附件 3

中华人民共和国国家计量技术规范

JJF XXXX-202X

固定污染源连续监测系统的数据可信度技术规范

Technology Specification for Data Trusted Level of Continuous Monitoring System of Fixed Pollution Sources

(征求意见稿)

xxxx - xx - xx 发布　　xxxx － xx - xx 实施

国家市场监督管理总局 发布

固定污染源连续监测系统的数据可信度技术规范

JJF XXX—XXXX

Technology Specification for Data Trusted Level of Continuous Monitoring System of Fixed Pollution Sources

归 口 单 位： 全国生态环境监管专用计量测试技术委员会

主要起草单位：

参加起草单位：

本规范委托全国生态环境监管专用计量测试技术委员会负责解释

本规范主要起草人：

×××（）

×××（）

×××（）

参加起草人：

×××（）

×××（）

×××（）

×××（）

目　　录

引　言

JJF 1001-2011《通用计量术语及定义》、JJF 1071-2010 《国家计量校准规范编写规则》、JJF 1032-2005《光学辐射计量名词术语及定义》和 JJF 1059.1-2012《测量不确定度评定与表示》共同构成支撑本规范制定工作的基础性系列规范。

本规范为首次制定。

固定污染源连续监测系统的数据可信度

技术规范

1. 范围

本规范适用于安装在固定污染源自动监测系统的数据可信度的技术要求和测评。具体对象包括仪器、仪表、数据采集传输功能模块等的数据可信度，其他与数据可信度相关的系统软硬件的技术要求和测评可参照本规范。

2. 引用文件

本规范引用了下列文件：

HJ 75 固定污染源烟气（SO2、NOx、颗粒物）排放连续监测技术规范

HJ 76 固定污染源烟气（SO2、NOx、颗粒物）排放连续监测系统技术要求及检测方法

HJ 1286 固定污染源废气 非甲烷总烃连续监测技术规范

HJ 1263 固定污染源废气 苯系物的测定 气袋采样/直接进样-气相色谱法

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 1243 固定污染源废气 非甲烷总烃连续监测系统安装技术规范

HJ/T 397 固定源废气监测技术规范

HJ/T 92 水污染物排放总量监测技术规范

HJ 212 污染物连续监控（监测）系统数据传输标准

HJ 355 水污染源连续监测系统（CODCr、NH3-N 等）运行技术规范

HJ 354 水污染源连续监测系统（CODCr、NH3-N 等）验收技术规范

JJF 1585 固定污染源烟气排放连续监测系统校准规范

JJF 1965 固定污染源碳排放连续监测系统校准规范

JJF 1206 时间与频率标准远程校准规范

GB/T 25069 信息安全技术 术语

GB/T 32905 信息安全技术 SM3 密码杂凑算法

GB/T 32918.2 信息安全技术 SM2 椭圆曲线公钥密码算法 第 2 部分:数字签名算法

GB/T 32918.3 信息安全技术 SM2 椭圆曲线公钥密码算法 第 3 部分:密钥交换协议

GB/T 32918.4 信息安全技术 SM2 椭圆曲线公钥密码算法 第 4 部分:公钥加密算法

GB/T 35276 信息安全技术 SM2 密码算法使用规范

GB/T 20520 信息安全技术 公钥基础设施 时间戳规范

GB/T 25056 信息安全技术 证书认证系统密码及其相关安全技术规范

GB/T 42570 信息安全技术 区块链技术安全框架

凡是注日期的引用文件，仅注日期的版本适用于本规范；凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本规范。

3. 术语和定义

下列术语适用于本规范

3.1 固定污染源 fixed pollution sources

通常是指向环境排放或释放有害物质或对环境产生有害影响的场所、设备和装置。

3.2 固定污染源连续监测系统

用于连续监测固定污染源排放颗粒物或者气体污染物或者水污染物排放浓度和排放量所需要的全套监测设备。

[来源：HJ 75-2017，3.3，有修改]

3.3 计量溯源性 metrological traceability

通过文件规定的不间断的校准链，测量结果与参照对象联系起来的特性，校准链中的每项校准均会引入测量不确定度。

[来源：JJF 1001-2011，4.14]

3.4 量值传递 dissemination of the value of quantity

通过对测量仪器的校准或检定，将国家测量标准所实现的单位量值通过各等级的测量标准传递到工作测量仪器的活动，以保证测量所得的量值准确一致。

[来源：JJF 1001-2011，9.60]

3.5 测量结果的计量可比性 metrological comparability of measurement results

简称计量可比性（metrological comparability）。

对于可计量溯源到相同参照对象的某类量，其测量结果间可比较的特性。

[来源：HJ 75-2017，5.35]

3.6 有效数据 valid data

符合本标准的技术指标要求， 经验收合格的 CEMS， 在固定污染源排放烟气条件下，CEMS 正常运行所测得的数据。

[来源：HJ 75-2017，3.5]

3.7 可信度 trustable level

对象所具有的必要的信任。

3.8 数据可信度 data trustable level

从数据的采集、传输和计算等环节评价的可信度。

3.9 可信时间 trustable time

经计量溯源具有一定不确定度水平的时间。

3.10 时间戳 time stamp

使用数字签名技术产生的数据,签名的对象包括了原始文件信息、签名参数、签名时间等信息 TSA 对此对象进行数字签名产生时间戳,以证明原始文件在签名时间之前已经存在。

[来源：GB/T 20520-2006，3.1]

3.11 杂凑值 hash value

杂凑算法作用于一条信息时输出的消息摘要（比特串）。

[来源：GB/T 32905-2016，2.4]

3.12 数字签名 digital signature

附加在数据单元上的一些数据，或是对数据单元做密码变换，这种附加数据或密码变换被数据单元的接收者用以确认数据单元的来源和完整性，达到保护数据，防止被人（例如接收者）伪造的目的。

[来源：GB/T 25069-2022，3.576]

3.13 CA 证书 CA certificate

由一个 CA 给另一个 CA 签发的证书，一个 CA 也可以为自己签发证书，这是一种自签名的证书。

[来源：GB/T 25056-2018，3.1]

3.14 可信视频 trusted video

具有可信度的视频。可采用但不限于时间戳技术、数字签名技术、CA 证书技术等可信技术对视频进行加密实现。

3.15 防篡改 tamper resistant

指对象具有判断是否被篡改的特性。

3.16 防抵赖 repudiation resistant

指对象具有判定发送者的特性。

3.17 数据可追溯 data traceability

指数据具有可判断其来源的特性。

3.18 数据加密 data encryption

对数据进行密码变换以产生密文的过程。

[来源：GB/T 39786-2021，3.5]

3.19 区块链 blockchain

将区块顺序相连，并通过共识协议、数字签名、杂凑函数等密码学方式保证的抗篡改和不可伪造的分布式账本。

[来源：GB/T 42570-2023，3.2]

4. 概述

固定污染源连续监测系统的数据可信度是监测数据质量的关键，与系统中数据采集仪器的计量特性共同决定了系统的数据质量。因此对于连续监测系统的计量监督，必须实施系统的数据可信度的测评。数据可信度主要从数据是否被篡改、是否能够防抵赖和是否可追溯三个方面进行测评。实现数据可信度的技术主要有时间戳、CA 证书和数字签名。因此对于固定污染源连续监测系统的数据可信度的计量监督，主要是通过对系统时间戳、CA 证书和数字签名的测评，判断系统是否具有防篡改、防抵赖和可追溯的功能。

5. 系统的数据可信度技术要求

5.1 系统组成与架构

具备数据可信度的固定污染源连续监测系统，须在数据的采集、传输和处理三个单元嵌入可信技术模块。可信技术模块包括但不限于时间戳、CA 证书、数字签名、数据加解密、区块链模块等。

5.2 系统的数据

系统的数据须包括采集数据、可信字段数据。采集数据是由系统中采集设备（单元）获取的数据，可信字段数据是由可信技术模块加工的数据，包括但不限于时间戳、CA 证书、数字签名、数据加解密、区块链数据等。

5.3 数据时间可信度技术要求

采集数据中的时间字段数据是否经过计量是（采集）数据时间可信度的标识，须是可信时间，其计量特性需符合 5.10.1 要求。

5.4 防篡改可信度技术要求

防篡改可信度的可信数据包括但不限于如下种类，须具备其中一种或几种。

1) 数字签名数据；

2) 加密数据；

3) 区块链数据。

5.5 防抵赖可信度技术要求

防抵赖可信度的可信数据包括但不限于如下种类，须具备其中一种或几种。

1) 时间戳数据

产生时间戳数据的时间戳服务器需通过“国家商用密码产品认证”。时间戳服务器具有证书管理、权限控制、时间戳签发、时间戳验证、时间同步、日志审计等功能，具备对国密 SM2、SM3 的算法支持。可对外提供精准时间戳应用接口服务。

2) CA 证书数据

发放 CA 证书数据的 CA 机构需获得由国家密码主管机构-国家密码管理局颁发密码许可证和国家工业和信息化部颁发《电子认证服务许可证》。

5.6 数据可追溯的技术要求

防抵赖可信度的数据可以是日志存储，也可以是其他技术。

日志存储数据须具有连贯性，存储空间能够满足一定时期的数据保存。例如半年以上。

5.7 数据加密的技术要求

1) 数据加密的密码器件（硬件）要求

须通过“国家商用密码产品认证”。密码器件可以是但不限于智能密码钥匙、TF 密码卡。密码器件具有数据加密、签名/验证、密钥对生成及管理、CA 证书存储及管理、Hash 运算、真随机数生成等功能，并具备对国密 SM2、SM3 的算法支持、具备内部密钥对私钥不可导出的特性。可用于身份认证、数据加密、PKI 应用等领域。通过应用密码器件内部密钥对（私钥不可导出）生成的 CA 证书，证书内部包含所绑定硬件设备或身份鉴别对象的标识信息，从而使密码器件具备身份认证的特性。

2) 密码器件服务程序（软件）要求

密码器件服务程序运行在密码器件所绑定的硬件设备的操作系统中，基于密码器件对外提供功能接口报备。并具备如下功能特征：

a) 与对的密码器件相绑定：程序启动时或进行接口的调用时检测对应密码器件的序列号或连续状态，根据序列号或连续状态的合法性控制服务程序是否向外提供接口服务；

b) 与对应的硬件设备或身份鉴别对象相绑定：程序启动时或进行接口的调用时读取硬件设备或身份鉴别对象标识信息与 CA 证书中的信息进行比对, 根据比对结果的合法性控制服务程序是否向外提供接口服务；

c) 接口访问采用 https 通信协议或其他具备传输加密和身份认证的通信协议；

d) 接口被调用时需具备身份验证和权限控制机制;

e) 提供 CA 证书信息读取、数字签名、签名验证等接口;

f) 具有完备的日志审计功能;

5.8 数据安全可信传输技术要求

数据安全可信传输程序/模块用于在数据的发送端和数据接收端建立安全的数据传输通路，并应用时间戳服务器和密码器件服务程序提供的功能接口对数据进行封包和拆包，以确保传输数据的真实可信。

数据安全可信传输程序/模块，应具备如下功能特征：

a) 数据发送端和数据接收端采用 https 通信协议或其他具备传输加密和身份认证的通信协议;

b) 数据封包：数据发送端对原始数据块进行时间戳签注。数据发送端对原始数据块或原始数据块+时间戳数据块的数据组合进行基于密码器件服务程序的数字签名。数据发送端将原始数据块+时间戳数据块+签名数据块（含证书信息）进行组合封包。

c) 数据拆包：数据接收端对接收到的数据包进行解析，还原出原始数据块、时间戳数块、签名数据块，根据对应的证书信息调取 CA 证对签名块进行验证。根据原始数据块哈希值和时间戳数据块，访问时间戳服务器的验证接口进行时

间戳验证。

5.9 可信视频的技术要求

视频是固定污染源连续监测系统中常用的可信监测手段。监测视频须具有可信度。可信视频需具备上述 5.3-5.8 的技术要求。

5.10 系统计量特性要求

5.10.1 系统时间的计量校准

系统中的时间均需经过计量校准，成为可信时间。 可信时间的准确性以时间偏差和计量不确定度表示。一般应满足：

平均时间偏差：0.1 ms；

不确定度：1.3ms（k=2）。

5.10.2 系统采集设备的计量校准

固定污染源连续监测系统中，用于烟气排放连续监测的系统，进行数据采集的设备各主要计量特性，在非工况状态下应满足 JJF 1585 中表 1 要求，在工况状态下应满足 JJF 1585 中表 2 要求。

6. 系统数据可信度测评要求

首次出厂上市的固定污染源连续监测系统，应对其进行数据可信度的测评。

经测评满足 5.3-5.10 要求（其中 5.9 为可选项）的固定污染源连续监测系统，可以判断为合格。不满足其中一项的，即判定为不合格。

对固定污染源连续监测系统进行数据可信度测评的机构应具有相关检测项的 CNAS 认可和 CMA 认证。

7. 系统数据可信度测评方法

7.1 硬件测评

7.1.1 系统时间测评方法

系统时间（含时间戳服务器）的测评按 JJF 1206、GB/T 20520 相关方法执行。

7.1.2 密码器件测评方法

密码器件的测评根据功能种类按 GB/T 32905、GB/T 32918、GB/T 35276、GB/T 25056 相关方法执行。

7.1.3 采集设备的测评方法

接入系统的采集设备的测评根据照设备种类，按照相应标准的相关方法执行。这些标准包括但不限于 HJ 75 、HJ 76 、HJ 1286、HJ 1013 、HJ/T 397 、HJ/T 92 、HJ 355、HJ 354、JJF 1585。

7.2 软件测评

7.2.1 黑盒模式

采用人工审查的方式，针对用户界面，基于程序的业务逻辑和系统功能点，进行逐个排查可能存在的数据可信度功能缺陷。黑盒测试有两种不同的方法，一种是定向功能分析法，该方法主要是根据程序的业务逻辑来审计的，根据系统的相关功能，大概推测可能存在哪些漏洞。常见功能漏洞：（包括但不限于）程序初始安装、站点信息泄漏、文件上传、管理、登录认证、权限管理、数据库备份恢复、找回密码、验证码；另一种方法是功能点人工审计，这是对系统某个或某几个重要的功能点进行人工审计，发现功能点存在的安全问题。功能点人工审计需要收集系统的设计文档、系统开发说明书等技术资料，以便审计人员能够更好的了解系统业务功能。由于人工审计的工作量极大，所以需要分析并选择重要的功能点，有针对性的进行人工代码审计。

7.2.2 白盒模式

白盒模式采用代码审计的方法，采用工具审计与人工审计（人工代码审计、人工审查工具审计结构、人工抽取代码检查）相结合，针对具体的代码进行检测。使用工具进行代码审，需要导入代码到测试环境，按预定代码策略进行审计，过滤代码审计结果，将漏洞进行分组（按漏洞类型，按功能模块）。使用人工审计时，一方面是基于工具测试的结果，分析和撰写相应的测试代码，结合人工检查找出工具发现的漏洞中不确定和存在误报的漏洞，另一方面是确认问题代码覆盖的范围，深入分析发现的漏洞，并分析漏洞在当前系统中的严重等级（也可按不同的标准如：OWASP，PCI 等）和代码引用的资源文件。白盒测

试有两种不同的方法，一种是整体代码审计，审计人员对被审计对象的所有代码进行整体审计，代码覆盖率 100%；另一种是敏感函数参数回溯法 (shell_exec)，即根据敏感函数逆向追踪参数传递的过程，大多数代码漏洞的产生是因为函数的使用不当导致，只要找到这样一些使用不当的函数，就可以快速挖掘对应的漏洞。

白盒模式测评等级高于黑盒模式。

8. 系统数据可信度的后续监管

经测评判定为数据可信度合格的固定污染源连续监测系统，如果在数据采集、传输和计算任一环节做了变更，均应再次对系统进行数据可信度测评。

经测评判定为数据可信度合格的固定污染源连续监测系统，如果使用者或者监管机构对系统的数据可信度产生质疑，也可对系统进行数据可信度测评。

附录 A

固定污染源连续监测系统数据可信度测评方法示例

某工厂烟气排放点新安装一套用于固定污染源烟气排放连续监测的系统，现对其工况下数据可信度进行测评。测评过程如下：

1) 对系统的组成和架构进行确认

经现场核查，该系统由五种测量数据采集设备（颗粒物、气态污染物、氧、流速、温度、湿度（水分含量））和数据传输（专网传输）、数据处理模块组成，使用了四种数据可信技术（时间戳、CA 证书、数字签名、数据加解密）。

2) 对系统的数据进行确认

经现场核查，该系统的数据包括了采集数据、可信字段数据。采集数据包含了颗粒物、气态污染物、氧、流速、温度、湿度（水分含量）五种数据，可信字段数据包括了时间戳、CA 证书、数字签名、数据加解密数据五种数据。数据协议为自定义格式。

3) 数据时间可信度测评

采集 10 次系统数据数据，计算其平均值，与时间戳服务器（具有国家计量院计量证书）的标准时间的平均偏差为：0.08 ms；

评估其不确定度：1.1ms（k=2）。符合 5.10.1 要求。

4) 防篡改可信度测评

该系统可信字段数据中包含了数字签名数据和加密数据，符合 5.4 的要求。

5) 防抵赖可信度测评

该系统可信字段数据中包含了时间戳数据和 CA 数据。其中时间戳服务器具有“国家商用密码产品认证”。 CA 证书数据由中国计量科学研究院发放。满足 5.5 的要求。

6) 数据可追溯测评

该系统具有日志存储，且具有连贯性，存储空间能够满足一年的数据保存。满足 5.6 的要求。

7) 数据加密测评

该系统使用的密码器件（硬件）是智能密码钥匙，通过了“国家商用密码

产品认证”。密码器件服务程序（软件）为自编，按照 7.2.2 代码审计的方法对其进行了审计。均满足 5.7 的要求，风险等级为低。

8) 数据安全可信传输测评

该系统使用专网传输，按照 7.2.2 代码审计的方法对其传输模块进行了审计，满足 5.8 的要求，风险等级为低。

9) 系统采集设备计量测评

经现场核查，系统中的五种测量数据采集设备（颗粒物、气态污染物、氧、流速、温度、湿度（水分含量））均具有有效计量证书，在工况状态下均满足 JJF 1585 中表 2 要求。

测评结论：根据以上 9 项测评，该系统数据可信度结论整体评估为合格，风险等级为低风险，该测评结论仅对本次所检测的系统有效。

附录 B

固定污染源连续监测系统数据可信度测评结果报告格式（参考）

固定污染源连续监测系统数据可信度测评结果报告（推荐）格式-原始记录

记录编号		证书编号			
送检单位					
系统名称					
型号/信息		出厂编号			
开发厂商					
客户地址					
测评日期		检测员		核验员	
测评所依据的技术文件（代号、名称）： JJF XXX-XXXX 固定污染源连续监测系统数据可信度技术规范					
检测环境条件及地点					
温 度:	℃	地点			
湿 度:	%RH	其他			
检测使用的标准/工具					
名 称	测评范围	编号	对应数据集	备注	
				A 黑盒审计 B 白盒审计 C 人工审计 D 工具审计	
测评结果					

序号	测评项目		测评结果				
	类	子类	模块单元	行号/对象	结果	合格与否（或风险等级）	备注
1	5.4	5.4.1					
2		5.4.1					
3		5.4.1					
4		5.4.2					
5	5.5	5.5.1					
6		5.5.1					
7		5.5.2					
8		5.5.3					
9							

10							
测评结论							
根据以上 X 项分项测评结果，该系统数据可信度结论整体评估为 X，风险等级为 X 风险，该测评结论仅对本次所检测的系统有效。							