ICS 11.120.20
CCS C45

中华人民共和国国家标准

GB/T XXXXX—XXXX

医疗装备操作系统总体技术要求

General technical requirements of the medical equipment operating system

(点击此处添加与国际标准一致性程度的标识)

草案稿

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
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。

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这些专利的责任。

本文件由全国医疗装备产业与应用标准工作组（SAC/SWG26）提出并归口。

本文件起草单位：北京东土科技股份有限公司

本文件主要起草人：

医疗装备操作系统总体技术要求

1 范围

本文规范了医疗装备操作系统的总体技术架构、安全可信技术、运行维护等要求。

本文适用于医疗装备操作系统及其应用的设计、开发与测试，也为终端设备生产商、应用软件开发商提供参考。

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。

3 术语和定义

下列术语和定义适用于本文件。

3.1

医疗装备操作系统 medical equipment operation system

医疗装备操作系统是一个专为医疗环境量身打造和优化的操作系统。它集成了传统操作系统的基本功能，并针对医疗装备的特殊需求进行了深入的增强与调整。

3.2

微内核 microkernel

微内核是一种操作系统设计的架构模式，它将操作系统内核中的基本功能模块化，将大部分操作系统服务作为系统外的可选组件实现，只包括最基本和最核心的功能。

3.3

硬件虚拟化 hardware virtualization

硬件虚拟化是一种资源管理技术，是将计算机的各种实体资源（CPU、内存、磁盘空间、网络适配器等），予以抽象、转换后呈现出来并可供分割、组合为一个或多个电脑配置环境。

3.4

混合关键部署 hybrid critical deployment

混合关键部署是指在一个嵌入式系统或云计算环境中，通过虚拟化、容器化等技术手段，将具有不同关键性等级（如实时控制、网络通信、系统管理等）的操作系统或应用混合部署在同一硬件平台上。

3.5

虚拟机 virtual machine

虚拟机是通过软件模拟的具有完整硬件系统功能的、运行在一个完全隔离环境中的完整计算机系统，每个虚拟机都有独立的CMOS、硬盘和操作系统，可以像使用实体机一样对虚拟机进行操作。

3.6

宿主机 host machine

宿主机是运行虚拟化软件的物理计算机，在虚拟化环境中，宿主机通过虚拟化软件创建并管理虚拟机。

3.7

容器 container

容器是一种沙盒技术，主要目的是为了将应用运行在其中，与外界隔离；及方便这个沙盒可以被转移到其它宿主机器。

4 缩略语

下列缩略语适用于本文件。

AI：人工智能（Artificial Intelligence）

UI：用户界面（User Interface）

API：应用程序编程接口（Application Programming Interface ）

CPU：中央处理器（Central Processing Unit）

POSIX：可移植操作系统接口（Portable Operating System Interface）

TCP/IP：传输控制协议（Transmission Control Protocol）

IPC：进程间通信(Inter-Process Communication)

BSP：板级支持包(Board Support Package)

CRC：循环冗余校验(Cyclic Redundancy Check)

TLS：传输层安全性协议(Transport Layer Security)

SSL：安全套接层协议(Secure Sockets Layer)

MAC：强制访问控制(Mandatory Access Control)

DAC：自主访问控制(Discretionary Access Control)

5 总体技术架构

医疗装备操作系统技术架构见图1所示，整体遵从分层设计，包含：内核层、服务层、应用层、安全可信、集成开发环境。

图1 医疗装备操作系统架构图

5.1 内核层

5.1.1 内核层主要组成与功能

内核层的主要组成与功能如下：

1) 文件系统：提供医疗装备操作系统的核心服务；支持系统的稳定性、安全性和可靠性。
2) 网络协议栈：支持功能的扩展和与其他系统的兼容性；通过设备驱动框架和应用编程接口（API）促进医疗设备的互联互通，赋予设备强大的生态能力。
3) 容器引擎：提供创建和管理容器的功能，可以通过指定容器的镜像和配置参数来创建容器实例。同时，容器引擎还可以监控容器的状态，自动恢复容器故障，并管理容器的生命周期。
4) 虚拟化：推动 AI 在医疗领域的应用，为诊断、治疗和康复提供灵活的解决方案。

5.1.2 内核层技术要求

医疗装备操作系统内核层是该类设备操作系统中的核心部分，负责管理和控制硬件资源、执行基本的系统功能，同时还为服务层提供必要的服务和接口实现。

5.1.2.1 微内核

微内核是操作系统内核功能的精简版本，提供最基本的功能，具体要求如下：

1) 应支持中断与异常管理，可处理硬件产生的中断和软件异常，确保系统能够及时响应和处理外部事件和错误条件。
2) 应支持进程线程管理，管理和调度系统中的进程和线程，确保多任务运行和合理资源分配。
3) 应支持不同进程之间的通信和数据共享，如：消息传递、共享内存等机制。
4) 应支持内存管理，包括内存分配、释放和保护等，确保程序能够正常运行并避免内存泄漏或冲突。
5) 应提供定时器与时钟管理功能，支持实时任务的调度和执行，管理系统的时间和定时任务，确保各种操作在预定的时间间隔内执行。
6) 应支持可定制性和模块化设计，便于医疗装备设备厂商定制和扩展的同时，不影响内核的稳定性和功能。

5.1.2.2 内核组件

内核组件为内核层提供了基础的管理和服务功能，具体要求如下：

1) 应支持文件系统，支持文件的创建、读写、删除和管理，并确保数据的安全性和完整性。
2) 应支持网络协议栈，如：TCP/IP 协议，使设备能够与其他设备或系统进行数据交换和通信。
3) 应提供诊断和调试工具，帮助开发人员追踪和解决系统运行中的问题和异常情况。
4) 应提供用户与操作系统交互的命令行界面，允许用户执行系统命令、管理文件和配置系统参数。
5) 宜支持容器化技术，应用程序在隔离的运行环境中执行，增强系统的安全性、灵活性和可维护性。
6) 宜集成 AI 算法库和框架，如：TensorFlow、PyTorch 等，用于开发和部署医学图像识别、病例预测等 AI 应用。
7) 宜提供图形处理的相关接口和库，支持医疗影像的实时显示和处理。

8） 宜支持数据库和数据传输，支持从医疗传感器和设备收集、存储和处理大量实时数据。

5.1.2.3 设备驱动框架

设备驱动框架主要用于管理和控制医疗装备中的硬件设备，并为上层应用和服务提供统一的设备访问接口，并对系统资源的管控和硬件设备的接口与协议定义。具体要求如下：

1） 应支持设备驱动接口的标准化定义。
2） 应支持设备初始化，包括硬件初始化、资源分配、中断初始化等。
3） 应提供设备配置接口，允许用户或系统管理员通过软件方式配置设备的参数和属性。
4） 应提供中断处理机制。
5） 应提供错误检测和报告机制。
6） 应支持兼容多种操作系统和平台环境，支持不同型号和品牌的硬件设备接入。

5.1.2.4 虚拟化

虚拟化支持多个虚拟机在同一台物理计算机上运行不同的操作系统和应用程序，并通过软硬件结合的方式避免不同虚拟机之间的干扰，具体要求如下：

1） 应支持在单一硬件平台上同时运行多个不同操作系统的能力。
2） 应支持多种操作系统和硬件配置，包括 CPU、内存、存储和网络等资源的分配和调整。
3） 应支持不同操作系统的虚拟机共享计算、存储和网络资源。
4） 应支持根据需求动态调整和分配虚拟机的计算资源，适应不同业务需求。
5） 应支持为不同的虚拟机配置不同的资源和优先级。
6） 应支持通过调度算法平衡资源分配，确保每个任务获得适当的 CPU 时间片。
7） 应支持根据优先级确保高优先级任务优先获得 CPU 时间。
8） 应支持虚拟机的创建、管理、删除和部署。
9） 应支持虚拟机之间能够安全地交换数据。
10） 设计和实施虚拟化技术，宜遵循医疗设备标准和相关的功能安全标准要求。

5.1.2.5 应用编程接口

为方便上层医疗服务组件及应用进行跨内核移植，操作系统应提供统一的应用编程接口，如POSIX接口，应支持以下接口：

1） 任务管理编程接口。
2） 任务同步与通信编程接口。
3） 进程管理编程接口。
4） 线程和同步编程接口。
5） 目录管理编程接口。
6） 信号处理编程接口。
7） 中断/异常管理编程接口。
8） 时钟/定时器管理编程接口。
9） 内存管理编程接口。
10） 文件系统编程接口。
11） 设备管理编程接口。
12） Shell 和工具编程接口。

13）系统服务编程接口。
14）用户界面编程接口。
15）网络通信编程接口。

5.2 服务层

5.2.1 服务层主要组成与功能

服务层的主要组成与功能如下：

1） 医疗协议：用于规范医疗设备之间通信和数据交换的协议。在服务层中，医疗协议的功能是定义设备之间的通信规则、数据格式和传输方式，以确保医疗设备之间能够正确、可靠地进行数据交换和协同工作。
2） 医疗影像处理：指对医学影像数据进行处理和分析的过程。在服务层中，医疗影像处理的功能包括图像重建、图像增强、分割和特征提取等技术，以提高医学影像的质量、准确性和可视化效果，并支持医疗诊断和治疗的决策。
3） 医疗数据采集：指收集和记录与患者健康相关的数据的过程。在服务层中，医疗数据采集的功能是通过传感器、监测设备或其他数据源，采集患者的生理参数、病历信息、实时监测数据等，并将其存储、处理和传输至其他系统或平台，以支持医疗监护、健康管理和医学研究等应用。
4） 逻辑控制：指根据特定的逻辑规则和算法对医疗设备进行控制和管理的过程。在服务层中，逻辑控制的功能是根据医疗设备的状态、输入数据以及预设的规则，进行实时的决策和控制，以确保医疗设备的正常运行、安全性和有效性。

5.2.2 服务层技术要求

医疗装备操作系统服务层是为医疗设备提供核心功能支持的软件层级，其中分布式通信技术，支持设备内外部系统的实时数据交换和远程管理，同时整合了多种医疗专用组件，用于实现特定的医疗功能和应用需求。

5.2.2.1 分布式确定性通信

分布式确定性通信主要实现服务间高效、可靠且确定性的通信，确保不同服务或组件之间能够按照预定的时间约束和通信协议，进行数据的实时传输和交互。具体要求如下：

1） 宜提供确定性调度组件，可结合内核调度机制，满足业务运行时间确定性要求。
2） 宜提供可配置的分布式确定性调度工具，可规划各个业务执行时序和确定性通信设置。
3） 宜提供分布式消息通讯机制，为各个业务应用间提供发布、订阅消息机制。

5.2.2.2 医疗协议

为方便医疗装备的上下游进行数据对接，医疗装备操作系统需要适配医疗行业协议：

1） 应支持与影像设备进行图像传输的专有医疗 DICOM 协议；
2） 应支持与医院信息系统（HIS、EMR、LIS、PACS）、临床实验系统、企业系统和药房系统进行数据传输的 HL7 协议。

5.2.2.3 医疗影像处理

操作系统为医疗影像应用的高效运行提供支撑，相应能力如下：

1) 应具备高速数据处理能力，支持高速的影像数据读取、处理和传输，确保影像数据的实时性和流畅性。
2) 应支持并行图像处理功能，具备多核或多处理器并行处理能力，能够同时处理多个影像任务。
3) 应支持不同类型装备影像数据的处理能力，如 X 射线、CT 影像、深度数据等。

5.2.2.4 数据采集

医疗装备操作系统需要支持医疗数据采集功能，以确保医疗服务的高效、准确和安全。

1) 应支持医疗设备的数据采集功能，对手术末端、光学定位仪、外围设备进行实时准确的数据采集。
2) 应支持数据加密，对敏感数据采集后进行加密传输，确保数据保密和完整性。

5.2.2.5 运动控制

运动控制用于装备动作的精准控制，以确保装备能够按照预定的轨迹、速度和精度执行动作。提供功能如下：

1) 应支持速度控制、精确位置控制、力控能力，满足基本的运动轨迹规划功能；
2) 应支持运动控制的安全功能，支持碰撞检测、避障、安全墙、机械臂紧急制动、安全配置、故障诊断，保障医疗场景下的控制安全性；
3) 应支持运动控制二次开发接口，满足自定义运动控制、轨迹规划、重力补偿、拖动示教等功能。
4) 宜提供高级轨迹规划功能，满足高精度和复杂运动的需求，提升运动控制性能。

5.2.2.6 逻辑控制

逻辑控制指根据预设的逻辑规则和算法，对医疗装备的各个部件、系统或过程进行控制和协调，提供功能如下：

1) 应支持基本的逻辑运算，满足医疗装备的精准控制；
2) 应支持复杂逻辑表达式的解析和执行，以满足复杂控制需求；
3) 宜提供事件驱动逻辑控制能力，以响应外部和内部的触发事件；

5.3 应用层

5.3.1 应用层主要组成与功能

应用层的主要组成与功能如下：

1) 患者管理：涉及记录和管理患者的医疗信息和个人资料。它包括创建患者档案、维护患者病历、管理治疗计划、跟踪患者进展和预约等。患者管理功能有助于医疗机构有效地管理患者流程和提供个性化的医疗服务。
2) 视频管理：涉及医疗设备中的视频监控和视频会议。它可以用于远程会诊、远程观察手术、培训和教育等场景。视频管理功能可以集成摄像头、视频录制和回放功能，帮助医生和医护人员进行实时的视频交流和远程协作。
3) 手术规划：涉及对手术过程进行规划和优化。它可以利用医学影像数据、手术模拟和虚拟现实技术，帮助医生制定手术方案、选择最佳的手术路径和手术器械，以提高手术的准确性和安全性。

4) 会议管理：涉及医疗设备中的会议组织和协作。它可以用于组织医学会议、学术讲座、病例讨论等活动。会议管理功能可以提供会议日程安排、参会人员管理、会议记录和讨论、远程参会等功能，促进医生和专家之间的交流和知识共享。
5) 设备管理：涉及医疗设备的监控、维护和管理。它包括设备状态监测、故障诊断、维护计划制定、设备报废和更换等。设备管理功能可以帮助医疗机构及时了解设备的运行状况，提高设备的可靠性和利用率，以保证医疗服务的连续性和质量。

5.3.2 应用层技术要求

为确保医疗设备能够高效、稳定地运行，在特定硬件条件下，操作系统性能应满足如下要求：

1) 任务切换时间应不大于 5μs。
2) 中断延迟时间应不大于 5μs。
3) 周期任务抖动时间应不大于 10μs。

6 安全可信技术要求

医疗装备操作系统的安全可信确保患者隐私安全、保障医疗服务连续性、提高系统可靠性和降低医疗事故风险。通过强化安全防护和认证机制，为医疗装备提供稳固的运行环境，确保医疗服务的高效与安全。

6.1 安全执行环境

在操作系统中实施的一系列技术和策略，旨在保护系统免受未经授权的访问、数据泄露、恶意软件以及其他安全威胁的影响。具体要求如下：

1) 宜支持用户身份验证、访问控制。
2) 宜支持数据加密。
3) 宜支持安全启动。
4) 宜支持安全更新和漏洞管理。

6.2 系统安全要求

通过设计、实施和维护各种技术和策略，以保护操作系统及其相关资源不受未经授权的访问、破坏或泄露。具体要求如下：

1) 应提供掉电安全文件系统保护机制，在任何异常掉电情况下，保证文件系统完整无损。
2) 宜提供安全容器功能，提供内存巡检、处理器巡检、任务监控、数据流监控等功能模块。
3) 宜提供安全配置管理，关闭不必要的服务和功能，减少攻击面。

6.3 网络安全要求

确保操作系统及其上运行的应用程序在网络环境中安全运行。具体要求如下：

1) 宜支持权限管理和访问控制机制，包括提供安全访问控制以及身份鉴别功能。
2) 宜支持嵌入式防火墙功能。
3) 宜支持 VPN 虚拟隧道功能。
4) 宜支持不同主体为完成各自承担任务所需的最小权限。
5) 宜禁止使用 root 账户（或等同）权限运行。

6） 宜支持强制访问控制（MAC）和自主访问控制（DAC）。

6.4 数据安全要求

通过操作系统的安全措施和技术手段，确保计算机系统中的数据不被未经授权的访问、修改、泄露或破坏。具体要求如下：

1） 宜支持 TLS/SSL 等协议加密数据。

2） 宜支持对存储在磁盘上的敏感数据进行加密。

7 运行维护

运维要求如下:

1） 应提供详细的用户手册和技术文档。

2） 应记录系统运行日志。

3） 应支持自动化安装部署、升级及补丁工具。

4） 应实现系统健康检测自动化

5） 应提供故障信息采集工具