ICS 13.020.10
CCS N 56

团　　体　　标　　准

T/CSES XXXX—XXXX

污染源自动监控（监测）设备软件配置与评估技术规范

Technical specification for software configuration and evaluation of pollutant automatic surveillance (monitoring) equipment

(征求意见稿)

20XX-XX-XX 发布　　20XX-XX-XX 实施

中国环境科学学会　　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　污染源自动监控（监测）设备软件配置总体要求 3

5　污染源自动监控（监测）设备软件配置基本要求 3

6　评估方法和内容 5

附　录　A　（规范性）　污染源自动监控（监测）设备软件配置技术要求 7

附　录　B　（规范性）　污染源自动监控（监测）设备动态密码管理及技术要求 10

附　录　C　（资料性）　污染源自动监控（监测）设备 OTA 升级技术要求 13

附　录　D　（规范性）　污染源自动监控（监测）设备软件配置评估技术要求 17

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这些专利的责任。

本文件由生态环境部环境工程评估中心提出。

本文件由中国环境科学学会归口管理。

本文件起草单位：生态环境部环境工程评估中心、西安长天长软件股份有限公司、北京雪迪龙科技股份有限公司、北京万维盈创科技发展有限公司、安徽皖仪科技股份有限公司、山东汇氏环境科技集团有限公司、安徽环境智能科技有限公司。

本文件主要起草人员：****。

污染源自动监控（监测）设备软件配置与评估技术规范

1 范围

本标准规定了污染物排放自动监测设备软件配置技术要求以及设备软件评估方法和内容。

本标准适用于规范污染物排放自动监测设备的软件功能以及对软件升级和动态密码获取的相关技术要求，指导第三方评估机构对污染源自动监控（监测）设备软件配置技术性能进行试验和评估，并将相关评估结果应用于生态环境管理部门对污染源自动监控（监测）设备实施穿透式监管。

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。

HJ 212 污染物在线监控（监测）系统数据传输标准

HJ 75 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 76 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 1013 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 377 化学需氧量（COD_{Cr}）水质在线自动监测仪技术要求及检测方法

HJ 101 氨氮水质在线自动监测仪技术要求及检测方法

HJ 355 水污染源自动监测系统（COD_{Cr} 、NH_3-N 等）运行技术规范

HJ/T 372 水质自动采样器技术要求及检测方法

HJ 609 六价铬水质自动在线监测仪技术要求

HJ 762 铅水质自动在线监测仪技术要求及检测方法

HJ 763 镉水质自动在线监测仪技术要求及检测方法

HJ 764 砷水质自动在线监测仪技术要求及检测方法

HJ 798 总铬水质自动在线监测仪技术要求及检测方法

HJ 926 汞水质自动在线监测仪技术要求及检测方法

3 术语和定义

下列术语和定义适用于本标准。

3.1

自动监控（监测）设备 automatic surveillance （monitoring） equipment

安装于排污单位监测现场用于直接或间接实施环境监测或污染源监控（监测）的仪器设备，简称现场机，包含数采仪、用电监控、工况监测、视频监控等各类仪器设备。

[来源：HJ 212—20XX（报批稿），3.3]

3.2

数据采集传输设备 equipment of data collection and transmission

采集各种类型监控（监测）仪器仪表的数据、完成数据存储及与上位机数据传输通信功能的单片机、嵌入式计算机、可编程自动化控制器（Programmable Automation Controller，PAC）或可编程序逻辑控制器（Programmable Logic Controller，PLC）等，简称数采仪。

[来源：HJ 212—20XX（报批稿），3.2]

3.3

数据标记 data mark

识别生产设施、污染治理设施的运行工况及现场机工作状态，用字符分类自动标记的操作。

[来源：HJ 212—20XX（报批稿），3.10]

3.4

空中下载技术 Over-the-Air Technology

通过无线网络传输对污染源自动监控（监测）设备软件安装或固件更新的技术，简称 OTA 。

3.5

软件 software

运行在污染源自动监控（监测）设备上的特定应用程序或系统组件的代码、数据和文件等。

3.6

固件 firmware

烧录并存储在硬件上使其运行和控制相应功能的软件。

3.7

升级包 upgrade package

用于更新污染源自动监控（监测）设备的固件或软件的内容及配置信息，以一定格式形成的数据包。

3.8

差分更新 delta update

OTA 的一种更新方法，升级包包含新旧版本之间的差异数据。在污染源自动监控（监测）设备上，通过还原算法将差异部分在原版本上进行还原，以实现升级到目标版本的过程。

3.9

全量更新 full update

OTA 的一种更新方法，升级包包含整个新版本数据。在污染源自动监控（监测）设备上，将整个软件包或模块进行替换，从而完成升级到目标版本的操作。

3.10

回滚 rollback

在升级后的版本未能通过确认或检测时，污染源自动监控（监测）设备恢复到之前的固件或软件版本的过程。

3.11

空中下载服务平台 OTA platform

用于管理和部署 OTA 升级机制的软件服务平台。

3.12

监督见证服务平台 Supervision and authentication service platform

部署于生态环境部污染源监控中心，用于监督和记录污染源自动监控（监测）设备升级过程的软件服务平台。

3.13

完整性验证数据 integrity validation data

用以检测数据或文件中错误或变化的值。

3.14

预升级检查 pre-upgrade check

在开始 OTA 升级之前，检查污染物自动监控（监测）设备的当前状态和条件的过程。

4 污染源自动监控（监测）设备软件配置总体要求

4.1 污染源自动监控（监测）设备一致性要求

4.1.1 污染源自动监控（监测）设备应具备设备唯一标识码。

4.1.2 污染源自动监控（监测）设备唯一标识码（SN 编码）和数采仪设备唯一标识码（ MN 编码 ）的编码规则应符合 HJ 212 规定要求。

4.1.3 设备唯一标识码应当作为工作参数实时上传。

4.1.4 设备唯一标识码应采取安全防御保护机制，防止其被非授权删除和修改。

4.1.5 设备唯一标识码应当在生态环境管理部门的监控信息平台中进行备案。

4.2 具体要求

4.2.1 污染源自动监控（监测）设备软件要求应符合已发布相关技术规范要求，如 HJ 75、HJ 76、HJ 101、HJ/T 372、HJ 377、HJ 609、HJ 762、HJ 763、HJ 764、HJ 798、HJ 926、HJ 1013 等标准规范。

4.2.2 相关技术规范未明确的要求应满足本规范第五章及附录 A 的相关要求。

5 污染源自动监控（监测）设备软件配置基本要求

5.1 污染源自动监控（监测）设备分级权限管理要求

5.1.1 污染源自动监控（监测）设备应至少具有三级操作管理权限，授予用户所需的最小权限，其中管理员具有系统运行参数设置权限，运维人员具有数据查看、日常查询和例行维护权限，具有可调参数调整权限，普通用户具有全部数据、参数、日志的查询和查看权限。

5.1.2 管理员及以上权限的登录密码应采用自动生成的动态形式，可通过生态环境管理部门监控信息平台获取，动态密码管理及技术要求见附录 B 。

5.2 污染源自动监控（监测）设备信号输出要求

5.2.1 污染源自动监控（监测）设备应具有工作参数和工作状态实时显示、实时输出功能。

5.2.2 污染物分析仪应具备数字通信接口或以太网络通信接口。

5.2.3 污染物分析仪应当输出污染物实测浓度，其状态转换、浓度折算以及单位换算等计算过程应在数采仪进行动态展示。

5.3 污染源自动监控（监测）设备日志记录要求

5.3.1 污染物分析仪、水质自动采样器、数采仪、视频监控设备、用电监控设备、工况监测设备应当具备日志记录功能，日志应当记录仪器自动或人为所有操作流程、参数前后变化情况、异常情况报警、程序更新升级情况等内容。

5.3.2 设备应具备记录远程控制指令的日志功能，日志记录的内容至少包括远程控制指令的时间、发送主体、远程控制对象、操作结果等。

5.3.3 设备日志存储时间应不少于 5 年，日志不得因系统升级、更换仪器配件、设备损坏或其他人为干扰等因素丢失。

5.3.4 设备应使用国产密码算法确保日志的真实性和完整性。

5.4 污染源自动监控（监测）设备软件功能要求

5.4.1 污染源自动监控（监测）设备应具备防止人为干扰监测数据的功能，不得具有数据模拟软件、模拟信号发生器、隐藏操作界面，用于过滤数据、限制数据上下限和修改监测数据及设备参数等任何数据造假的功能和漏洞。

5.4.2 污染源自动监控（监测）设备应具备自动标记功能，数据标记应符合《污染物排放自动监测设备标记规则》要求。

5.4.3 污染源自动监控（监测）设备工作状态应当根据设备工作流程自动生成。

5.4.4 污染源自动监控（监测）设备应具备身份识别或访问控制权限，禁用非授权的远程控制指令。

5.4.5 联网传输要求应按照 HJ 212 要求配置，严格按照生态环境主管部门要求开展入网活动；未经生态环境管理部门允许，不得向其他单位、机构或组织传输数据。

5.4.6 污染物分析仪工作参数调整后监测数据变动不应超过 ± 5% F.S（F.S 指分析仪满量程值）。

5.4.7 污染物分析仪校准系数应当采用标准物质校准和调整的方式变更，不可手动变更。

5.4.8 污染物分析仪应当具备校准曲线自动拟合功能，不得人为取舍校准结果进行拟合。

5.4.9 污染源分析仪具备参数异常报警功能，包括但不限于仪器设备设置的固定参数和动态参数。

5.4.10 污染物分析仪工作流程一般情况下不可修改，确需修改的应通过软件更新方式实现。

5.5 污染源自动监控（监测）设备软件升级要求

5.5.1 污染源自动监控（监测）设备软件应具备本地升级和 OTA 升级两种方式。

5.5.2 污染源自动监控（监测）设备生产制造商应建设空中下载服务平台，应符合以下内容：

a）具备接口与数据调阅等功能；

b）具备记录、查询升级包历史信息功能；

c）具备访问监督见证服务平台的能力；

d）能够按照规定的格式、内容向监督见证服务平台上报信息。

5.5.3 污染源自动监控（监测）设备软件升级包，应符合以下要求：

a) 升级包应具有唯一标识，应与空中下载服务平台标识一一对应；

b) 升级包应包含完整性验证数据，如 MD5 校验；

c) 当全量更新的升级包大小超过 100M 时，宜采用差分更新等方式缩小升级包。

5.5.4 污染源自动监控（监测）设备软件升级功能，应符合以下要求：

a) 污染源自动监控（监测）设备应该具备直接或间接互联网通信能力；间接互联网通信能力，应依托数采仪实现；

b) 在软件升级前，应在监督见证服务平台验证升级包真实性和完整性；

c) 在软件升级后，应在监督见证服务平台上报升级信息。

5.5.5 污染源自动监控（监测）设备软件升级安全，应符合以下要求：

a) 软件升级系统应通过安全保护机制，保护设备软件升级系统的可信根、引导加载程序、系统固件不被篡改，或在被篡改后通过安全保护机制使其回滚或恢复出厂设置或无法正常启动；

b) 升级包不应使用包含国家信息安全漏洞共享平台-国家信息安全漏洞库（CNVD-CNNVD）公布的超过 90 d 的高危及以上的安全漏洞第三方库和开源组件；

c) 升级包中不应包含恶意代码，升级包宜采用混淆或者加壳等机制防止直接读取代码；

d) 升级包宜经过漏洞和安全扫描工具的认证；

e) 升级包下载过程中应采用加密传输方式。

5.5.6 污染源自动监控（监测）设备软件发现可被利用篡改监测数据的漏洞时，设备生产制造商应及时进行软件升级封堵。

5.5.7 污染源自动监控（监测）设备软件 OTA 升级时应由运维人员及以上权限确认后方可升级。

5.5.8 用于本地升级的 USB 接口、SD 卡接口应对接入设备中的文件进行访问控制，仅允许读写指定格式的文件或安装执行指定签名的应用软件。

5.5.9 应对非授权的第三方应用的安装进行提示，并对已安装的非授权的第三方应用进行访问控制，限制此类应用直接访问系统等。

5.5.10 采用本地升级的软件应在联网时与空中下载服务平台进行校验。

5.5.11 软件升级数据应具备自动备份功能，且数据存储时间应不少于 5 年。

5.5.12 OTA 升级技术要求见附录 C。

6 评估方法和内容

6.1 评估范围

污染源自动监控（监测）设备软件配置的评估范围包括数据采集传输仪、废气分析仪（包含颗粒物及烟气参数）、水质分析仪、水质自动采样器、废水流量计和水质参数等设备，评估其送测设备软件内容包括但不限于分级权限管理、信号输出、日志记录、软件功能、软件升级和设备一致性等。

6.2 评估使用设备

评估设备主要包括：

a) 污染源自动监控（监测）系统数据模拟平台；

b) 动态密码模拟信息管理平台；

c) 生态环境监管部门监督见证服务模拟平台；

d) 通讯接口测试工具；

e) 数据采集传输设备（用于数采仪以外的设备评估）；

f) 便携式计算机。

6.3 评估方法

6.3.1 污染源自动监控（监测）设备软件配置的评估方法主要包括查阅技术资料、现场勘察、询问、现场操作演示等，具体评估技术要求见附录 D。

6.3.2 污染源自动监控（监测）设备软件功能防篡改评估应遵循行为独立，方法科学、评估准确、结果公正、过程公开的原则。

附 录 A
（规范性）
污染源自动监控（监测）设备软件配置技术要求

A.1 水质自动采样器软件技术要求

A.1.1 分级权限管理

A.1.1.1 应当具备分级权限，各级权限下的功能应符合5.1相关要求。

A.1.2 信号输出要求

A.1.2.1 应当具备工作参数、工作状态输出功能。

A.1.3 日志记录要求

A.1.3.1 日志至少应包含运行日志、操作日志、开门日志、留样日志、报警日志、参数修改记录、断电记录、登录记录、软件升级记录等内容。

A.1.3.2 日志记录内容包括相关操作的用户、时间、事件、数值或状态前后变化情况等。

A.1.3.3 应当具备历史记录查询功能。

A.1.3.4 日志记录不允许被修改或删除。

A.1.4 软件功能要求

A.1.4.1 水质采样器工作流程不得具备被随意更改或关闭功能。

A.1.4.2 不得具有后台隐藏界面（如可修改参数的后台隐藏界面）功能。

A.1.4.3 不得具有人为随意修改关键运行参数（如采样时间、排空时间等）功能。

A.1.4.4 水质自动采样器可依托数采仪网络能力具备 OTA 升级功能的，应符合5.5要求。

A.1.4.5 软件升级记录应当具备查询功能。

A.2 水质分析仪或废水流量计技术要求

A.2.1 分级权限管理

A.2.1.1 应当具备分级权限，各级权限下的功能应符合5.1相关要求。

A.2.2 信号输出要求

A.2.2.1 水质分析仪不得具备限制测量输出上限值功能，最大输出上限等于最大物理量程上限值。

A.2.2.2 废水流量计不得具备限制测量输出上限值功能，最大输出上限等于测量流量装置最大上限值。

A.2.2.3 水质分析仪及废水流量计应当采用数字量输出原始监测数据。

A.2.2.4 水质分析仪及废水流量计应当具备工作参数、工作状态输出功能。

A.2.3 日志记录要求

A.2.3.1 日志存储类型至少应包含运行日志、操作日志、校准日志、报警日志、参数修改记录、断电记录、登录记录、软件升级记录等内容。

A.2.3.2 日志记录内容包括相关操作的用户、时间、事件、数值或状态前后变化情况等。

A.2.3.3 应当具备历史记录查询功能。

A.2.3.4 日志记录不允许被修改或删除。

A.2.4 软件功能要求

A.2.4.1 不得安装有干扰真实监测数据的软件或具备安装此类软件的功能。

A.2.4.2 不得具有后台隐藏界面（如可修改参数的后台隐藏界面）功能。

A.2.4.3 不得具有人为修改关键测量参数（如吸光度值等）功能。

A.2.4.4 依托数采仪的水质分析仪软件具备 OTA 升级功能的，应符合5.5要求。

A.2.4.5 软件升级记录应当具备查询功能。

A.3 废气分析仪软件技术要求

A.3.1 分级权限管理

A.3.1.1 应当具备分级权限，各级权限下的功能应符合5.1相关要求。

A.3.2 信号输出要求

A.3.2.1 不得具备限制测量输出上限值功能，最大输出上限等于最大物理量程上限值。

A.3.2.2 污染物分析仪测量的污染物浓度为湿基浓度时，监测数据应当如实输出，其状态转换计算过程应如实在数据采集传输仪进行展示。

A.3.2.3 污染物分析仪应当采用数字量输出信号，烟气参数可以通过模数转换设备后输出。

A.3.2.4 污染物分析仪应当具备工作参数、工作状态输出功能。

A.3.3 日志记录要求

A.3.3.1 日志存储类型至少应包含运行日志、操作日志、校准日志、报警日志、参数修改记录、断电记录、登录记录、软件升级记录等内容。

A.3.3.2 日志记录内容包括相关操作的用户、时间、事件、数值或状态前后变化情况等。

A.3.3.3 应当具备日志记录历史记录查询功能。

A.3.3.4 日志记录不允许被修改或删除。

A.3.4 软件功能要求

A.3.4.1 不得安装具备干扰真实监测数据的软件（如随机数据模拟软件等）或具备安装此类软件的功能。

A.3.4.2 不得具有后台隐藏界面（如可修改参数的后台隐藏界面）功能。

A.3.4.3 污染物分析仪可依托数采仪网络能力具备 OTA 升级功能的，应符合5.5要求。

A.3.4.4 软件升级记录应当具备查询功能。

A.4 数采仪软件技术要求

A.4.1 分级权限管理

A.4.1.1 应当具备分级权限，在各级权限下的功能应符合5.1相关要求。

A.4.2 软件功能要求

A.4.2.1 应当对用户自行安装软件进行权限控制。

A.4.2.2 安装软件应当留下记录，且记录不可被删除或修改。

A.4.2.3 不得安装除操作系统自带功能之外的软件。

A.4.2.4 不得安装带有随机信息模拟功能的软件。

A.4.2.5 数采仪开机自动运行数据传输软件，不可人为退出。出现意外退出时，应当具备自动重启功能。

A.4.2.6 宜采用无法访问或修改底层应用的操作系统，如 Linux 嵌入式系统；软件数据库、系统参数配置文件不允许被人为修改。

A.4.2.7 数采仪程序软件具备 OTA 升级功能的，升级内容和版本信息应被记录和存储。

A.4.2.8 具备远程扩展功能时，应当保留操作记录日志，且操作记录不可被修改。

A.4.2.9 数采仪不得具备远程修改关键参数功能。

A.4.3 数据处理要求

A.4.3.1 应当采用数字量信号连接分析仪。

A.4.3.2 应当具备工作参数、工作状态查询及上报功能。

A.4.3.3 应当可以查询污染源参数的工况值、标况值、湿基值、干基值、折算值及其计算公式（组态软件变动后应能实时更新，变动记录可查）。

A.4.4 日志记录要求

A.4.4.1 日志存储类型应至少包含参数修改记录、数据补传记录、断电记录、通讯记录、登录记录、受控参数记录、软件升级记录、工作状态记录、修改时间记录。

A.4.4.2 日志记录内容包括相关操作的用户、时间、事件、数值或状态前后变化情况等。

A.4.4.3 应当具备历史记录查询功能。

A.4.4.4 日志记录不允许被修改或删除。

附 录 B
（规范性）
污染源自动监控（监测）设备动态密码管理及技术要求

B.1 动态密码管理一般要求

B.1.1 密码用途

自动监控（监测）设备动态密码的用途如下：

a）动态密码用于管理员对自动监控（监测）设备进行高级设置；

b）动态密码用于执法人员现场监督检查时查询系统信息。

B.1.2 密码管理

自动监控（监测）设备的动态密码应满足以下要求：

a）动态密码由自动监控设备制造商进行管理，并建立动态密码信息平台管控动态密码使用过程，设备制造商对动态密码安全负责；

b）动态密码不应少于6位，应采用国密算法技术，密码不应设置固定值、顺序值、规律值等易于破解的数值；

c）动态密码不应通过任何明文形式传输、转移、存储；

d）每台自动监控（监测）设备均应设置独立的动态密码，动态密码的有效期不超过1小时；

e）动态密码应为一次性密码，登录设备后失效，不可重复使用；

f）动态密码的使用应不依赖于自动监测设备的联网，自动监测设备应在未联网情况下保障动态密码的正常使用；

g）动态密码生产机制应定期更新，更新频次不低于1次/季度。

B.1.3 动态密码使用关键信息

自动监控（监测）设备的动态密码获取（公开）时，应记录以下关键信息：

a）排污单位（运维服务商、设备制造商）需要获取设备动态密码时，动态密码信息管理平台需要识别用户信息，根据排污单位提供的自动监控（监测）设备唯一识别码获取动态密码，信息管理平台应记录的信息包括但不限于以下内容：密码获取途径、获取IP地址、动态密码使用人、发放时间、有效期、用途；

b）生态环境监管部门需要获取设备动态密码时，动态密码信息管理平台应记录监管部门的信息包括但不限于以下内容：密码获取途径、使用人单位、动态密码使用人、发放时间、有效期、用途。

B.2 动态密码共享要求

B.2.1 共享范围

动态密码信息管理平台应建立动态密码共享服务，便于运维单位和监管获取动态密码，共享范围包括自动监控（监测）设备的运维人员，生态环境主管部门的监管人员。

B.2.2 共享方式

动态密码信息管理平台应提供数据接口方式共享动态密码，数据接口需进行安全认证，接口参数应满足以下要求：

a）通信协议采用 HTTPS ，请求方法为 POST ，请求头设置 Authorization 作为认证信息，认证内容为用户名和密码；

b）认证信息加密格式：用户名 +“：”+ 密码，使用 SM4 加密算法（工作模式：ECB，填充模式：PKCS7Padding），加密结果再用Base64编码；

示例：

用户名为：testuser，密码为：AezF0nZRs4kypuGO

密钥为：msbE74gsiSHSEh5eSg3eFT42fDx12GCY

加密后为：AtHbsBF89s+eElU5GrulPPNK8zLlJZYMe9ce59Imlw4=

c）请求参数见表B.1。

表B.1 获取动态密码请求参数表

序号	参数名	参数类型	描述
1	deviceCode	string	自动监控（监测）设备唯一标识
2	cIP	string	获取密钥的IP地址
3	User	string	动态密码使用人
4	purpose	string	用途
5	applicant	string	申请单位
6	getDate	date	密码申请时间：YYYY-MM-DD hh:mm:ss

d）返回参数见表B.2。

表B.2 获取动态密码返回参数表

序号	名称	类型	描述
1	code	string	响应码：0为无错误，1为有错误需要重传，其他为具体错误码
2	success	boolean	返回是否成功
3	msg	string	错误消息内容
4	password	string	动态密码
5	expirationdate	date	密码有效期

B.3 动态密码使用记录共享

动态密码使用关键信息应实时向生态环境部污染源监控中心的监督见证平台同步，同步方式采用数据接口方式，接口认证方式与B2.2相同，请求参数和返回参数分别见表B.3，B.4。

表B.3 共享动态密码使用记录请求参数表

序号	参数名	参数类型	描述
1	manufactorID	string	设备制造商ID
2	model	string	设备型号
3	type	string	设备类别，数采仪1，水分析仪2，气分析仪3，采样器4

序号	参数名	参数类型	描述
4	deviceCode	string	自动监控（监测）设备唯一标识
5	cIP	string	获取密钥的IP地址
6	User	string	动态密码使用人
7	purpose	string	用途
8	applicant	string	申请单位
9	getDate	date	密码申请时间：YYYY-MM-DD hh:mm:ss
10	expirationdate	date	密码有效期

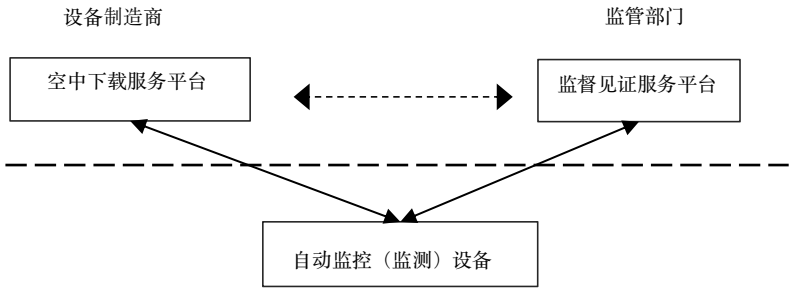
表B.4　　共享动态密码使用记录返回参数表

序号	名称	类型	描述
1	code	string	响应码：0为无错误，1为有错误需要重传，其他为具体错误码
2	success	boolean	返回是否成功
3	msg	string	错误消息内容

附 录 C
（规范性）
污染源自动监控（监测）设备 OTA 升级技术要求

C.1 系统结构

污染源自动监控（监测）设备 OTA 升级技术包括空中下载服务平台、监督见证服务平台、自动监控（监测）设备三部分组成，三部分之间的数据通信依托电信运营商提供的公用互联网服务。结构示意图见图C.1。



图C.1 系统结构示意图

C.2 升级方式分类

C.2.1 按发现机制

根据实现空中下载的机制，污染源自动监控（监测）设备的升级方式可分为以下三类。

a）命令升级：通过污染源自动监控（监测）设备的控制界面或配套的移动应用界面由人工操作发起版本查询，反馈结果并得到确认后开始的空中升级；

b）推送升级：污染源自动监控（监测）设备及其空中下载服务平台在运行中，通过提前设定的机制自动进行版本查询，当有可升级版本时，在污染物自动监控（监测）设备的控制界面或配套的移动应用界面中提示信息，由人工操作，确认后开始的空中升级；

c）静默升级：污染源自动监控（监测）设备及其空中下载服务平台在运行中，通过提前设定的机制，进行版本查询。当有可升级版本时，直接完成对污染源自动监控（监测）设备的升级。

C.2.2 按升级内容

根据更新内容及目标不同可分为固件升级（FOTA）和软件升级（SOTA）。

C.3 空中下载服务平台数据上报要求

软件版本信息和设备升级信息内容应按表C.1和C.2 要求上报。

表C.1 软件版本信息

序号	信息编码	信息项目	类型	长度	备注
1	ModelID	适用于自动监控（监测）设备型号	字符	20	
2	Version	升级版本号	字符	10	
3	VersionNotes	升级版本说明	字符	200	
4	Size	升级包的字节大小	数字	4	单位MB，如：245MB
5	VersionRelease	软件发布时间	字符	50	

表C.2 设备升级信息表

序号	信息编码	信息项目	类型	长度	备注
1	SN	自动监控（监测）设备唯一标识码	字符	24	
2	Version	每次升级版本信息	字符	10	
3	UpgradeTime	每次升级的时间点	字符	14	yyyyMMddhhmmss
4	UpgradeResult	每次升级是否成功	数字	1	成功1；失败0
5	OldVersion	每次升级前的版本信息	字符	10	
6	Notes	每次升级过程的信息记录	字符	200	

C.4 升级过程要求

C.4.1 升级发起阶段

升级包上传至空中下载服务平台，通过命令升级、推送升级或静默升级方式发起 OTA 升级阶段，要求如下：

a）升级包上传至空中下载服务平台时，应与监督见证服务平台备案的升级包进行一致性验证；

b）服务器存储升级包时，应至少包含以下信息：升级包应用的产品类型及版本、升级包更新需要的空间大小、升级包更新的内容；

c）进行 OTA 升级管理时，厂商记录的升级信息应包含以下信息：升级的目的、升级可能影响设备的功能、升级目标设备范围及其最新已知配置和升级兼容性的数据信息、如何执行升级以及执行升级的先决条件；

d）有定时自动发起版本查询的机制时，时间间隔不应超过 24 h ，如定时间隔中有其他查询进行，可顺延计时；

e）发起版本查询，应有重试和超时退出机制，版本查询的结果宜在空中下载服务平台有记录；

f）在版本查询的过程中，污染源自动监控（监测）设备发生断网或电源中断的情况，恢复正常后应能继续或重新进行版本查询。

C.4.2 预升级检查阶段

a）污染源自动监控（监测）设备从空中下载服务平台取得升级包信息，并进行预升级检查的阶段。进入下载阶段前，要求如下：升级包大小不超出污染源自动监控（监测）设备内可用空间；

b）污染源自动监控（监测）设备当前工作状态符合 OTA 升级的状态要求；

c）对于能源供应为电池的污染源自动监控（监测）设备，应明确 OTA 升级所需的电量，污染源自动监控（监测）设备当前电量不应小于 OTA 升级所需电量，宜在显示界面给予保证电量和有效供电的提示；

d）除静默升级外，在固件/软件下载开始前，应具备取消下载动作的功能；

e）预升级检查的结果宜在空中下载服务平台的功能；

f）污染源自动监控（监测）设备执行预升级检查时，应正常工作，不影响用户使用。

C.4.3 下载阶段

污染源自动监控（监测）设备与空中下载服务平台通信，将目标升级包从空中下载服务平台下载到本地并存储的阶段，要求如下：

a）若固件/软件下载会影响污染源自动监控（监测）设备的功能运行，下载前应确认是否中断用户使用，若不符合条件，应启动相应的升级退出或者延时流程，当正在执行有时序要求的任务时（如测量、数据上报、校准等）宜完成当前任务后进行下载；

b）在固件/软件下载阶段，污染源自动监控（监测）设备应在污染源自动监控（监测）设备的控制界面或配套的移动应用界面给予用户升级包下载剩余时间预期的提示，如进行的是局部功能的软件升级（SOTA），不影响控制的基本功能，在用户没有使用该功能时可不予提示；

c）在固件/软件下载阶段，若污染源自动监控（监测）设备出现断网或电源中断的情况，恢复后应保持功能正常；

d）污染源自动监控（监测）设备应将升级包下载的结果上报到空中下载服务平台；

e）若 OTA 升级是在污染源自动监控（监测）设备运行中进行，该固件/软件下载不应影响设备运行安全。

C.4.4 升级安装阶段

污染源自动监控（监测）设备将下载完成的升级包进行安装，并切换为运行固件或运行软件的安装阶段，要求如下：

a）自动监控（监测）设备应对下载的升级包与监督见证服务平台备案的信息进行完整性、一致性校验，若未确认其完整性、一致性，则自动监控（监测）设备应拒绝进行更新；

b）自动监控（监测）设备安装前应确认是否会中断用户使用，若不符合条件，应启动相应的升级退出或者延时流程，当正在执行任务时（如测量、数据上报、校准校验等，或时间间隔有既定的要求）宜完成当前任务后完成升级；

c）在执行安装时，应在自动监控（监测）设备本地的控制界面或配套的移动应用界面给予用户升级剩余时间的提示，如进行的是局部功能的 软件升级（SOTA），在用户没有使用该功能时可不予提示；

d）升级完成后应验证以下内容：验证升级后的版本号与升级包的版本号一致、验证功能设备是否正常运行，验证不通过的应该回滚或恢复出厂设置；

e）切换安装的结果，应上报到空中下载服务平台和监督见证服务平台。

C.5 升级的其他要求

OTA 升级环节还应遵循以下要求：

a）当生产具有软件升级功能的设备时，设备制造商应具备软件升级管理体系；

b）对于每次软件升级，设备制造商应记录并存储相关升级信息，该信息至少应保存至设备停产后 5 年；

c）本地升级或 OTA 升级，升级前均应自动在监督见证服务平台查询升级包是否备案；

d）升级活动包括但不限于修改软件Bug、增加功能、排除监测数据篡改风险；

e）所有的升级活动应向监督见证服务平台进行备案；

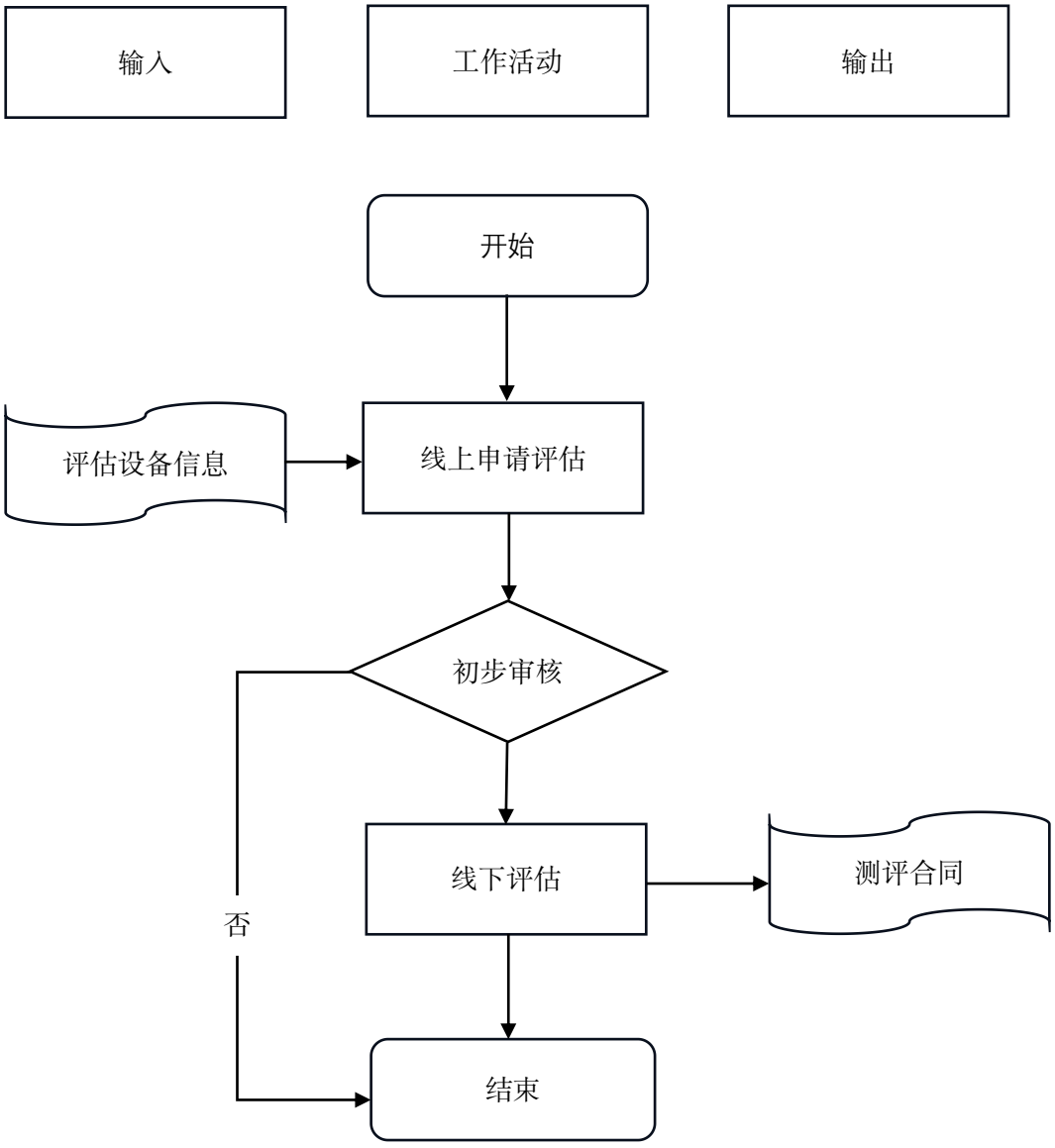
f）每次软件升级信息通知给设备用户。若因设备硬件原因无法通过设备系统告知用户的，设备制造商应证明其具备合理技术措施实现信息告知。

附 录 D
（资料性）
污染源自动监控（监测）设备软件配置评估技术要求

D.1 评估工作流程

D.1.1 评估申报线上填报工作流程

评估申报线上填报工作流程如下图D.1所示。



D.1 评估申报线上填报工作流程图

线上申报需要的评估设备信息如下表D.1所示。

表D.1 设备评估申报信息表

类别	评估设备信息	备注
基本信息	厂家基本信息	包含厂家生产资质、营业执照、产品认证证书等
	评估设备基本信息	包含设备型号、出厂日期、设备原理
	评估设备软件基本信息	包含软件版本、功能说明等
操作手册	评估设备操作手册	电子版操作手册
随机清单	随机硬件、软件清单	硬件设备清单明细、预装软件清单明细（包含：软件数据库类型、软件安装位置、路径、功能说明，软件操作说明，版本号等）
操作权限	各级权限操作账号	提供不同权限操作账号（用户、管理员以及管理员账号）
厂家申明	厂家提供一致性声明承诺书	厂家需提供送测产品与在售产品一致性的承诺说明

注：以上均需提供中文版

D.2 评估准备

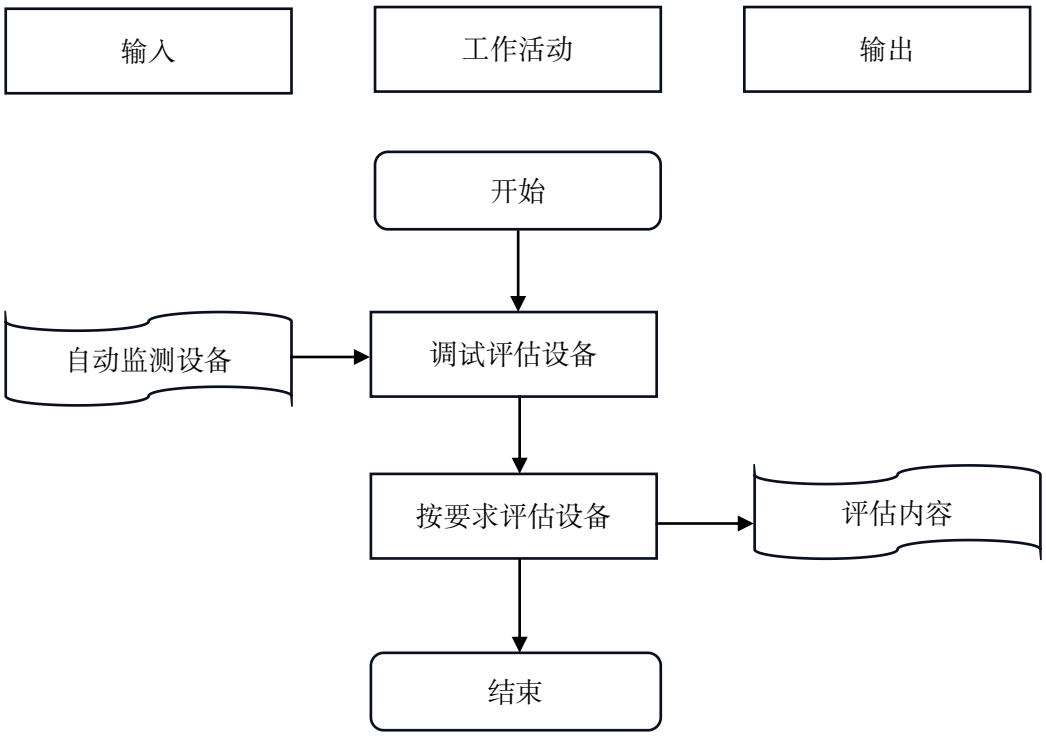
D.2.1 检查污染源自动监控（监测）设备各部件，调整设备至正常工作状态；检查被评估设备的软件版本是否为正式版。

D.2.2 将污染源自动监控（监测）设备与污染源自动监控（监测）系统数据模拟平台连接；数采仪以外的设备可以使用评估机构提供的数采仪进行连接。

D.2.3 测试污染源自动监控（监测）设备是否正常工作，与污染源自动监控（监测）系统数据模拟平台、生态环境监管部门监督见证服务模拟平台连接是否正常。

D.2.4 污染源自动监控（监测）设备投入自动采样，稳定运行3个工作日后开始进行评估工作。

D.2.5 污染源自动监控（监测）设备软件功能防篡改评估工作流程如下图D.2所示。



D.2 评估工作流程图

D.3 评估内容

污染源自动监控（监测）设备软件配置评估内容具体见下表D.2。

表D.2 设备评估内容表

序号	评估项目	功能要求	检查方法
1	设备一致性要求	污染源自动监控（监测）设备应具备设备唯一标识码。	查阅生产制造厂提供的技术资料或通过询问的方式确定设备是否具备唯一标识码。
2		污染物分析仪 SN 设备编码应当作为工作参数实时上传。	检查上报的通讯报文中是否上报 SN 码和 MN 码
3		污染源自动监控（监测）设备的污染物分析仪唯一标识码（SN 编码）和数采仪设备唯一标识码（MN 编码）规则应符合 HJ 212 规定要求。	查看设备 SN 编码和数采仪 MN 编码结构是否符合 HJ 212 相关要求
4		设备唯一标识码应采取安全防御保护机制，防止其被非授权删除和修改。	根据设备 SN 编码和 MN 码存储地址，使用软件分析工具非授权删除和修改存储在设备内的 SN 编码和 MN 编码数据，判定设备是否满足要求。
5		设备唯一标识码应当在生态环境管理部门的监控信息平台中进行备案。	出具在生态环境管理部门的监控信息平台获取或备案的相关证明材料。
6	权限管理要求	设备应具有三级管理权限（普通用户，运维人员以及管理员），且各级权限下的功能应符合5.1.1相关要求。	检查设备权限分级情况，调阅每个权限下操作权限是否符合5.1.1相关要求。
7		管理员及以上权限的登录密码应采用自动生成的动态形式，动态密码管理技术要求应符合附录 B 相关要求。	通过动态密码模拟信息管理平台获取动态密码，检查获取的密码是否符合附录 B 相关要求。
8	信号输出要求	污染源自动监控（监测）设备应具有工作参数和工作状态实时显示、实时输出功能。	使用通讯接口测试工具读取设备输出信号，查看结果是否具备工作参数和工作状态；比对现场读取结果与数采仪和污染源自动监控（监测）系统数据模拟平台中查询的结果是否一致。
9		污染物分析仪应具备数字通信接口或以太网络通信接口。	检查设备的通讯接口是否具备数字量通讯接口或以太网络通信接口。
10		污染物分析仪应当输出污染物实测浓度，其状态转换、浓度折算以及单位换算等计	查看分析仪输出结果是否为实测浓度；修改计算公式查看公式展示界

		算过程应在数采仪进行动态展示。	面是否变动，修改后计算结果是否与人工计算结果一致；调阅单位换算公式是否正确。
11	日志记录要求	污染物分析仪、水质自动采样器、数采仪、视频监控设备、用电监控设备、工况监测设备应当具备日志功能，日志应当记录仪器自动或人为所有操作流程、参数前后变化情况、异常情况报警、程序更新升级情况等内容。	将污染源自动监控（监测）设备分别置于自动和手动测量状态各测量连续测量48小时和对所有工作流程手动测试后，检查设备日志是否记录完整；进行修改设备参数、模拟设备故障、更新设备程序等操作，检查设备日志是否记录完整。
12		设备应具备记录远程控制指令的日志功能，日志记录的内容至少包括远程控制指令的时间、发送主体、远程控制对象、操作结果等。	触发设备远程控制功能，检查是否存在安全日志，安全日志记录的内容是否包含远程控制指令的时间、发送主体、远程控制对象、操作结果等信息。
13		设备日志存储时间应不少于5年。	检查日志记录的时间跨度是否不少于5年或是否具备日志留存不少于5年的能力。
14		日志不得因系统升级、更换仪器配件、设备损坏或其他人为干扰等因素丢失。	通过系统升级、更换仪器配件等方式查看日志记录是否丢失或是否具备日志记录恢复的能力。
15		设备应使用国产密码算法确保日志的真实性和完整性。	根据设备内存储的日志清单及存储的地址，通过通讯调试接口篡改、伪造修改日志文件，检查是否可伪造、篡改该文件。
16		各类设备日志记录要求应符合附录 A 相关要求。	按照附录 A 相关要求逐一测试。
17	软件功能要求	污染源自动监控（监测）设备应具备防止人为干扰监测数据的功能，不得具有数据模拟软件、模拟信号发生器、隐藏操作界面，用于过滤数据、限制数据上下限和修改监测数据及设备参数等任何数据造假的功能和漏洞。	根据设备应用清单逐一测试软件功能是否具备模拟数据、隐藏界面、修改数据等篡改、伪造监测数据的功能。
18		污染源自动监控（监测）设备应具备自动标记功能，数据标记应符合《污染物排放自动监测设备标记规则》要求。	将污染源自动监控（监测）设备置于《污染物排放自动监测设备标记规则》表 1 状态下，使用通讯接口测试工具读取设备输出信号中工作状态代码是否符合标记规则要求

			，同时查看污染源自动监控（监测）系统数据模拟平台标记内容是否符合要求。
19		污染源自动监控（监测）设备工作状态应当根据设备工作流程自动生成。	检查污染源自动监控（监测）设备显示的工作状态是否与实际工作状态一致；手动操作切换设备状态，查看设备是否进入对应工作状态。
20		污染源自动监控（监测）设备应具备身份识别或访问控制权限，禁用非授权的远程控制指令。	使用非授权用户向污染源自动监控（监测）设备发送远程指令，查看设备是否能被远程操作。
21		联网传输要求应按照 HJ 212 要求配置，严格按照生态环境主管部门要求开展入网活动；未经生态环境管理部门允许，不得向其他单位、机构或组织传输数据。	查看污染源自动监测（监控）系统数据模拟平台接收到的历史报文，数据格式是否符合 HJ 212 要求；开启设备全部移动蜂窝通信通道和 WLAN 通信通道，依次模拟测试设备处于未上电、仅上电、数采仪未上电、数采仪仅上电数据传输功能正常启用的状态，并使用网络数据抓包工具对外通信网络通道同时抓包，且总抓包时长不少于3600 s，解析通信报文数据，检查目的 IP 地址中是否包含模拟平台 IP 地址，判定设备是否满足要求。
22		污染物分析仪工作流程一般情况下不可修改，确需修改的应通过软件更新方式实现。	进入各级权限查看是否具备更改设备工作流程功能；根据被评估机构或组织提供软件组态软件等工具，检查设备工作流程是否具备防篡改能力。
23		污染源自动监控（监测）设备具备参数异常报警功能，包括但不限于仪器设备设置的固定参数和动态参数。	根据被评估机构或组织提供的系统参数合理范围文档，测试人员通过直接修改或者间接修改的方式，查看设备是否具备超范围异常报警功能。
24		污染物分析仪应当具备校准曲线自动拟合功能，不得人为取舍校准结果进行拟合。	通过检查污染物分析仪曲线自动拟合功能，查看设备是否具备人为取舍校准结果再拟合的功能。
25		污染物分析仪工作参数调整后监测数据变动不超过 ± 5% F. S。	调整工作参数记录监测结果前后变化是否超过 ± 5% F. S。

26		污染物分析仪校准系数应当采用标准物质校准和调整的方式变更，不可手动变更。	登录污染物分析仪各级用户，查看设备校准系数是否能够人为修改。
27	软件升级要求	污染源自动监控（监测）设备软件应具备本地升级和 OTA 升级两种方式。	查看污染源自动监控（监测）设备是否具备本地升级和 OTA 升级方式。将被评估机构或组织提供的升级包校验信息备份至生态环境监管部门监督见证服务模拟平台中，使用本地升级和 OTA 升级分别测试是否满足要求。
28		设备生产制造商应建设满足需求的空中下载服务平台。	测试升级功能时同时验证设备制造商的空中下载服务平台是能够满足5.5.2要求。
		污染源自动监控（监测）设备软件升级包是否符合5.5.3要求。	对被评估机构或组织提供的升级包进行模拟升级，对照5.5.3测试升级包是否符合要求。
29		污染源自动监控（监测）设备软件升级功能是否符合5.5.4要求。	查看设备是否具备直接或间接互联网通信能力。采用间接互联网通信的，使用评估机构提供的数据采集传输设备进行测试；对升级包进行篡改，查看设备是否能够验证发现问题；升级软件后查看监督见证服务平台是否按照附录C.3要求上报信息。
30		污染源自动监控（监测）设备软件升级安全是否符合5.5.5要求。	设备生产制造商操作演示升级篡改后升级包的回滚功能；查看第三方库和开源组件是否存在高危及以上的安全漏洞；提供不适用存在安全漏洞的证明材料；测试升级包下载过程是否经过加密传输。
31		污染源自动监控（监测）设备软件发现可被利用篡改监测数据的漏洞时，设备生产制造商应及时进行软件升级封堵。	设备生产制造商提供发现可被利用篡改监测数据的漏洞时，积极采取措施的承诺书。
32		软件 OTA 升级时应由运维人员及以上权限进行确认后方可升级。	测试升级功能时同时查看设备是否具备确认升级功能。
33		用于本地升级的 USB 接口、SD卡接口应对接入设备中的文件进行访问控制，仅允许读写指定格式的文件或安装执行指定签名的应用软件。	根据设备制造商提供的 USB 接口、SD 卡接口的总结文档或 USB 接口、SD 卡接口支持的文件类型清单，分别在具备 USB 接口、

			SD 卡接口的移动存储介质中注入指定格式文件、指定签名的应用软件和其他非指定格式文件和非指定签名的应用软件，将移动存储介质分别连接到设备 USB 接口、SD 卡接口，尝试执行非指定格式文件和非指定签名的应用软件，判定设备是否满足要求。
34		设备应对非授权的第三方应用的安装进行提示，并对已安装的非授权的第三方应用进行访问控制，限制此类应用直接访问系统等。	根据被评估机构或组织提供已授权的第三方应用，使用工具篡改其代码，并安装、执行篡改后的授权第三方应用，判定设备是否满足要求。若篡改后的授权第三方应用无法安装或被限制访问超出访问控制权限的资源，视为应用非正常运行，满足要求。
35		OTA 升级技术要求应符合附录 C 相关要求。	使用被伪造、被篡改的升级包，使用离线升级工具将该升级包下载或传输到现场端，执行本地或远程升级，判定设备是否满足要求。
36	设备其他要求	污染源自动监控（监测）设备软件要求应符合已发布相关技术规范要求，如 HJ 76、HJ 101、HJ 102、HJ 103、HJ/T 372、HJ 377、HJ 1013 等标准规范。	按照 HJ 76、HJ 101、HJ 102、HJ 103、HJ/T 372、HJ 377、HJ 1013 以及附录A的要求查看设备是否满足相关要求。
37		相关技术规范未明确的要求应满足本规范第五章及附录A的相关要求。	