附件 8

HJ

中华人民共和国国家生态环境标准

HJ □□□□-202□

固定污染源现场监测设备防范篡改伪造功能通用要求

General requirements for anti-tampering and anti-falsification functions of on-site monitoring equipment for stationary pollution sources

（征求意见稿）

202□-□□-□□发布　　202□-□□-□□实施

生　态　环　境　部　发布

目　　次

前　　言 ii
1 适用范围 1
2 规范性引用文件 1
3 术语和定义 1
4 软件要求 3
5 硬件要求 5
6 禁止功能 6
7 监测设备防范篡改、伪造功能检查 7
附录 A （规范性附录） 固定污染源现场监测设备日志记录内容 9
附录 B （资料性附录） 固定污染源现场监测设备软件功能检查推荐方法 10

前　言

为贯彻《中华人民共和国生态环境法典》和《生态环境监测条例》，防治生态环境污染，改善生态环境质量，规范固定污染源现场监测设备防范篡改、伪造功能要求，制定本标准。

本标准规定了固定污染源现场监测设备防范篡改、伪造功能通用要求。本标准实施之日前已在用的固定污染源现场监测设备，自本标准实施之日起不应具有本标准所列禁止功能，并于XXXX年XX月XX日前达到本标准要求；本标准实施之日起新生产的监测设备应符合本标准要求。

本标准的附录 A 为规范性附录；附录 B 为资料性附录。

本标准为首次发布。

本标准由生态环境部生态环境监测司、法规与标准司组织制订。

本标准主要起草单位：中国环境监测总站、生态环境部环境工程评估中心。

本标准生态环境部 202□年□□月□□日批准。

本标准自 202□年□□月□□日起实施。

本标准由生态环境部解释。

固定污染源现场监测设备防范篡改伪造功能通用要求

1 适用范围

本标准规定了固定污染源现场监测设备防范篡改、伪造功能的通用技术要求。

本标准适用于具备可编程软件程序，在固定污染源现场实现样品采集、分析测试、数据计算或传输等功能的监测设备。

特定类型固定污染源现场监测设备有专项技术标准的，按相应标准执行；无专项标准或专项标准未作规定的，执行本标准。涉及数据安全管理的，按国家有关法律法规及标准规范要求执行。

2 规范性引用文件

本标准引用了下列文件或其中的条款。凡是注明日期的引用文件，仅注日期的版本适用于本标准。凡是未注日期的引用文件，其最新版本（包括所有的修改单）适用于本标准。

GB/T 7408.1 日期和时间 信息交换表示法 第1部分：基本原则

HJ 212 污染物自动监测监控系统数据传输技术要求

HJ XX 固定污染源便携式监测设备数据传输技术要求

JJF 1182 计量器具软件测评指南

JJF 2356 计量器具软件标识通用要求

3 术语和定义

下列术语和定义适用于本标准。

3.1

固定污染源现场监测设备 on-site monitoring equipment for stationary pollution sources

安装或携带至固定污染源现场能够实现样品采集、测试、数据计算或数据传输的监测设备，简称现场监测设备。

3.2

P型监测设备 build-for-purpose monitoring equipment

以微控制器/单片机（MCU）为核心，运行实时操作系统（RTOS）或裸机程序，针对特定测量任务进行软硬件一体固化设计的监测设备，统称P型监测设备。

3.3

U型监测设备 universal monitoring equipment

以应用处理器（MPU）为硬件核心、运行通用操作系统，通过软件配置实现不同监测任务的监测设备，统称U型监测设备。

注：U 型监测设备可能会存在以微控制器/单片机（MCU）为核心，运行实时操作系统（RTOS）或裸机程序的功能模块，该部分应参照 P 型监测设备的相关要求进行管理。

3.4

监测软件 monitoring software

监测设备中实现污染物监测、计算、数据采集与传输、日志记录等直接影响监测结果真实性、准确性和完整性的软件模块，包括固件。

注：不包括操作系统。

3.5

软件标识 software identification

可代表监测设备软件或软件模块的可读字符串。

3.6

固件 firmware

硬件设备或驻留在此设备上的作为只读软件的计算机指令和数据的组合。

3.7

保护性接口 protective interface

对流向监测软件的所有数据进行安全保护的软件接口，其通过硬件或软件方式实现数据的访问控制、过滤或校验，防止未授权或异常数据进入监测设备。

3.8

完整性校验 integrity check

通过循环冗余校验（CRC）、哈希算法等计算数据校验值并与参考值比对，以确认数据是否完整、未被篡改的过程。

3.9

数字签名 digital signature

利用密码学方法在软件或数据上附加的，用于确认其来源真实性、完整性的数据。

3.10

时间戳 time stamp

用来表示某次测量或某个事件发生时间的唯一字符串，格式符合 GB/T 7408.1 要求。

3.11

日志记录 logging

包含时间戳、事件信息记录的连续数据文件，用于记录可能影响监测数据真实性、准确性和可追溯性的操作和事件。

3.12

封缄 sealing

对监测设备相应组件或部位所做的特别保护，以防止对监测设备硬件或软件实施调整、修改或更换等未经授权的操作。

3.13

软件保护 software protection

为防止未经授权的修改或更换，对监测设备中与监测数据真实性、准确性直接相关的软件模块、参数、计算公式及数据存储区域所采取的封缄保护措施，包括硬件封缄和软件封缄。

3.14

软件检查 software examination

根据特定流程查验软件特性的技术操作，如技术文档分析或在受控条件下的程序运行。

4 软件要求

4.1 软件标识

4.1.1 监测软件应具有符合 JJF 2356 要求的软件标识，其组成包括：监测设备类型（P 型或 U 型）、监测设备分类编码、软件版本、发行日期、完整性校验值等。完整性校验值由设备内置校验程序对监测软件程序文件逐字节计算生成，可采用 CRC 校验或哈希算法。如选择 CRC 校验算法，P 型监测设备宜采用 CRC16 校验方法进行校验，U 型监测设备宜采用 CRC32 校验方法进行校验。

4.1.2 设备每次启动过程中，应能在屏幕显著位置自动显示软件标识；设备运行过程中，应能通过软件菜单查看软件标识。无显示屏的设备，应具备通过通信接口传输到其他组件显示或打印的功能。

4.1.3 监测软件的安装、升级应执行加载、完整性校验、来源真实性校验和安装流程。监测软件程序文件应由内置的引导加载程序执行，不　　应绕过引导加载程序直接写入，并通过引导加载程序进行完整性校验（CRC 或哈希算法）和来源真实性校验（数字签名），两项校验均通过方可执行安装。

4.1.4 监测软件升级等引起软件内容变化时，应生成新的软件标识。监测软件升级不应造成数据及配置参数丢失或损坏。

4.1.5 设备生产制造商应声明软件标识的设计方式与计算方法，并提供进行外部验证的方法及相应接口，确保监测软件程序文件、校验值可导出可验证，导出通道应实施访问控制，确保仅授权人员在受控条件下使用。

4.2 参数与计算公式

4.2.1 应对设备参数实施分类管理，对关键参数实施防范篡改保护：

a）A 类参数为不可修改参数。A 类参数应封装为独立二进制模块，存放于只读存储区，通过保护性接口调用，调用时进行 CRC 或哈希算法完整性校验，校验不通过拒绝执行相关计算。包括定量分析模型的固定常数（如朗伯-比尔定律中的摩尔吸光系数）、固定计算常量（如标准大气压）、固定采样测试参数（如进样体积）、数据换算固定系数（如摩尔-质量转换系数）等。

b）B 类参数为配置参数。B 类参数由设备第二类权限角色根据现场情况配置，参数配置修改应生成日志记录。包括监测点位信息（如烟道截面积）、参比方法校准系数（如速度场系数）、测试条件参数（如消解温度）、浓度计算常量参数（如基准含氧量）等。

c）C 类参数为自动生成参数。C 类参数应由设备在受控的测量、校准调整、运行自检过程中自动生成，不应具备人工输入、修改功能。包括设备运行状态参数（如光源强度）、测量信号值（如电压、电流、吸光度等）、校准系数（如校准斜率、截距）等。测量信号值应与监测数据同步记录，性能参数、校准系数应设置阈值范围，接近阈值或超出阈值时应采取响应措施。其中，校准系数超出阈值时不应允许校准系数调整。

4.2.2　所有参与监测数据计算的公式应在设备出厂时固化，封装为独立二进制模块，存放于只读存储区，通过保护性接口调用，调用时进行 CRC 或哈希算法完整性校验，校验不通过的，设备应拒绝执行相关计算并记录异常事件日志。

4.2.3　设备应能显示其实际使用的关键参数、计算公式、变量含义、变量单位及适用条件，且与设备说明书中列明的内容保持一致。

4.3　日志管理

4.3.1　监测设备应对设备运行状态、设备操作等重要信息形成日志记录。设备运行状态发生变化或任一权限角色执行操作时，均应自动生成相应日志。不应具有用于选择日志记录范围、记录频次或选择性忽略特定事件的功能。日志记录应支持按类型查询和导出。

4.3.2　日志记录类型及记录内容见附录 A。

4.4　监测数据及日志记录存储保护

4.4.1　监测数据及日志记录仅允许由监测软件产生。

4.4.2　自动监测设备应按照 HJ 212 要求进行授时；便携式监测设备应通过北斗卫星或网络进行授时定位。监测数据及日志记录的时间戳应从设备内部硬件时钟读取，任何对监测设备时钟的修改操作均应生成不可删除的日志记录。

4.4.3　监测数据及日志记录存储应采用先入先出策略，仅允许按预设规则自动覆盖最早数据、日志。监测数据与日志记录应分区独立存储。现场监测设备中的监测数据和日志记录保存期限不少于 2 年。

4.4.4　未与生态环境部门监管平台联网传输的本地存储数据与日志记录应加密存储，宜采用国密 SM4 算法加密。

4.5　软件运行环境

监测设备运行的操作系统应具备基本安全防护能力，防范未经授权的访问、修改或配置变更。具体要求如下：

a）监测设备操作系统应遵循最小化安装原则，仅安装运行监测软件所必需的操作系统内核、系统服务、驱动及组件。对于支持组件化定制的操作系统（如嵌入式 Linux 等），应进行裁剪，移除不必要的功能模块；对于无法进行组件裁剪的操作系统，应禁用非必要的系统服务及账户；

b）设备启动后应直接进入监测软件界面，不应通过组合键、手势或后台进程等方式切换至操作系统桌面环境或获取操作系统操作权限；

c）操作系统及监测软件应禁用具有远程操作功能的组件、服务，禁止安装远程控制软

件。监测软件中确有必要保留的设备远程维护功能，应仅在受控条件下启用，且在日志中记录；

d）操作系统应启用系统日志记录功能，并对以下事件进行完整记录：端口开启与关闭、外部设备接入、远程登录及访问、用户登录与登出、系统服务启停等。

4.6 异常响应要求

4.6.1 监测设备应具备功能、性能、操作异常检测与响应能力，能够自动识别异常情况，根据异常情况对监测数据及设备安全性的影响程度，执行分级响应，生成异常响应处置日志：

a）一级异常（如定位授时失败、设备性能参数临近阈值、通信中断等）应发出声、光或界面报警提示；

b）二级异常（如校准系数超出阈值、设备性能参数超出阈值等）应报警并对生成的数据按规则进行标记；

c）三级异常（如监测数据和日志记录被手动删改、计算公式和关键参数调用校验失败等）应报警并限制或停止对设备的操作。

4.6.2 异常响应应遵循由低到高的升级原则，同一异常事件满足多个响应条件时，应执行最高级响应。

4.6.3 异常检测与响应逻辑应封装为独立模块，固化于固件或受保护存储区，未经授权不应修改、停用或绕过。

4.7 软件操作权限

4.7.1 应用软件操作权限应实施分类管理，应设置三类权限，各类权限对应的全部功能均应在操作菜单下显示，未授权功能项应处于不可操作状态。

4.7.2 第一类权限角色为设备生产者、销售者，不应授权或转交他人使用。第一类权限角色具有设备所有功能的访问和操作权限，应采用数字证书、生物信息识别或动态口令等方式进行身份认证，认证通过后方可登录并操作。

4.7.3 第二类权限角色为设备操作与维护人员，权限包括：监测数据、参数、日志查询，设备日常操作与运行维护，以及 B 类参数的配置修改。应具备登录账号、口令设置管理功能。

4.7.4 第三类权限角色为设备查阅人员，无需密码登录，可查看与第一类权限相同的全部功能，但不可进行任何操作。

5 硬件要求

5.1 基本要求

5.1.1 监测设备的硬件设计应确保未经授权的物理拆卸或硬件修改能够被有效阻止或能够被检测并留有可追溯的证据。硬件防范篡改、伪造措施应与软件保护措施协同，形成一体化防护体系。

5.1.2　监测设备应具有永久、不可擦除、唯一的标识编码，标识编码的生成和管理执行HJ 212和HJ XX的相关规定。

5.2　物理封缄保护

5.2.1　监测设备宜配置独立供电的开壳计数器或开封计数器，对设备外壳开启及封印启封次数进行记录，该计数器的初始值应在设备上永久标记，不应具备清零或重置功能。

5.2.2　监测软件、监测数据以及日志的存储介质应采取印封或铅封等物理封缄措施，封装于设备外壳内部或采用专用封罩保护，防止未经授权的拆卸、替换或读取。

5.2.3　影响监测数据准确性、真实性的可变电阻器、可调增益器等可调节器件，以及样品采集管路中的控制阀门、流量调节装置等关键器件，应施加印封或铅封，确保不破坏封印的情况下无法调整或更换。

5.2.4　印封应采用具备防潮、防热和防伪功能的材料制成，带有设备厂商标识；铅封应采用金属或其他材料制成；封缄应确保在不破坏封印的情况下无法打开设备或调整关键部件。封缄被拆除后应加装原厂封缄标识。

5.3　物理接口

监测设备出厂前应删除用于研发、测试的软件功能和程序代码，关闭或熔断所有非必要的物理接口。其中，P 型监测设备应关闭或熔断非必要的 JTAG、SWD 等程序烧录和调试接口，U 型监测设备应在 BIOS 或固件层面禁用非必要的接口。监测数据传输及软件维护所需的接口应实施访问控制。

5.4　数据传输

5.4.1　监测设备对外提供的数据接口（含物理接口和网络端口）应仅支持数据读取操作，不应支持通过该接口对设备内部存储的监测数据、日志记录或参数进行写入、修改或删除。

5.4.2　监测设备与数据采集传输仪或监控平台之间的连接应采用直连方式。监测数据及日志记录的传输应采取单向传输机制，仅允许由设备向外输出，不允许外部反向传输写入。

6　禁止功能

6.1　所有人机交互界面、功能菜单及操作路径均应在设备上公开明示，不应设置未公开的访问入口或指令（组合按键、特殊代码、通信触发、调试指令及隐藏端口等），用于进入隐藏界面、执行隐藏功能或启动其他应用程序等。

6.2　不应具备通过物理或化学手段（吸附、吸收、稀释、过滤、冷凝、化学反应等）改变被测物质状态、浓度的任何功能。监测方法标准规定的必要预处理措施除外。

6.3　不应设置任何可切换至非实测信号源的物理接口、逻辑通道或软件选项（包括内部固定电信号、预置模拟信号等）。所有用于测量的信号输入路径应设计为唯一且固定。

6.4　不应具备以下数据模拟、筛选、删改的功能：

a）通过固定值、随机数等方式模拟生成监测数据；

b）通过数据筛选、数字滤波、平滑等算法处理，致使部分监测数据不被记录或不参与

计算，导致监测结果失真；

c）删除、修改、隐藏监测数据；

d）自动虚假生成停运、校准、故障、维护等数据标记。

6.5　不应具备根据已知标准物质浓度值，不经真实测量，直接生成或预制校准结果或校准参数（包括斜率、截距等）的功能；不应将真实校准生成的校准参数不应用于对应测量的数据计算。

6.6　不应具备接收外部指令，触发设备改变运行状态、篡改监测数据的功能。

6.7　监测设备不应在信号传输链路上设置任何可能导致监测信号衰减、畸变或失真的元器件、电路或功能模块；监测设备与数据采集传输仪或监控平台之间不应设置可对数据进行修改的中间装置。

6.8　不应具备其他可能用于篡改、伪造监测数据的功能。

7　监测设备防范篡改、伪造功能检查

7.1　检查内容

检查时可根据需要，从本标准第 4 章、第 5 章、第 6 章所规定的软件及硬件要求中选择部分或全部项目进行检查。

7.2　检查方法

生态环境主管部门对在用监测设备进行检查时，可根据设备类型和检查条件，选择适宜的检查方法。

a）硬件检查：对设备硬件进行外观及结构检查，确认物理封缄、关键电路封禁、调试接口状态、信号传输线路、样品采集传输管路、开壳计数器记录等防范篡改措施的完好性；

b）软件检查：在不运行程序的情况下，对监测软件程序文件以及系统配置、接口定义、端口开放情况、存储内容等进行分析，包括完整性校验、代码审查、控制流分析、数据流分析、接口分析等，检查是否符合要求；在设备运行状态下，通过实际操作、指令注入等方式，验证设备功能是否与声明一致、保护机制是否有效，包括功能测试、接口测试、异常注入测试、历史存储数据分析等，软件检查推荐方法见附录 B。

7.3　问题分类

7.3.1　存在本标准第 6 章所列禁止功能，或存在 A 类参数可被修改、C 类参数可被人工输入或修改、计算公式可被编辑等情形的，属于监测设备具备篡改、伪造功能。

7.3.2　存在不符合本标准第 4 章、第 5 章其他防范篡改、伪造要求的情形的，属于监测设备存在篡改、伪造风险漏洞。

7.4　配合事项

监测设备生产者、销售者应配合生态环境主管部门对在用监测设备软件的检查工作：

a）提供与设备实际配置及运行情况一致的技术文档，至少包括：硬件组件组成及相关

功能，硬件接口类型、用途及启用状态；操作系统版本、运行进程、内核模块、系统服务、驱动及组件清单，防火墙规则，以及开放的网络端口及其用途；监测软件模块列表，软件接口及命令描述，参数及计算公式列表，软件标识计算方法及获取方式；

b）提供与设备中实际运行版本一致的监测软件程序文件、完整性校验工具、调试接口访问工具等技术支持，并指派技术人员协助验证操作；

c）如实说明设备的软件保护机制、封缄设计、权限分级设置等技术实现方式，不应隐瞒或提供虚假信息。

附 录 A

（规范性附录）

固定污染源现场监测设备日志记录内容

表 A.1　固定污染源现场监测设备日志记录内容

日志类型	日志分类	记录内容	示例
设备操作日志	登录记录	登录账号、登录账号权限级别、登入时间、登出时间、登录方式	登录方式：口令、扫码、指纹
	校准记录	校准时间、校准参数、校准内容、标准物质标称值、测定值、校准偏差	校准内容：零点校准、量程校准
	参数修改记录	修改时间、参数名称、修改前值、修改后值	参数名称：烟道截面积、速度场系数、消解温度、消解时长、TOC 与 COD_{Cr} 转换系数等
	公式选配记录	选配时间、公式名称、选配前公式、选配后公式	公式名称：氮氧化物折算公式、排放流量计算公式等
	软件升级记录	升级时间、升级版本号、旧版本号、升级结果	升级结果：升级成功、升级失败回滚至旧版本
	时间修改记录	修改方式、修改时间、修改前时间、修改后时间	修改时间：2026-10-11 08:30:15
设备运行日志	工作状态记录	开始时间、结束时间、状态类型	状态可分为开机、关机、联网、校准、测试、吹扫、清洗、故障、通信中断。应将完整采样测试步骤形成日志记录
	报警记录	开始时间、报警内容、恢复时间	报警内容包括：设备故障、断电、通信异常、定位授时失败、完整性校验失败、来源真实性校验失败、性能参数超阈值、校准参数超阈值。性能参数超阈值、校准参数超阈值还应记录参数名称、参数阈值范围、参数数值
	安全事件记录	事件类型、开始时间、结束时间、处理情况	事件类型包括：调试接口启用、端口开启、外部设备接入、系统服务启停、远程访问。其中端口开启、外部设备接入、系统服务启停为操作系统日志记录内容

附 录 B

（资料性附录）

固定污染源现场监测设备软件功能检查推荐方法

本附录所列检查方法名称参考JJF 1182。对应的检查内容根据固定污染源监测设备具体情况进行适当调整。对监测设备软件进行检查时，应重点考虑以下检查方法和内容。方法选择、检查次序可根据实际情况调整。

表 B.1　软件检查推荐方法概述

方法描述	检查内容	应用条件和工具	方法操作
文档分析和设计评价（AD，Analysis of the document and evaluation of the design）	设备功能、性能设计符合性	被验证设备文档齐全、软件包标识明确	查看设备产品文档所列设备功能设计，评价设备软件功能、接口、算法等各项设计与标准规范的符合性
计量功能测试验证（VFTM，Verification by functional testing of metrological functions）	算法正确性、不确定度、补偿和纠正算法、计算规则	操作手册、标准样品或计量标准器具	对照操作手册，用标准样品或标准器具测试设备的计量性能，查验其算法、公式、修正等准确性、有效性
软件功能测试验证（VFTSw，Verification by functional testing of software functions）	通信，示值，防篡改，参数、数据与日志保护，功能诊断等功能的正确运行及系统配置	操作手册、软件文档	对操作手册、软件文档按描述的特性进行实际手工操作检查、测试。 常规功能：通过对开关、按键或按键组合、菜单所列功能项等操作观察设备响应。 通信：按照操作手册和软件文档配置通信接口及参数，与配套接收平台或模拟平台建立连接，发送和接收规定的数据或命令，核对通信状态、传输数据及其标识与设备显示、存储结果的一致性；模拟传输延时、通信中断和恢复等情形，查验软件是否按照规定作出提示或告警，并完成确认应答、数据缓存、重传或补传、恢复连接及日志记录等响应。 示值：结合计量功能测试验证。 参数、数据与日志保护：激活保护手段，尝试修改、删除相关数据，查验设备响应情况。 防篡改：对照软件文档，查验设备软件防篡改功能设计，结合相关不合规操作，验证设备防篡改功能。 功能诊断：诱发、模拟或实施一个设备故障、功能异常，或尝试修改相关功能表征参数数值，查验设备是否检测到并作出控制。 系统配置：尝试修改系统配置或软件运行环境，查验软件是否禁止更改或停止运行。
测量数据流分析（DFA，Metrological data flow analysis）	软件分离、命令对设备功能影响	软件文档、软件代码、编辑器、通用软件分析工具	从接收传感器原始测量数据的硬件端口开始，逐个搜索读取原始测量数据、将原始数据转

方法描述	检查内容	应用条件和工具	方法操作
			换为中间值、最终值的子程序，所有用于存储这些中间值的变量和传输这些值的子程序均应在软件代码中查找到。
代码审查和代码走查（CIWT，Code inspection walkthrough）	软件的任何特性	软件代码、通用软件分析工具	使用软件分析工具审查指定软件代码或全部代码，查验程序功能和特性与文档要求是否一致。
软件模块测试（SMT，Software module testing）	特定软件模块功能正确性	软件代码、软件模块测试的运行环境	将被测试模块置于测试环境中，专用的测试程序模块调用被测软件模块，输入所需的输入数据，测试程序接收被测模块的输出数据，并与参考期望值进行比较。

表 B.2　固定污染源现场监测设备功能检查方法

序号	检查内容	检查项	检查方法组合	检查要点
1	4.1 软件标识	标识内容组成符合要求；可显示、可查看	AD + VFTSw	文档审查标识格式；功能测试验证标识可显示、可查看
2		软件安装、升级执行校验	AD + VFTSw + CIWT	文档审查升级流程；功能测试验证校验失败拒绝安装、功能测试升级后验证标识变更；代码审查引导加载程序逻辑
		升级后标识更新；由内置的引导加载程序执行，不应绕过		
3	4.2 参数与计算公式管理	参数分类管理：A 类参数只读存储、调用时校验；B 类参数权限配置、生成日志；C 类参数自动生成，禁止人工输入或修改	AD + VFTSw +CIWT + SMT	文档审查参数分类及权限设置；代码走查 A 类存储及校验逻辑；模块测试验证 A 类参数校验失败拒绝计算；功能测试 B 类参数验证配置权限及日志生成；代码审查排查 C 类参数人工输入接口，功能测试尝试人工修改
4		参数管理：公式固化、只读存储、调用校验，显示与说明书一致	AD + VFTSw + CIWT + SMT	文档审查公式封装；功能测试可修改性；代码走查校验逻辑；模块测试验证校验失败拒绝计算并记录日志
5	4.3 日志管理	日志自动生成，内容完整	AD +VFTSw + CIWT	文档审查日志记录要求；功能测试验证各类日志内容；代码审查排查选择性记录逻辑
6	4.4 存储保护	写入控制：监测数据及日志记录仅应用软件可写入	DFA + CIWT	数据流分析追踪写入路径；代码审查排查未授权写入途径
7		时间戳保护：监测数据及日志记录：从硬件时钟读取、禁止外部修改	AD + VFTSw + CIWT	文档审查时钟设计；功能测试尝试修改时间戳；代码审查时间戳来源
8		数据覆盖：按先入先出策略，覆盖最早数据	AD + VFTSw + DFA	文档审查数据存储策略；功能测试验证 FIFO 策略；数据流分析确认无中间插入/修改
9		便携监测设备加密存储	AD + CIWT	文档审查加密算法；功能测试加密情况；代码审查加密实现
10	4.5 运行环境	最小化安装，裁剪非必要组件，禁止切换至桌面环境	AD + VFTSw	文档审查组件清单；功能测试验证运行环境，代码审查非法进入桌面环境的逻辑程序
11		禁止远程操作功能；记录端口、存储、登录等	AD + VFTSw	文档审查；功能测试验证远程功能禁用、OS 日志记录

序号	检查内容	检查项	检查方法组合	检查要点
		操作系统事件日志		
12	4.6 异常响应	分级响应	AD + VFTSw + CIWT	文档审查分级逻辑；功能测试模拟各类异常验证响应；代码审查异常处理
13	4.7 权限管理	三类权限、对应功能菜单全部显示：一类权限认证，二类权限账号口令管理，三类权限仅查看不可操作	AD + VFTSw	文档审查权限定义；功能测试验证权限隔离、认证强度、口令管理、操作范围
14	5.1 设备唯一标识编码	具有永久不可擦除的 SN 码	AD + VFTSw	文档审查；平台与设备比对查验
15	5.2 物理封缄保护	开壳控制	AD + VFTSw	文档审查；功能测试验证计数不可清零
16		存储介质印封或铅封保护	AD	外观及结构检查
17		可调器件、管路阀门等关键器件封缄	AD	外观及结构检查
18	5.3 物理接口禁用	关闭/熔断非必要接口	AD + VFTSw	文档审查；功能测试验证接口禁用状态
19	5.4 数据传输	数据接口只读，禁止写入	AD + VFTSw + CIWT	文档审查；功能测试尝试写入操作； 代码审查接口权限
20		直连单向传输，无中间装置	AD + VFTSw	文档审查拓扑；功能测试验证单向传输
21	6.1 禁止隐藏功能	禁止未公开访问入口	AD + CIWT	文档审查确认所有命令/接口已声明；代码审查排查未文档化的后门入口
22	6.2 禁止改变样品	禁止物理/化学手段改变被测物质	AD + VFTM	文档审查确认预处理环节符合方法标准；计量功能测试验证样品传输管路无旁路、无附加处理单元； 硬件检查
23	6.3 禁止信号模拟	禁止切换至非实测信号源	AD + VFTSw + CIWT	文档审查信号路径设计；功能测试验证所有测量信号输入路径唯一且固定；代码审查排查模拟信号切换逻辑
24	6.4 数据变造	禁止固定值、随机数模拟生成数据	AD +VFTSw + CIWT + SMT	文档审查数据生成机制；功能测试注入异常输入验证输出非模拟值；代码走查分析数据生成逻辑模块测试验证数据采集路径
25		禁止数据筛选或算法处理导致数据失真	AD + VFTM + CIWT	文档审查滤波/平滑算法； 计量测试验证全量程数据记录完整性； 代码审查选择性丢弃逻辑
26		禁止删除、修改监测数据	AD +VFTSw + DFA + CIWT	文档审查数据处理方式；功能测试尝试删改操作；数据流分析追踪数据写入路径；代码审查确认仅 FIFO 覆盖策略
27	6.5 禁止虚假校准	禁止直接生成校准结果	VFTSw + CIWT + SMT	功能测试验证校准须经真实测量；代码走查分析校准参数生成逻辑；模块测试验证校准－计算关联
28	6.6 禁止外部操控	禁止外部指令篡改数据	AD + VFTSw + CIWT	文档审查所有外部指令列表；功能测试注入非法指令；代码审查排查未声明命令处理
29	6.7 禁止传输干扰	禁止信号传输链路干扰	AD + VFTM	文档审查硬件设计；计量测试验证传输链路信号完整性