过程中受到干扰或被恶意篡改的风险；
- b) 应实现对传输通道两端主体身份的鉴别和认证。

4.6.2.6 数据备份与灾备恢复功能（如适用）

- a) 应支持对重要数据和个人信息的备份功能，并能够人工开启、关闭和设置自动备份策略；
- b) 应明确告知重要数据和个人信息的备份渠道（器械自身和工作站等）、备份位置、备份份数、备份数据访问方式；
- c) 应具备硬件、软件损坏或损毁后的数据恢复能力；
- d) 应定期开展灾难恢复演练，确保备份数据能够满足医疗器械正常生产使用。

4.6.3 系统异常安全管控

为防止因系统出现故障时无法控制机械臂导致临床事故,远程机器人系统应具备控制机械臂停止工作的功能。

- a) 设备应能够实时且不间断地监测子系统模块状态,当设备检测到自身设备会影响临床检测的故障时,应让机械臂停止工作;
- b) 本地端具备保护性停止功能和紧急停止功能,并输出提示信息。

4.6.4 运行环境

产品技术文档中应指明远程通信的软硬件环境要求,及外部网络环境要求,包括网络适配器、网络架构、网络类型、网络参数等。

5 测试方法

5.1 远程功能要求

5.1.1 远程通信

5.1.1.1 通信方式

检查随附文件。

注:示例见附录A

5.1.1.2 组网方式

检查随附文件。

5.1.1.3 网络性能要求

检查随附文件及相应的研究资料。

5.1.1.4 网络实时监测

- a) 将 MEE/S ERT 按照规定的组网方式建立远程连接,并在连接链路上放置网络损伤仪;
- b) 操作进入远程端主从控制,检测连接是否正常;
- c) 使用网络损伤仪设定网络参数,使网络条件与 4.1.1.1 要求的一致;
- d) 观察 MEE/S ERT 对网络条件的监测是否准确;
- e) 调节网络参数,检查相应的监测参数是否准确。

5.1.1.5 远端与本地端提示信息

- a) 按照4.1.1中规定的网络条件建立远程连接;
- b) 操作进入远程端控制模式中;
- c) 通过操作制造系统信息提示,包括操作提示、异常警告和错误报警等;
- d) 在远程端观察是否能看到相应提示信息;
- e) 在远程端观察是否能看到网络状态信息;
- f) 调节网络参数,检查相应的监测参数是否准确,相应的提示或报警符合4.1.1.4的要求。

5.1.1.6 远程图像延时

- a) 将 MEE/S ERT 按 4.1.1 中规定的网络条件建立远程连接,并使网络条件处于最恶劣网络环境;

- b) 将远程控制端和本地端放在同一空间下；
- c) 将秒表放在远程端屏幕边缘，用内窥镜观察秒表，使秒表时间图像在远程端屏幕上清晰显示；
- d) 秒表开启计时，用高速摄像机（曝光时间设定不低于 1/4000s）将秒表和远程端屏幕图像拍摄到一张图片中；
- e) 观察图片中秒表和远程屏幕中秒表的时间差，即为图像延时。共测量 3 次，测试结果取平均值。

5.1.1.7 远程图像质量

- a) 将 MEE/S ERT 按 4.1.1 中规定的网络条件建立远程连接，并使网络条件处于最恶劣网络环境；
- b) 参考本地图像质量测试方法进行测试，应附件 4.1.1.7 的要求。

5.1.1.8 与联合使用器械通信的延时

- a) 将 MEE/S ERT 按 4.1.1 中规定的网络条件建立远程连接，并使网络条件处于最恶劣网络环境；
- b) 将远程控制端和本地端放在同一空间下；
- c) 在远程端进行联合适用器械的激发或停止操作；
- d) 采用示波器显示信号相应时差。

5.1.1.9 操作数据存储要求

按照随附文件的要求进行操作数据的存储，并查看其相应数据的存储位置和数据同步情况。

5.1.1.10 审计能力

查看 MEE/S ERT 的日志记录，是否分别记录本地端和远程的操作。

5.1.1.11 应急功能

- a) 将 MEE/S ERT 按 4.1.1 中规定的网络条件建立远程连接，并使网络条件处于最恶劣网络环境；
- b) 操作进入远程端主从控制；
- c) 本地操作者通过相应的操作是否能主动获取控制权；
- d) 使用网络损伤仪将网络参数调节至操作规定的阈值；
- e) 观察控制权是否按说明书的规定进行自动切换；
- f) 操作观察本地端、远程端分别按下急停按钮时，系统是否都能响应，手术器械末端停止距离应满足制造商的规定。

5.1.2 远程音视频通信

5.1.2.1 远程音视频通信方式

- a) 将 MEE/S ERT 按最恶劣网络环境建立远程连接，并使网络条件处于最恶劣网络环境；
- b) 通过操作可建立远程端和本地端的音视频通信。

5.1.2.2 音画同步

- a) 将 MEE/S ERT 按最恶劣网络环境建立远程连接，并使网络条件处于最恶劣网络环境；
- b) 通过操作建立远程端和本地端的会议功能；
- c) 使用音视频流畅度测试设备分别在远程端分析音视频内容和在本地端分析音视频内容；
- d) 分析音频信号与视频信号的同步时间差；

- e) 负号代表画面在前，正号代表音频在前。

5.1.2.3 音画延时

- a) 将 MEE/S ERT 按最恶劣网络环境建立远程连接，并使网络条件处于最恶劣网络环境；
- b) 通过操作建立远程端和本地端的会议功能；
- c) 使用专业音视频流畅度测试设备在远程端输入音视频信息；
- d) 在本地端分析音视频信息接收的延时；
- e) 使用音视频流畅度测试设备在本地端输入音视频信息；
- f) 在远程端分析音视频信息接收的延时。

5.1.2.4 视频帧率与分辨率

- a) 将 MEE/S ERT 按最恶劣网络环境建立远程连接，并使网络条件处于最恶劣网络环境；
- b) 通过操作建立远程端和本地端的会议功能；
- c) 使用音视频流畅度测试设备分别在远程端和本地端分析音视频画面的帧率和分辨率。

5.1.2.5 视频与执行装置同步

- a) 将 MEE/S ERT 按最恶劣网络环境建立远程连接，并使网络条件处于最恶劣网络环境；
- b) 在本地端视频视野范围内放置秒表，并确保远程端视频内可清晰观察，记录秒表的实际值与远程端视频

5.1.3 双医生控制台热备及切换

- a) MEE/S ERT 按最恶劣网络环境建立远程连接，并使网络条件处于最恶劣网络环境；
- b) 按制造商随附文件操作，可实现远程端与本地端医生控制权切换。

5.2 软件功能

5.2.1 设备连接

- a) 将采用机器人技术的医用电气设备按最恶劣网络环境建立远程连接；
- b) 在远程端查看是否具有支持查看本地端设备在线列表和管理功能。
- c) 查看远程端是否支持选择指定的本地端建立远程网络连接，若能连接，连接成功后是否给出提示；
- d) 分别在远程端/本地端查看是否支持自行断开与现有本地端/远程端的连接；
- e) 通过网络建立远程端连接，进入远程主从控制，查看机械臂实时运动控制，动态图像传输，实时参数调节以及音视频交流功能。

5.2.2 数据管理

- a) 将采用机器人技术的医用电气设备按最恶劣网络环境建立远程连接；
- b) 在本地端进行新建、浏览、发送病人信息操作；
- c) 在远程端进行编辑、预览、查看和发送报告；
- d) 检查随附文件是否对存储的数据类型，授权要求等规定。

5.2.3 使用限制

核查随附文件。

5.2.4 应急措施

核查随附文件。

5.2.5 访问控制

核查产品技术文档是否指明在进行远程通信时，如何鉴别通信双方的身份（包括设备的身份与操作者的身份），以及用户身份鉴别机制覆盖的通信请求（如基于非对称加密和用户名密码机制进行身份鉴别的令牌获取请求、基于令牌的患者数据传输请求、无身份鉴别机制的影像数据传输请求等）。

5.3 接口

核查技术文档是否包括基于OSI或其他网络通信参考模型指明在模型的每一层中，产品所使用的传输协议。

5.4 运行环境

核查随附文件。

5.5 机器人性能要求

- a) 将 MEE/S ERT 按最恶劣网络环境建立远程连接，并使网络条件处于最恶劣网络环境；按照制造商规定的方法进行测试，测试方法与本地端一致。

5.6 安全要求

5.6.1 网络安全

5.6.1.1 网络测试

- a) 按照说明书进行用户密码登入操作方可进行访问控制；
- b) 使用抓包工具对传输数据协议进行测试。

5.6.1.2 网络报警

在5.1.1.4的基础上使用网络损伤仪分别设置延时、丢包率、抖动等制造商明确地对远程通信影响的参数，将各参数设置到制造商规定的报警阈值，观察内窥镜手术系统是否有报警及安全措施。

5.6.1.3 网络异常安全管控

按制造商明确的远程安全措施进行操作测试或查看。

5.6.2 数据安全

5.6.2.1 数据去标识化功能

- a) 用户登录后，查看显示用户信息，查看是否显示除用户名和密码外的其他个人信息；
- b) 查看软件的日志文件，除记录运行过程中的所有操作和状态信息外是否显示医患个人信息；
- c) USB 设备拍照存储图片查看，查看除图像外是否显示医患个人信息；
- d) 查看产品其他部件（如有），是否显示医患个人信息

5.6.2.2 数据完整性与真实性保障功能

- a) 产品装配完整，通过远程网络连接启动，本地端和远程端建立业务连接；

- b) 用 Wireshark 或其他工具通过网络抓包获取业务数据传输信息;
- c) 分析数据传输保密性、真实性以及各组成间的通信加密。

5.6.2.3 数据存储加密/保密功能

使用医疗数据安全检测工具测试产品数据存储保密性。

- a) 验证注册用户表数据库密码字段是否加密;
- b) 登录输入用户名密码, 验证用户密码为隐藏不可见;
- c) 验证日志文件加密存储。

5.6.2.4 数据传输保密功能

- a) 产品装配完整, 通过远程网络连接启动, 本地端和远程端建立业务连接;
- b) 用 Wireshark 或其他工具通过网络抓包获取业务数据传输信息;
- c) 分析数据传输保密性、真实性以及各组成间的通信加密。

5.6.2.5 数据传输完整性保障功能

- a) 系统装配完整, 通过远程网络连接启动系统, 主从端建立连接;
- b) 用 Wireshark 或其他工具通过网络抓包获取业务数据传输信息;
- c) 使用医疗数据安全检测工具测试产品数据传输完整性, 验证数据传输完整, 及各个组成间的通信加密。

5.6.2.6 数据备份与灾备恢复功能

参考GB/T 29765-2021制定数据恢复性测试方案, 对产品进行数据安全测试, 考察数据备份与灾难恢复功能, 在数据受到损坏时, 自动备份数据是否能够正确恢复医疗器械的正常生产使用。系统异常安全管控

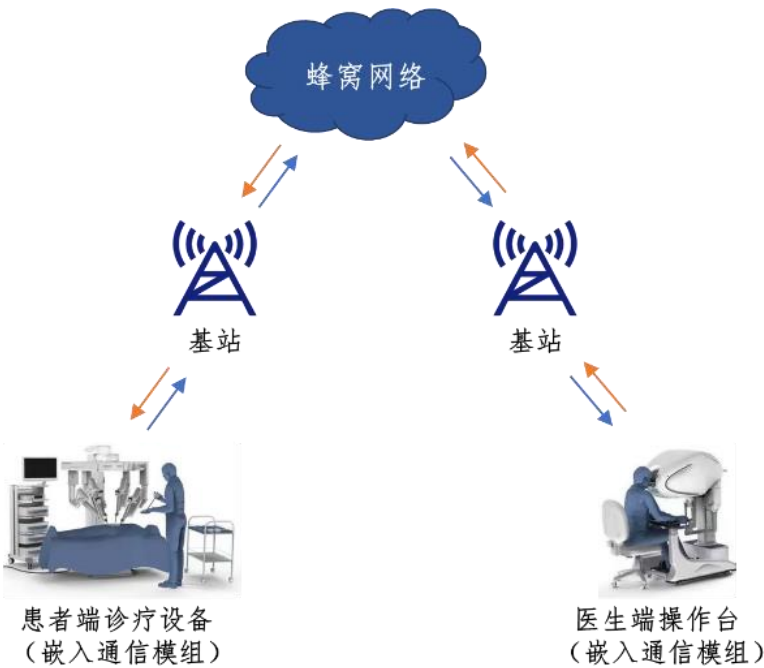
5.6.3 运行环境

检查随附文件。

附录 A
(资料性)
组网方式及网络条件举例

A.1 组网方式

医疗器械通过内嵌4G/5G移动通信模块连接到4G/5G蜂窝通信网络,实现远程数据传输和双向业务连接。其网络拓扑示例如下图所示。



A.2 网络条件

网络参数	要求
最低宽带	$\geq 60\text{Mbps}$
传输速率	$\geq 60\text{Mbps}$
允许的最大延时(RTT)	$\leq 100\text{ms}$
抖动	$\leq 30\text{ms}$
丢包率	$\leq 0.1\%$
误码率	$\leq 10^{-9}$
允许的最大用户并发数和形式	并发数为 1, 形式: 1 台远程端控制台对应 1 台本地端

附 录 B

(资料性)

采用机器人技术医用电气设备远程控制下的性能要求

B.1 基本要求

- a) 手术机器人性能应符合 YY 9706.277, YY/T 1712-2021 标准的相关要求。
- b) 若配有脚踏开关的设备, 可参考 YY/T 1057-2016 的要求。

B.2 设备安全要求

安全方面需符合 GB 9706.1-2020。

B.3 设备控制性能

B.3.1 控制距离准确度

主从控制 X、Y、Z 方向位置准确度标称值, 实测值不劣于标称值。

B.3.2 主从控制距离重复性

主从控制 X、Y、Z 方向位置重复性标称值, 实测值不劣于标称值。

B.3.3 主从控制姿态准确度

主从控制姿态准确度标称值, 实测值不劣于标称值。

B.3.4 主从控制姿态重复性

主从控制姿态重复性标称值, 实测值不劣于标称值。

B.3.5 机械臂有效操作力

机械臂有效操作力标称值, 实测值不劣于标称值。

B.3.6 末端夹持力

末端夹持力标称值, 实测值不劣于标称值。

B.3.7 主从控制延迟时间

主从控制延迟时间标称值, 实测值不劣于标称值。

B.4 音视频业务流畅度

B.4.1 视频卡顿率

医生端与病人端传输视频卡顿率标称值, 实测值不劣于标称值。

B.4.2 视频破损占比

视频破损占比标称值, 实测值不劣于标称值。

B.4.3 视频帧率

医生端与病人端传输视频帧率标称值, 实测值不劣于标称值。

B.4.4 音视频同步性能

医生端与病人端传输视频音画同步延迟标称值, 实测值不劣于标称值。

B.5 网络适应能力指标

B.5.1 传输速率

应明确（由制造商或责任方在随机文件中申明）设备正常运行所要求的最低上下行网络速率。

B.5.2 传输时延

应明确（由制造商或责任方在随机文件中申明）设备正常运行所要求的最大端到端时延以及网络时延。

B.5.3 丢包率

应明确（由制造商或责任方在随机文件中申明）设备正常运行所要求的最高丢包率。

B.5.4 抖动

应明确（由制造商或责任方在随机文件中申明）设备正常运行所要求的最高抖动。

附录 C

(资料性)

测试工具与环境

C.1 测试环境

采用机器人技术的医用电气设备/系统的产品检测应在满足规定的网络配置要求的最不利网络情况下或通过模拟最不利实验网络进行测试,以确保网络最劣的情况下安全性、有效性满足要求。实验室检测环境应包括功能完备且参数可调的模拟蜂窝通信网、互联网和数据专线组网接入的远程数据通信网络、电波 MIMO-OTA 暗室、电磁屏蔽室、高精度时间同步网络以及多个高度逼真的医疗应用实景测试区,以体现各类组网方式应用中的端到端网络特性,进行全面精细的验证和量化测评,并屏蔽外界电磁干扰、非预期无线信号和随机事件干扰。

每个网络测试区的可调节性能参数包括带宽、时延、抖动、丢包率、误码率等,应能够模拟远程腹腔镜手术机器人在远程距离和环境下所有可能遇到的网络情况,例如:模拟各种外界干扰情况、各种网络性能劣化、各种网络性能受限、跨运营商/跨地域连接等测试场景,检验腹腔镜手术机器人远程状态下的操作性能、音视频通信、网络安全、异常管控等远程应用功能及性能的有效性和安全性。

C.1.1 环境条件

除非制造商另有规定,采用机器人技术的以用电气设备/系统的工作环境条件应满足:

- a) 环境温度: 10℃-30℃。
- b) 相对湿度: 30%-70%。
- c) 大气压力: 700hPa-1060hPa。

C.1.2 电源条件

除非制造商另有规定,采用机器人技术的以用电气设备/系统的电源条件应满足:

- a) 电源电压: 220V-240V AC, 电压波动范围不超过标称值 $\pm 10\%$ 。
- b) 电源频率: 50Hz, 不超过标称值 $\pm 1\text{Hz}$ 。

C.1.3 测试条件

除非制造商另有规定,远程腹腔镜手术机器人的测试条件应满足:

- a) RA 设备按产品说明书要求完成安装和调试。
- b) 试验时应尽量避免外界的振动、噪声、电磁场等物理干扰,光照适当,使之不影响各项试验工作的正常进行。

C.2 测试工具示例

序号	测试设备
1	4G/5G 基站
2	4G/5G 核心网
3	电波 MIMO-OTA 暗室
4	电磁屏蔽间
5	功率放大器
6	专用网络损伤设备
7	专业高增益天线
8	专用测试 SIM 卡
9	专业级音视频测试仪
10	专业级网络测试仪
11	专业级频谱分析仪
12	高速摄像机（须具备网络接口）
13	专业级安全接触力检测设备
14	专业级机械执行机构运行精度检测设备
15	多通道高速数据采集分析设备
16	医疗物联网安全检测工具
17	医疗数据安全检测工具
18	商用密码应用安全检测工具
19	恶意代码防护能力检测工具
20	APP 安全合规检测工具
21	网络流量分析工具
22	位移传感器
23	三维测量系统
24	专业级示波器
25	秒表