附件 9

《固定污染源现场监测设备防范篡改伪造功能通用要求（征求意见稿）》编制说明

《固定污染源现场监测设备防范篡改伪造功能通用要求》标准编制组

二〇二六年十月

项目名称：固定污染源现场监测设备防范篡改伪造功能通用要求

项目统一编号：2026-56.2

承担单位：中国环境监测总站、生态环境部环境工程评估中心

编制组主要成员：王军霞，刘常永，杨伟伟，陈岩，王慧，秦宇，刘健，王成，李宗超，周刚

标准支持单位技术管理负责人：王磊

生态环境监测司项目负责人：仇鹏

目　　录

1　项目背景 1
1.1　任务来源 1
1.2　工作过程 1
2　标准制订的必要性分析 3
2.1　落实上位法要求，为上位法实施提供技术支撑 3
2.2　填补标准体系空白，为设备监管提供统一的判定依据 3
2.3　堵塞设备端造假漏洞，从技术源头遏制监测数据造假 3
2.4　推动监管模式从“事后追查”向“事前防控”转变 4
2.5　用“明规则”替代“潜规则”，促进监测设备行业健康发展 4
3　国内外相关标准情况 4
3.1　国外相关标准研究的发展现状 4
3.2　国内相关标准研究的发展现状 5
4　标准制订的基本原则和技术路线 6
4.1　标准制订的基本原则 6
4.2　标准制订的技术路线 6
5　本标准主要内容 8
5.1　适用范围 8
5.2　规范性引用文件 8
5.3　术语和定义 8
5.4　软件要求 8
5.5　硬件要求 10
5.6　禁止功能 11
5.7　监测设备防范篡改、伪造功能检查 11
6　标准实施建议 11
7　参考文献 12

《固定污染源现场监测设备防范篡改伪造功能通用要求（征求意见稿）》编制说明

1 项目背景

1.1 任务来源

固定污染源现场监测设备为排污单位自行监测、生态环境执法监测、比对监测提供硬件支撑，是环境监测体系的关键装备。《生态环境监测条例》提出开展自行监测应当使用符合国家标准和规范的监测设备，并要求企事业单位不得通过不正常运行、破坏监测设备、擅自修改监测设备参数、使用作弊工具等手段造成监测数据失真；《排污单位自行监测管理办法》进一步明确开展自行监测应当使用符合国家相关标准和规范的监测设备、标准器具以及有证标准物质，监测设备应当具备防范篡改、伪造监测数据的相关功能；《关于加强技术防控提升排污单位自行监测质量的通知》（环办监测函〔2024〕214号）也明确要求各地排查现场监测设备可能存在的不当干预功能。总体来看，当前针对固定污染源现场监测设备防范篡改、伪造的专项技术要求仍不完善。HJ 76修订时已明确增加防篡改相关内容，但由于无法覆盖废气中其他污染物、废水、噪声自动监测设备及便携式监测设备等防篡改功能要求，亟需通过通用标准统一规定，再由专用仪器标准结合设备特性进一步明确。据此，有必要制定《固定污染源现场监测设备防范篡改伪造功能通用要求》标准，建立覆盖监测设备软硬件防范篡改、伪造功能的统一技术要求，为落实法规政策要求、压实相关主体责任、提升监测设备技术防控能力、保障监测数据真实可靠提供基础支撑。

1.2 工作过程

1.2.1 成立标准编制组

2025年4月初，中国环境监测总站作为项目承担单位，组织成立标准编制组，明确标准研究目标、工作分工和进度安排，统筹推进文献调研、问题梳理、专题调研、文本起草和专家研讨等工作。初步拟定了标准制订的工作目标，确定了工作计划与任务分工。

1.2.2 开展法规、标准和案例调研

2025年4月中旬，编制组系统梳理了环境领域的《生态环境法典》《生态环境监测条例》《排污许可管理条例》《关于加强技术防控提升排污单位自行监测质量的通知》等法规政策文件以及计量领域的通用要求标准，研究固定污染源自动监测、现场手工监测、数据传输、计量软件和信息安全等相关标准，重点识别现场监测设备在隐藏功能、权限管理、参数保护、日志留痕、接口控制、异常响应等方面的共性风险点和现有标准空白。

1.2.3 文本编制与研讨

2026年4月27日至30日，编制组组织6家设备厂商开展集中编制工作，完成标准草

案编制，咨询计量行业专家和部分生态环境领域科研人员，对草案进行研讨，编制组根据专家意见不断完善草案文本及编制说明。

1.2.4 开展专题调研与技术交流

2026 年 4 月至 7 月，编制组围绕计量器具、电动车管理和软件测评技术开展专题调研与技术交流。4 月 6 日赴太仓市调研电子计价秤监管实践，重点了解“三码一封”技防手段和集生产、检定、监管、维修于一体的全链条智慧监管体系；5 月 14 日赴内蒙古自治区调研燃油加油机防作弊监管，重点了解将设备身份、软件版本、维修拆封和经营数据相互印证的“四方验证”管理机制；5 月 21 日赴广州市工业和信息化部电子第五研究所、广东省计量科学研究院，重点交流电子设备防范篡改与防抵赖技术路径、嵌入式设备安全验证方法、计量器具防作弊监管实践，以及通用要求类标准条款写作的颗粒度、符合性验证路径和落地可行性；7 月 22 日赴工业和信息化部标准化研究所，就软件测评防范篡改监管手段、电动自行车白名单管理、一车一机一池一充编码规则等问题开展交流，梳理了当前技防标准监管难点与优化方向。根据调研情况进一步完善草案文本。

1.2.5 组织设备防范篡改伪造验证

2026 年 6 月，为进一步检验标准草案的可操作性和技术要求的合理性，编制组组织开展了设备防范篡改、防伪造功能验证。依据前期调研形成的重点风险清单，选取典型监测设备，采用调试分析、固件解包、程序辅助分析、端口扫描、抓包与协议分析、漏洞扫描、无线通信测试、芯片接口测试等技术手段，并结合大模型开展验证。形成了典型设备验证报告，初步掌握了当前设备防范篡改伪造功能的实现现状、主要薄弱环节及验证难点。

1.2.6 召开预研究项目结题论证暨制修订项目开题论证会

2026 年 6 月 30 日，生态环境监测标准预研究项目结题论证暨制修订项目开题论证会以腾讯会议方式召开。专家组听取了项目主编单位关于项目主要技术内容、编制工作过程等情况的汇报，经质询讨论，认为项目定位准确，提供材料齐全、内容完整、格式规范，技术路线合理可行，对国内外标准、文献及当前存在问题的调研较为充分，内容科学合理，满足当前管理需求。专家组建议进一步加强与固定污染源便携式监测设备数据传输技术要求等相关标准的内容协调，并按照《环境保护标准编制出版技术指南》（HJ 565）对标准文本和编制说明进行规范性编辑。编制组根据专家意见对标准文稿和编制说明进行了修改完善。

1.2.7 征求意见稿技术审查会

2026 年 8 月 28 日，生态环境监测司召开《固定污染源废气（SO_2、NO_X、颗粒物）排放连续自动监测技术规范》等 4 项国家生态环境标准征求意见稿技术审查会，会上专家一致通过本标准征求意见稿技术审查。

2 标准制订的必要性分析

2.1 落实上位法要求，为上位法实施提供技术支撑

《生态环境监测条例》第25条：企事业单位应当建立健全监测数据质量管理制度。企事业单位及其负责人对监测数据的真实性、准确性负责。企事业单位不得实施或者明示、暗示有关单位、个人实施下列对监测数据弄虚作假的行为：（一）未实际开展监测，直接出具监测报告；（二）篡改、伪造原始监测记录、监测数据；（三）故意漏检监测项目或者改变监测条件；（四）调换监测样品或者擅自改变采样点位、时间等，干扰采样环境或者采样活动；（五）通过不正常运行、破坏监测设备，擅自修改监测设备参数设置，虚假标记自动监测设备状况或者生产设施、污染防治设施工况，或者使用作弊工具等手段，使监测数据失真；（六）其他对监测数据弄虚作假的行为。最高法、最高检环刑解释第11条：违反国家规定，针对环境质量监测系统实施下列行为，或者强令、指使、授意他人实施下列行为，后果严重的，应当依照刑法第二百八十六条的规定，以破坏计算机信息系统罪定罪处罚：（一）修改系统参数或者系统中存储、处理、传输的监测数据的；（二）干扰系统采样，致使监测数据因系统不能正常运行而严重失真的；（三）其他破坏环境质量监测系统的行为；《生态环境法典》第80条：禁止通过干扰采样、调换样品、改变监测条件、虚假监测、篡改或者伪造记录等方式对生态环境监测数据弄虚作假或者指使对生态环境监测数据弄虚作假。禁止通过侵占、损毁或者擅自移动、改变等方式干扰、破坏生态环境监测设施、设备或者指使干扰、破坏生态环境监测设施、设备。

但从现有制度体系看，上位法和政策文件更多提出原则性要求与监管要求，对于现场监测设备应当具备哪些防范篡改伪造功能，如何通过设备端落实“禁止什么、控制什么、记录什么、出现异常如何处置”等关键要求，仍缺少统一、细化、可核查的技术支撑标准。本标准的制订，有助于将法规政策要求转化为设备侧可执行、可验证的技术条款，为《生态环境监测条例》落地实施提供技术支撑。

2.2 填补标准体系空白，为设备监管提供统一的判定依据

目前，生态环境监测标准体系已在监测方法、性能指标、运行管理和数据传输等方面形成了较为系统的技术要求，但针对固定污染源现场监测设备防范篡改、伪造功能的专项通用要求仍属空白。监管部门在开展现场排查、技术核查和责任认定时，缺少统一的设备端判定依据；设备生产企业在产品设计和功能配置时，也缺少统一遵循的技术底线。

本标准围绕禁止功能、软件标识、权限管理、参数与计算公式保护、日志管理、数据及日志记录存储保护、软件运行环境、异常响应、硬件防护、接口控制和检查要求等提出系统规定，能够有效填补现行标准体系空白，为设备监管、监督检查、产品研发和技术改造提供统一依据。

2.3 堵塞设备端造假漏洞，从技术源头遏制监测数据造假

从当前现场监测实践看，监测数据失真风险已经由单一参数修改扩展到隐藏功能、越权操作、关键参数篡改、计算公式修改、日志删除、远程维护通道滥用、外部接口写入等多个环节。一些设备存在隐藏菜单、组合按键、特殊代码、未受控远程登录、校准系数可强行修

改、日志记录不全等问题，为监测数据造假留下了技术空间。

本标准聚焦设备端最容易影响数据真实性和可追溯性的关键风险点，提出设备不得具备的功能以及必须具备的保护、记录、校验和响应机制，能够把防造假要求前移至设备设计、研发、生产和运维环节，从技术源头堵塞漏洞，压缩利用设备实施数据造假的空间。

2.4 推动监管模式从“事后追查”向“事前防控”转变

传统监管模式更多依赖事后检查、异常追溯和案件查办，对设备端的技术防护和过程留痕关注不足。一旦设备本身存在不当干预功能，监管部门即使事后发现异常，也往往面临证据链不完整、原因难追溯、责任难界定等问题。通过制订本标准，能够推动设备在出厂前即固化关键参数保护、日志留痕、软件校验、异常响应、接口受控等功能，将监管重点由“事后追查”向“事前防控、事中留痕、事后可追溯”转变。

2.5 用“明规则”替代“潜规则”，促进监测设备行业健康发展

当前行业内不同企业在设备安全设计、权限控制、接口管理、日志保护等方面水平不一，部分产品因缺少明确约束而存在“成本优先、合规不足”的情况，不利于行业公平竞争和健康发展。本标准通过建立统一、公开、可验证的技术规则，把设备端防范篡改伪造要求由经验判断转化为明晰规则，有利于引导企业按照统一标准开展研发设计、测试验证和产品改造，推动行业从“潜规则”竞争转向“明规则”竞争，促进固定污染源现场监测设备规范化、高质量发展。同时，标准实施后可增强设备运行过程透明度和可核查性，为非现场监管、智慧监管、精准执法提供稳定的设备基础支撑，提升全过程监管效能。

3 国内外相关标准情况

3.1 国外相关标准研究的发展现状

从国外情况看，污染源监测领域现有标准更多聚焦监测方法、性能评价、质量保证和数据报送，对设备防不当干预功能本身形成专门通用标准的并不多。可借鉴的成熟经验，主要分布在法制计量、工业控制安全和通用产品安全评估等领域。

在法制计量领域，《非自动衡器》（OIML R76）、《国际法制计量术语表》（OIML V 1:2013）等标准和相关实践强调软件识别、法制相关参数保护、封缄、事件记录和干预后复核等要求，对“哪些功能需要受保护、修改后如何保持可追溯”提供了直接参考。在工业控制和信息安全领域，信息安全、网络安全和隐私保护—信息技术安全评估准则（ISO/IEC 15408）系列、联邦信息处理标准-加密模块安全要求（FIPS 140-3）、工业自动化和控制系统安全：IACS 组件的安全技术要求（IEC 62443-4-2）等标准强调建立从硬件、固件、操作系统到应用层的信任链，采用安全启动、完整性校验、权限分离、接口受控和密码模块保护等措施，适合为监测设备的软件保护、升级校验、异常检测和接口控制提供技术借鉴。

国外经验的启示在于吸收其在可信标识、关键参数保护、日志审计、接口最小开放和分层验证方面的基本理念，并结合生态环境监测设备现场使用、成本约束和监管场景形成可落地要求。

3.2 国内相关标准研究的发展现状

3.2.1 相关法律规章

近年来，我国不断完善生态环境监测相关法律法规和管理制度，对污染源监测数据质量、监测设备管理以及弄虚作假责任追究提出了更明确的要求，为固定污染源现场监测设备防范篡改、伪造功能要求的研究提供了制度基础。

在政策文件层面，《关于推进生态环境监测体系与监测能力现代化的若干意见》等文件提出，要构建天地一体、上下协同、信息共享的生态环境监测网络，持续提升监测数据质量和监测数据公信力。《关于加强技术防控提升排污单位自行监测质量的通知》（环办监测函〔2024〕214号）则进一步从技术防控角度作出专门部署，明确要求各地排查现场监测设备可能存在的不当干预功能，重点关注隐藏操作界面、远程登录或遥控、外部数据导入、日志记录不全、校准参数可强行修改、软件升级信息不备份以及现场手工监测设备缺少定位授时、防伪功能等问题。这些要求表明，设备端防范篡改伪造能力已成为提升自行监测质量的重要环节。

此外，部分地方也结合本地监管需要，探索建立了与固定污染源监测相关的参数联网、视频联网、过程留痕、异常预警等制度安排，为设备防不当干预要求落地实施提供了实践基础。总体上看，现有法律规章和政策文件已对固定污染源现场监测设备提出了越来越明确的真实性、可追溯性和防干预要求，但尚需通过专门标准将上述要求细化为统一、可执行、可验证的技术条款。

3.2.2 相关标准规范

从现有标准体系看，我国已在固定污染源自动监测、监测方法、数据传输、计量软件控制等方面形成了较为丰富的标准基础，为本标准研究提供了重要支撑。

在生态环境监测领域，围绕固定污染源自动监测系统，已发布《固定污染源烟气（SO_2、NO_X、颗粒物）排放连续监测技术规范》（HJ 75）、《固定污染源烟气（SO_2、NO_X、颗粒物）排放连续监测系统技术要求及检测方法》（HJ 76）、《固定污染源废气非甲烷总烃连续监测系统技术要求及检测方法》（HJ 1013）等标准，对系统组成、技术性能、检测方法和运行管理提出了明确要求。《污染物自动监测监控系统数据传输技术要求》（HJ 212）则对自动监测数据采集、报文格式、通信方式和传输要求作出了统一规定。这些标准在自动监测系统建设和运行管理方面已形成较成熟体系，但其重点主要在于测量性能、运行规范和数据传输，对设备隐藏功能防控、关键参数防范篡改、日志不可删改、异常分级响应等方面尚缺少系统性规定。

在计量和软件控制领域，《计量器具控制软件的通用要求》（GB/T 42555）、《计量器具软件标识通用要求》（JJF 2356）、《计量器具软件测评指南》（JJF 1182）等文件，对软件标识、软件保护、参数固化、事件记录、封缄和软件验证等提出了较为成熟的要求，为本标准中软件标识、参数管理、日志留痕和验证机制的设计提供了直接参考。《污染源自动监测设备软件配置与评估技术规范》（T/CSES 188）等行业技术文件，也为污染源监测设备软件配置和功能评估提供了借鉴基础。

与此同时，加油机、电子秤等商用计量器具防作弊领域在软件封装、参数保护、日志记

录、封缄管理和维修后重新确认等方面积累了较为成熟经验，对监测设备防范篡改伪造要求的提出具有较强参考价值。总体上看，现有标准体系已经在环境监测和计量软件控制两个层面形成了一定基础，但尚未针对固定污染源现场监测设备防范不当干预建立专门的通用要求标准，特别是在软硬件一体化防护、异常响应、在用设备验证等方面仍存在明显空白。本标准的研究，正是在现有标准体系基础上，对上述空白进行补充和完善。

3.2.3 固定污染源现场监测设备技术现状

目前，固定污染源现场监测设备种类较多、技术路线差异明显，不同设备在测量原理、系统结构、参数设置及数据处理方式上各不相同，面临的篡改风险和技防需求也存在差异。连续自动监测设备系统组成复杂，涉及采样、预处理、分析、数据采集与传输等多个环节，关键参数、计算公式和校准系数易成为干预对象，具备远程维护和通信功能的设备尤其需要防范隐藏操作和越权调参。便携式及移动式监测设备流动性强，不同品牌在定位授时、软件架构、接口协议、日志管理和原始记录留存等方面参差不齐，过程留痕和现场真实性支撑不足。数据采集传输设备接口多、权限高，容易成为参数篡改和日志删除的通道。总体看，现有设备防范篡改功能配置不均衡，尚缺乏统一、可验证的技术要求，这正是本标准研制的现实基础。

4 标准制订的基本原则和技术路线

4.1 标准制订的基本原则

（1）依法合规，设置专项标准接口。紧扣生态环境监测设备监管和防范人为干预、篡改伪造监测数据的法规政策要求，重点提出适用于不同监测设备的基础性、通用性要求，同时为自动监测设备、现场手工监测设备、数采传输设备等后续分类细化和专项标准制定留出衔接空间。

（2）问题导向，聚焦设备端造假风险。针对现场监测数据造假中暴露的设备端漏洞和薄弱环节，重点围绕隐藏功能、参数篡改、数据导入、日志删除等突出问题设置条款，通过功能禁止、防范措施和干预留痕等要求，有针对性明确监测设备防范篡改伪造要求。

（3）软硬协同，构建闭环防护体系。坚持“以软件为主、兼顾硬件”的技术思路，既强化监测软件标识、参数与计算公式保护、日志管理、存储保护、运行环境、异常响应和权限管理等软件层面防护，防止通过软件非法操作干预监测过程和监测结果；又通过监测硬件要求对设备唯一标识、物理封缄、物理接口和数据传输等环节提出控制要求，防止硬件拆解、改装或通过接口干预数据，形成软件防护与硬件封缄相结合的闭环防护体系。

（4）可操作、可验证，兼顾技术发展。标准条款以可查、能测、能判定为基本要求，便于设备生产者落实、检测机构验证和监管部门现场核查。同时，标准重点提出功能和管理层面的原则性要求，不限定具体技术实现路径，为未来设备安全防护、身份认证、完整性校验、异常识别等技术升级留有余地。

4.2 标准制订的技术路线

本标准的制订严格遵循国家生态环境标准制修订有关要求，重点围绕固定污染源现场

监测设备防范篡改、伪造的关键风险环节开展研究。在技术路线设计上，聚焦设备端可能影响监测数据真实性、准确性和可追溯性的主要问题，提出禁止功能要求，重点研究软件控制、硬件防护、参数与计算公式管理、日志留痕、接口受控、异常响应和功能验证等方面的通用技术要求，明确现场监测设备在防不当干预方面应具备的基础功能边界和验证思路。

标准编制过程中，系统梳理了生态环境监测、排污许可、自行监测质量管理以及计量软件控制、设备防作弊、信息安全等领域的法规、政策和标准要求，精准识别固定污染源现场监测设备在隐藏功能、越权操作、参数篡改、数据伪造、日志删除、异常干预和远程访问等方面的风险点。同时，通过集中编制、专题调研、技术交流、典型设备验证和开题论证，充分听取设备生产企业、计量技术机构、科研单位及生态环境管理部门意见，研究形成兼顾风险防控需求、技术可实现性和现场可操作性的标准框架。

在此基础上，本标准围绕适用范围、规范性引用文件、术语和定义、禁止功能、监测软件要求、监测硬件要求、监测设备防范篡改伪造功能检查及资料性附录等内容构建总体结构，既体现了固定污染源现场监测设备防范篡改伪造的共性要求，又为后续具体设备标准细化和检查方法完善预留空间。标准制订技术路线如图 1 所示。

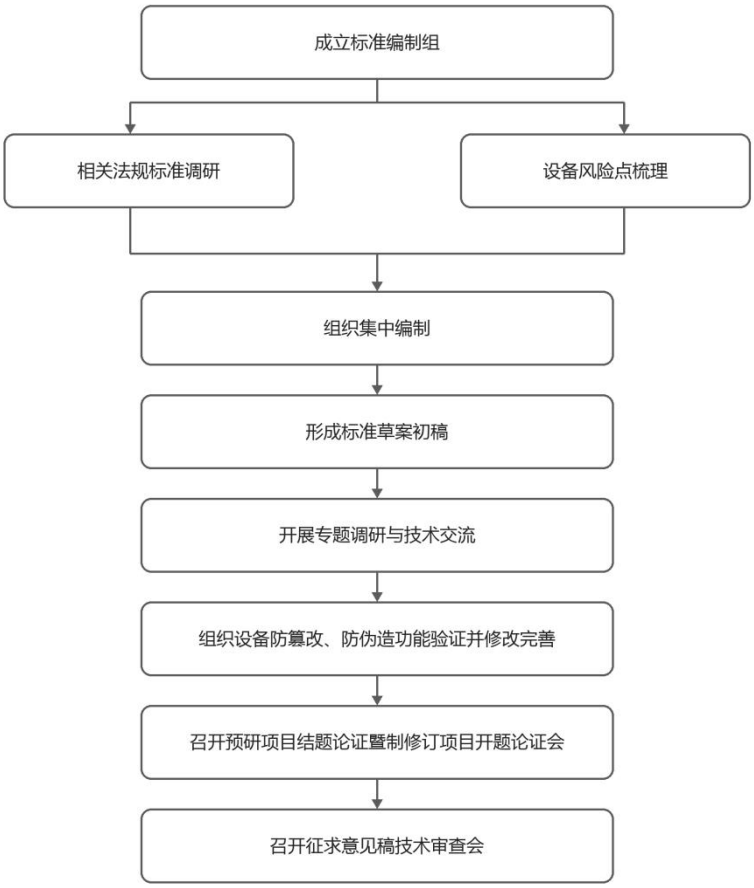


图 1　标准制订技术路线

5　本标准主要内容

本标准共设置 7 章，并设置规范性附录 A 和资料性附录 B，主要包括适用范围、规范性引用文件、术语和定义、软件要求、硬件要求、禁止功能、监测设备防范篡改伪造功能检查等内容。

5.1　适用范围

明确了本标准的适用对象和边界。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；无专项技术标准或专项技术标准未作规定的，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。

5.2　规范性引用文件

本标准引用 GB/T 7408.1 日期和时间 信息交换表示法 第 1 部分：基本原则，参考其关于“时间戳”的术语和定义；引用 HJ 212《污染物自动监测监控系统数据传输技术要求》和 HJ XX 《固定污染源便携式监测设备数据传输技术要求》衔接固定污染源自动监测设备和便携监测设备的数据传输及设备标识管理要求；引用 JJF 1182《计量器具软件测评指南》，参考软件功能检查推荐方法；引用 JJF 2356《计量器具软件标识通用要求》，支撑软件标识等条款设计。

5.3　术语和定义

对本标准涉及的关键术语进行了界定，包括固定污染源现场监测设备、P 型监测设备、U 型监测设备、监测软件、软件标识、固件、保护性接口、完整性校验、数字签名、时间戳、日志记录、封缄、软件保护、软件检查等。

5.4　软件要求

本章是本标准的主要章节，内容涵盖软件标识、参数与计算公式、日志管理、监测数据及日志记录存储保护、软件运行环境、异常响应和软件操作权限等方面，重点规定设备在软件层面应具备的控制要求。

5.4.1　软件标识

本节规定了软件标识的组成、生成方式以及通过引导内置程序执行加载、完整性校验、来源真实性校验和软件安装升级流程。

5.4.2　参数与计算公式

本节针对影响监测结果的设备关键参数和计算公式提出防范篡改伪造保护要求，将关键参数分为三类：不可修改的 A 类参数、由第二类权限角色根据现场情况配置并留痕的 B 类参数以及由设备自动生成且不应具备人工输入和修改功能的 C 类参数。针对这三类参数提出差异化的防范篡改伪造防护要求，同时要求参与监测数据计算的公式固化存储、完整性

校验并可查询展示，以防止通过修改参数或计算逻辑篡改、伪造监测数据。

5.4.3 日志管理

本节规定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。

日志记录类型及记录内容见附录 A。附录 A 将日志记录划分为设备操作日志和设备运行日志，明确登录、校准、参数修改、公式选配、软件升级、时间修改、工作状态、报警、安全事件等记录内容。

5.4.4 监测数据及日志记录存储保护

本节对监测数据及日志记录的存储保护作出规定。要求监测数据及日志记录仅允许由监测应用软件生成，不得通过网络、本地或进程间通信等方式提供任何未经授权的访问或写入途径。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，不得支持外部写入或直接修改时间戳数值；自动监测设备时钟应按照 HJ 212 要求进行授时校准，便携式监测设备应通过北斗卫星或网络进行授时校准，并同时记录定位信息。

同时，标准要求监测数据及日志记录存储采用先入先出策略，仅允许按预设规则自动覆盖最早数据和日志，禁止在存储序列中间插入、修改或删除数据，监测数据与日志记录应分区独立存储。并对监测设备中的监测数据和日志记录保存期限提出要求，不得少于 2 年。未与生态环境部门监管平台联网传输的本地存储数据及日志记录应加密存储，宜采用国密 SM4 算法加密。

5.4.5 软件运行环境

本节规定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。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，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、端口及账户。

同时，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；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，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；操作系统应启用日志记录功能，并对端口开启与关闭、外部设备接入、远程登录及访问、用户登录与登出、系统服务启停等事件进行完整记录。

5.4.6 异常响应要求

本节规定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，并生成异常响应处置日志。

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；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；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。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；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。

5.4.7 软件操作权限

本节对应用软件操作权限分类管理提出要求，规定应设置三类权限，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。第一类权限角色为设备生产销售者，具有设备所有功能的访问和操作权限，不应授权或转交他人使用，并应采用数字证书、生物信息识别或动态口令等方式进行身份认证；第二类权限角色为设备操作与维护人员，可进行监测数据、参数、日志查询、设备日常操作与运行维护以及 B 类参数配置修改，并应具备登录账号、口令设置管理功能；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。

5.5 硬件要求

5.5.1 基本要求

本节规定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，硬件防范篡改措施应与软件保护措施协同形成一体化防护体系。同时，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。

5.5.2 物理封缄保护

本节规定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，计数器初始值应在设备上永久标记，不应具备清零或重置功能。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，影响监测数据准确性、真实性的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，也应施加印封或铅封。

本节还规定印封、铅封等封缄材料和封缄方式应满足防潮、防热、防伪和不可无痕开启要求，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。

5.5.3 物理接口

本节规定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。

5.5.4 数据传输

本节规定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。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，不得设置可对数据进行修改的中间装置；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。

5.6 禁止功能

本章明确了 8 类不应具备的功能，包括隐藏功能、改变样品、信号模拟、数据变造、虚假校准、外部操控、传输干扰以及其他可能用于篡改、伪造监测数据的功能。

5.7 监测设备防范篡改、伪造功能检查

本章规定生态环境主管部门可根据需要，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。可根据设备类型和检查条件，选择适宜的检查方法（硬件检查、软件检查），对设备防范篡改伪造要求的符合性进行检查，并给出软件检查推荐方法（附录 B）。对检查发现的问题分为两类：监测设备具备篡改、伪造功能和监测设备存在篡改、伪造风险漏洞。明确存在本标准第 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。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。并从设备生产者、销售者需配合的事项等方面作出规定。

6 标准实施建议

为切实推动本标准落地实施、筑牢污染源监测数据可信基础，助力环保物联网规范化监管，需从系统架构与各方主体两方面统筹推进。系统层面，现场监测设备、传输网络、监管上位平台协同落实防范篡改条款，完整实现数据、参数、日志全链条可信采集传输；实施层面，主管部门做好标准宣贯培训，设备厂商对标监测软件标识、权限控制、参数与公式固化、日志记录、存储保护、异常响应、硬件封缄、接口管控和检查配合等要求完成产品设计生产，排污单位落实日常自查，平台运维单位完善安全审计、风险预警功能。设备生产、使用、监管各相关单位均应落实标准要求，充分发挥标准防范数据篡改伪造、提升环境精细化监管水平的作用。

本标准对监测设备区分新生产设备和在用设备分别规定适用要求。新生产设备自本标准实施之日起即须全面符合本标准要求；在用设备给予一定过渡期，但自本标准实施之日起即不得具有第 6 章所列禁止功能。禁止功能均属于可直接用于篡改、伪造监测数据的功能，与数据真实性直接冲突，不存在整改过渡的合理理由，故要求即时消除。在用设备达到本标准全部要求可能涉及软件升级、硬件改造、物理封缄加装等工作，需要一定实施周期，为此设定过渡期，具体截止日期由标准发布时根据行业实际情况确定。过渡期内，设备生产者应配合完成软件升级和硬件改造，排污单位应结合设备检定、校准或维护周期统筹安排达标工作；过渡期届满后，所有在用设备均应全面符合本标准要求。上述分类管理安排与《生态环境监测条例》《排污单位自行监测管理办法》等关于监测设备不得造成数据失真、应当具备防范篡改伪造功能的要求相衔接，为相关单位履行法定义务提供了明确的技术路径和合理的时间预期。

7 参考文献

[1] 生态环境部办公厅. 关于加强技术防控提升排污单位自行监测质量的通知：环办监测函〔2024〕214 号[Z]. 2024.

[2] 中华人民共和国全国人民代表大会. 中华人民共和国生态环境法典[Z]. 2026.

[3] 中华人民共和国国务院. 生态环境监测条例[Z]. 2025.

[4] 中华人民共和国国务院. 排污许可管理条例[Z]. 2021.

[5] 国家质量监督检验检疫总局、中国国家标准化管理委员会.信息技术 软件工程术语: GB/T 11457—2006 [S]. 北京：中国标准出版社，2006.

[6] 国家市场监督管理总局、国家标准化管理委员会. 计量器具控制软件的通用要求: GB/T 42555—2023 [S]. 北京：中国标准出版社，2023.

[7] 生态环境部. 污染物自动监测监控系统数据传输技术要求: HJ 212—2025 [S]. 北京：中国环境出版社，2025.

[8] 国家市场监督管理总局. 计量器具软件测评指南: JJF 1182—2021 [S]. 北京：中国标准出版社，2021.

[9] 国家市场监督管理总局. 计量器具软件标识通用要求: JJF 2356—2025 [S]. 北京：中国标准出版社，2025.

[10] International Organization of Legal Metrology. Non-automatic weighing instruments - Part 1: Metrological and technical requirements - Tests: OIML R 76-1: 2026 [S]. Paris: OIML, 2026

[11] International Organization for Standardization, International Electrotechnical Commission. Information security, cybersecurity and privacy protection - Evaluation criteria for IT security: ISO/IEC 15408-2: 2026 [S]. Geneva: ISO/IEC, 2026.

[12] International Electrotechnical Commission. Security for industrial automation and control systems - Part 4-2: Technical security requirements for IACS components: IEC 62443-4-2:2019 [S]. Geneva: IEC,2019.

[13] National Institute of Standards and Technology. Security requirements for cryptographic modules: FIPS 140-3 [S]. Gaithersburg: NIST, 2019.