|  |  |
| --- | --- |
| ICS  | 35．020 |
| CCS  | L 00      |

|  |
| --- |
|  3202 |

无锡市地方标准

DB 3202/T XXXX—XXXX

物联网 大型医用设备健康监测系统通用技术要求

Internet of Things General technical requirements for health monitoring system of large medical equipments

XXXX - XX - XX发布

XXXX - XX - XX实施

无锡市场监督管理局  发布

目次

前言 II

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 缩略语 2

5 系统结构 2

5.1 概述 2

5.2 健康监测系统 2

5.3 系统接口 3

6 监测管理平台 3

6.1 设备信息管理 4

6.2 安全事件管理 4

6.3 工作环境管理 4

6.4 运行状态监测 4

6.5 维护维修管理 4

6.6 质量控制 5

6.7 操作人员管理 5

6.8 健康评估 5

7 物联网网关 5

8 大型医用设备感知终端 5

9 系统安全要求 6

9.1 网络安全 6

9.2 数据传输安全 6

9.3 数据安全 6

参考文献 7

1. 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。

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这些专利的责任。

本文件由无锡市卫生健康委员会提出并归口。

本文件起草单位：江南大学附属医院、江苏省人民医院、新亿成科技（江苏）有限公司、无锡市卫生健康统计信息中心、无锡物联网产业研究院、苏北人民医院、深圳市大数据研究院无锡创新中心、江南大学、北京大学深圳医院、宜兴市中医医院、赛诺联合医疗科技（北京）有限公司、无锡市第五人民医院、北京朋创天地科技有限公司、无锡市第二人民医院、凯思轩达医疗科技无锡有限公司。

本文件主要起草人：刘丽、高宇峰、钱英、刘星宇、顾志成、钱维林、仲辉、花磊、何利文、方伟、钱鹏江、周军华、陈书义、鲍颖芳、李鑫、李开良、成鹰、羊月祺、王涛、成晨、周小虎、郭煜、徐荣、高靖颖、杨小娟、荣健。

物联网 大型医用设备健康监测系统通用技术要求

* 1. 范围

本文件给出了物联网大型医用设备健康监测系统的系统结构、监测管理平台、物联网网关、大型医用设备感知终端和系统安全要求。

本文件适用于大型医用设备健康监测系统的设计、开发、验收评估和应用管理。

* 1. 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/T 22239-2019 信息安全技术 网络安全等级保护基本要求

GB/T 33745-2017 物联网 术语

GB/T 35273—2020 信息安全技术 个人信息安全规范

GB/T 37025-2018 信息安全技术 物联网数据传输安全技术要求

GB/T 38624.1-2020 物联网 网关 第一部分：面向感知设备接入的网关技术要求

GB/T 38636—2020 信息安全技术 传输层密码协议（TLCP）

GB/T 39725-2020 信息安全技术 健康医疗数据安全指南

GB/T 41479-2022 信息安全技术 网络数据处理安全要求

WS/T 654-2019 医疗器械安全管理

DB32/T 4435-2022 物联网 大型医用设备使用监督管理平台通用技术要求

* 1. 术语和定义

GB/T 33745-2017、GB/T 22239-2019、GB/T 38624.1-2020和DB32/T 4435-2022界定的以及下列术语和定义适用于本文件。

大型医用设备large medical equipment

纳入国家卫生健康委员会发布的《大型医用设备配置许可管理目录》内的医用设备。

[来源：DB32/T 4435-2022，3.2]

大型医用设备健康监测系统 large medical equipment health monitoring system

对大型医用设备的工作环境、运行状态、维护维修、质量控制、操作人员等维度的实时状况进行监测及评估的软硬件集合。

物联网网关 internet of things gateway

具有数据存储能力、计算能力和协议转换能力等特征，可通过北向接口与应用平台建立通信连接和通过南向接口与感知设备进行通信的实体。

1. 实体可以是独立设备或软件。

[来源：GB/T 38624.1-2020，3.1]

大型医用设备感知终端 large medical equipment sensing terminal

一种具有唯一标识，能够采集、预处理并传输大型医用设备相关数据，及工作环境等信息的硬件设备，并提供接入网络的能力。

* 1. 缩略语

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

HTTP：超文本传输协议（HyperText Transfer Protocol）

* 1. 系统结构
		1. 概述

大型医用设备健康监测系统包括监测管理移动终端大型医用设备感知终端、监测管理平台、物联网网关及其接口等部分，核心要素包括对工作环境、运行状态、维护维修、质量控制、操作人员等维度的健康评估。

本文件提出对设备健康监测的功能要求、安全要求以及对接口的通用技术要求。

* + 1. 健康监测系统

健康监测系统包括监测管理终端、监测管理平台、物联网网关、大型医用设备感知终端、接口等组成部分，系统结构如图1，系统各组成部分描述如下：

1. 监测管理终端，医疗机构人员对大型医用设备的健康信息进行查询、录入和更改的终端，如移动通信终端、一体机、手持终端。
2. 监测管理平台，对大型医用设备的数据进行安全管理及评估，其功能主要包括设备信息、安全事件、工作环境、运行状态、维护维修、质量控制、操作人员、健康评估，这些功能是实现大型医用设备的数据采集、显示、提醒、评估的基本功能。
3. 物联网网关，是监测管理平台与大型医用设备的数据交换和消息传输通道。医疗机构应根据大型医用设备的分布情况安装多个物联网网关，每个物联网网关可以管理多台医用设备，通过物联网网关实现对设备健康监测系统的部署。
4. 大型医用设备感知终端，采集大型医用设备健康信息的装置。
5. 接口，设备健康监测系统各构件间的接口，如A01、A02和A03接口。

 

1. 大型医用设备健康监测系统结构
	* 1. 系统接口

系统接口表示实体之间存在的逻辑关联和通信链路，这些接口与对应实体的对照关系见表1。

1. A01接口，为物联网网关与大型医用设备感知终端的传输接口。
2. A02接口，为物联网网关与监测管理平台的访问接口，应支持物联网网关通过广域网或局域网接入设备健康监测系统，通过授权访问机制，对非授权用户/设备不提供访问服务。
3. A03接口，为监测管理平台与监测管理终端的接口，医疗机构医学工程专业人员、经授权的设备厂商运维人员等可通过该接口对设备健康信息进行管理，或通过该接口实现指令执行和信息反馈。
4. 接口编号与对应实体对照关系

|  |  |
| --- | --- |
| 接口编号 | 对应实体 |
| A01 | 大型医用设备感知终端 | 物联网网关 |
| A02 | 物联网网关 | 监测管理平台 |
| A03 | 监测管理平台 | 监测管理终端 |

* 1. 监测管理平台
		1. 设备信息管理

具有设备所属医疗机构、配置许可、设备验收、资产信息等信息的管理功能，包括但不限于：

1. 按需实现显示设备信息内容。
2. 按需进行设备信息更新。
3. 按需显示大型医用设备的使用情况。
4. 系统按许可证装机时间自动计算显示设备的使用年限。
	* 1. 安全事件管理

全面管理和响应与安全相关的事件，确保事件的感知、处理和改进。包括但不限于如下内容：

1. 应具备及时感知和识别与安全相关的事件的能力。事件识别应基于事先设定的安全规则和阈值，通过监测设备状态、异常数据、告警信息等进行准确的事件识别。
2. 应自动或手动生成事件报告，其中包括事件的类型、位置、时间、严重程度等关键信息。事件报告应提供清晰的描述和必要的上下文，便于后续的处理和分析。
3. 应建立完善的处置记录系统，记录事件不同类型的通知方式、事件详细信息、事件处理过程和结果，以及相关人员的行动和措施。处置记录应包括事件的起始状态、处理过程的详细步骤、所采取的措施和对事件的影响评估等信息。
4. 应能跟踪事件的状态和进展，确保处理步骤的完成和准确记录，包括但不限于文本记录方式和录屏记录方式。
5. 应能进行事件评估，对事件的原因、影响和处理效果进行综合评估。评估结果应包括对事件处理的有效性、改进措施的可行性和相关风险的分析。
	* 1. 工作环境管理

监测管理平台对设备所需的正常工作环境要求进行统一管理，包括但不限于如下内容：

1. 工作环境指标管理，应根据不同类别、不同型号、不同厂家对设备环境的具体要求，生成具体的工作环境指标，如温度、湿度、电压、电流等。
2. 应对不符合设备要求的异常环境进行监测和告警。
	* 1. 运行状态监测

采用统一的采集方式对不同类型的设备进行主机工作状态及运行数据的统计、分析及展示，包括但不限于以下内容：

1. 应记录和监测设备的主机工作状态，如设备主机的硬盘空间使用率、日常质控结果等指标。
2. 应记录和统计设备的工作年限，便于对设备的使用寿命和维护计划进行评估和管理。
3. 应统计设备的每天的开关机时间和工作时长，包括累计工作时长和单次工作时长，便于评估设备的使用频率和运行状况。
4. 应记录和统计设备的检查人次。
5. 应记录设备的工作模式数据，不涉及个人信息，包括但不限于检查部位、检查序列。
6. 应提供工作量负荷预警功能，包括对工作量异常的提醒和对同台设备的月度差异、同类设备的差异化提醒，便于医疗机构对设备的运行情况进行及时分析和调整。
	* 1. 维护维修管理

可记录或查询日常维护性检验、检查、校准时应记录的事项与内容要求，包括但不限于定期检查、检验、校准、保养、维护、故障类别、故障持续时间、故障发生频率、配件更换数量和价格、维护保养时限提醒等。

* + 1. 质量控制

监测管理平台可对设备质量进行管理及控制，应符合DB32/T 4435-2022中5.8的要求。

* + 1. 操作人员管理

监测管理平台对操作人员资质及培训的管理，操作人员包括操作技师及医学工程人员。包括但不限于以下内容：

1. 操作人员的技术档案管理，技术档案应包括其学历、培训经历、资历、职务和技术职称等方面的内容。
2. 操作人员数量的动态管理。
3. 操作人员的工作年限管理。
4. 操作人员技能培训管理。
	* 1. 健康评估

监测管理平台对大型医用设备进行健康评估管理，包括但不限于以下内容：

1. 应对大型医用设备各健康维度进行分值计算，健康维度包括安全事件、工作环境、运行状态、维护维修、质量控制、操作人员，提供设备健康状态评估值。
2. 应对各类型各品牌的设备进行健康评估。
3. 医疗机构应每年进行至少一次大型医用设备的健康评估，并依据设备健康评估结果对医用设备进行风险等级评定，并进行相应风险等级管理。
4. 应对大型医用设备进行绩效评估，可分类型、品牌等进行统计。
	1. 物联网网关

物联网网关负责连接不同的感知设备和系统，并实现数据的传输和通信，包括但不限于以下功能：

1. 连接性管理，具备与不同感知设备和系统连接的能力，支持多种通信协议和接口。通信协议包括但不限于MQTT、HTTP等，接口包括物理接口、数据接口等。
2. 安全性管理，物联网网关自身应支持通过认证，数据加密和访问控制等措施来防止未经授权的访问和恶意攻击，并实现对大型医用设备的安全状态监测。
3. 通信与控制管理，应支持对所连接大型医用设备感知终端的集中管理和监控功能，包括运行状态的查询、固件版本的查询和远程升级等。
4. 数据聚合与处理，应收集从感知终端中传输的数据，并进行聚合和处理，并对数据进行过滤和分析，以提取有用的信息，并将其传送到平台进行进一步的处理和存储。
	1. 大型医用设备感知终端

大型医用设备感知终端是设备健康监测管理中的关键组件，能够识别设备、采集设备数据，并将数据进行预处理和传输，实现大型医用设备的实时健康监测。

1. 应具有可被感知识别的唯一标识，该标识可与相应的大型医用设备绑定，用于设备识别、数据关联的管理。
2. 应具有采集医用设备运行和工作环境数据的功能，包括但不限于设备工作电流信号、环境温湿度。
3. 应支持采集数据的预处理、数据传输等功能。
4. 应支持对其连接的物联网网关进行身份标识和鉴别的能力，确保大型医用设备的实时健康监测数据只被可信网关获取。
	1. 系统安全要求
		1. 网络安全

网络安全保护能力级别应符合GB/T 22239-2019中5.2的划分依据，安全通用要求符合对应等级下的安全通信网络、安全区域边界、安全计算环境、安全管理等有关规定，系统应符合对应等级下的物联网安全扩展要求。此外，需要对大型医用设备的电子接口进行注册管理，包括但不限于可记录、查询设备网络接口及电子数据交换机接口的类型、方式、技术特性等内容，并可监测其接口的工作状态。

* + 1. 数据传输安全

物联网网关与设备健康监测系统之间应支持TLS/SSL协议，设备健康监测系统传输数据全过程应加密保护，防止数据在传输过程中遭遇恶意窃取、非法篡改，保证链路安全，TLS/SSL协议应符合GB/T 38636-2020的要求。

* + 1. 数据安全

应对设备在运行过程中产生和收集的数据提供安全保护，其保护能力应满足GB/T 41479-2022 《信息安全技术 网络数据处理安全要求》和GB/T 35273—2020《信息安全技术 个人信息安全规范》等标准中的相关要求。同时系统还应支持以下但不限于以下数据安全保护能力：

1. 防数据泄露：应禁止从设备上拷贝数据到未授权的U盘等存储介质。应识别设备的未授权网络连接并生成安全事件告警信息，并对未授权网络连接进行记录，包括但不限于与未授权连接相关的源地址、源端口、目的地址、目的端口、协议类型、起始和终止时间、流量大小等。
2. 防数据篡改：应对设备的运维工具等软件程序进行安全性检测，防范勒索软件和病毒木马等恶意代码对数据的破坏。
3. 防数据滥用：应支持对违规和异常访问设备的行为进行识别、记录、告警和拦截。
4. 防数据毁损：应对重要数据采用多种数据备份机制，防止单一数据备份机制失效带来的数据毁损。

参考文献

[1] 关于发布大型医用设备配置许可管理目录（2018年）的通知（国卫规划发[2018]5号）

[2] 关于发布大型医用设备配置与使用管理办法（2018年）的通知 (国卫规划发[2018]12号)

[3] 医疗器械监督管理条例 中国人民共和国国务院令 第739号

[4] 医疗器械网络安全注册审查指导原则（2022年修订版）

[5] WS/T 654-2019 医疗器械安全管理 第四部分：风险管理

[6] 中华人民共和国数据安全法（2021年）