ICS 91.140
CCS P 47

团 体 标 准

T/CEATEC XXX—2025

物联网智能燃气调压器数据安全规范

Data safety specification for IoT intelligent gas regulator

（征求意见稿）

2025-XX-XX 发布 2025-XX-XX 实施

中国欧洲经济技术合作协会 发 布

目　　次

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专利的责任。

本文件由中国欧洲经济技术合作协会提出并归口。

本文件主要起草单位：。

本文件主要起草人：。

本文件为首次编制。

物联网智能燃气调压器数据安全规范

1 范围

本文件规定了物联网智能燃气调压器数据安全的总体要求、数据分类与安全级别、数据传输安全、数据存储与访问控制、安全审计与运维和应急处置。

本文件适用于采用物联网技术（如NB-IoT、LoRa、4G/5G等）的智能燃气调压器（以下简称“调压器”）及其关联系统的数据安全管理。其他燃气物联网设备可参照执行。

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。

GB 27790 城镇燃气调压器

GB/T 34037 物联网差压变送器规范

GB/T 36951 信息安全技术 物联网感知终端应用安全技术要求

GB/T 37025 信息安全技术 物联网数据传输安全技术要求

GB/T 37092 信息安全技术 密码模块安全要求

3 术语和定义

GB 27790界定的及下列术语和定义适用于本文件。

3.1

物联网智能燃气调压器 IoT intelligent gas regulator

具备对压力、流量、温度等参数进行采集、存储、远程传输及智能调控功能，并通过有线或无线通信方式（如物联网专网、互联网）实现数据交互的燃气调压装置。

4 总体要求

4.1 物联网智能燃气调压器数据安全应遵循安全性、可靠性、可用性和可维护性的原则，构建覆盖数据全生命周期（包括数据采集、传输、存储、处理、交换和销毁）的安全防护体系。安全防护体系的构建宜参考 GB/T 37025 中关于物联网安全框架的指导原则。

4.2 数据安全防护应基于数据分类分级（见第 5 章）实施，对不同级别的数据采取相适应的保护措施。

4.3 系统应实现端到端的安全防护，涵盖感知层（智能调压器终端）、网络层（通信网络）和应用层（主站管理平台）。感知终端的安全技术应符合 GB/T 36951 的相关要求

4.4 智能调压器及其关联系统在设计与实现时，应遵循隐私保护原则，在收集和处理用户数据前应明确告知目的并获取授权，仅收集实现功能所必需的最小化数据。

4.5 涉及密码技术时，其应用与管理应符合国家密码管理相关规定及 GB/T 37092 的要求。

4.6 应建立并维护数据安全管理体系，明确安全职责，定期进行安全风险评估与审计，并制定相应的应急处置预案。

5 数据分类与安全级别

5.1 数据分类原则

物联网智能燃气调压器产生的数据应根据其重要性、敏感性和泄露后可能造成的影响，进行科学分类与分级管理。分类方法可参考GB/T 34037中关于数据类型的划分原则。

5.2 数据分类与安全级别要求

数据分类与安全级别应符合表1的规定。

表1 数据分类与安全级别

数据类别	示例	安全级别	保护要求
设备标识数据	设备 ID、序列号、固件版本	一般数据	确保完整性，防止非法篡改。
工艺参数数据	进口/出口压力、流量、温度、设备状态（开/关）	重要数据	确保完整性、保密性；传输和存储过程中宜采取防篡改和加密措施。其准确性应符合 GB 27790 中对参数测量的相关要求。
控制指令数据	阀门开关指令、压力设定值指令	敏感数据	确保高强度的机密性、完整性和不可否认性；应进行双向身份认证，并采用安全算法加密保护。
安全告警与日志数据	泄漏报警、压力异常、非法访问尝试、操作日志	敏感数据	确保高强度的完整性、机密性和可用性；应严格防篡改、防删除，并安全存储以备审计。
用户隐私数据	用户标识、地理位置信息（若关联）	敏感数据	应严格遵循隐私保护原则，进行脱敏或匿名化处理；收集和使用前须获得用户明确授权。

6 数据传输安全

6.1 通信协议安全

6.1.1 智能调压器与主站平台之间传输重要和敏感数据时，宜采用TLS、DTLS等安全通信协议，或在应用层实现等效的安全机制。相关安全技术要求应符合GB/T 37025的规定。

6.1.2 使用受限应用协议时，应配置安全模式；使用消息队列遥测传输（MQTT）时，应使用基于证书或预共享密钥的认证加密。

6.1.3 对于采用非IP网络的通信，应在应用层启用加密和消息认证码机制。

6.2 数据完整性保护

6.2.1 重要和敏感数据在传输过程中应进行完整性校验，可使用散列函数或数字签名技术，以防止数据在传输中被篡改。

6.2.2 系统在检测到数据传输完整性被破坏时，应能启动数据重传机制或立即触发安全告警。

6.3 数据保密性

6.3.1 敏感数据（如控制指令）必须使用国家密码管理部门核准的加密算法进行加密处理。

6.3.2 密钥管理应符合GB/T 37092的要求，建立完善的密钥生成、存储、分发、更新和销毁机制。

6.4 可用性与抗重放攻击

6.4.1 传输的数据单元中应包含有效的时间戳或序列号，以支持新鲜性校验，抵御数据重放攻击。

6.4.2 在通信网络中断的情况下，智能调压器宜具备本地数据缓存能力，并在通信恢复后支持断点续传。

7 数据存储与访问控制

7.1 身份认证

7.1.1 智能调压器接入网络或访问主站平台时，应进行身份认证，确保接入实体的合法性。
7.1.2 身份认证机制应根据安全级别选择，宜支持以下一种或多种方式组合：
a）基于口令的认证：应采用强口令，并定期更换。口令存储应加密，传输应受安全协议保护；
b）基于数字证书的认证：宜采用国家密码管理部门核准的数字证书进行双向认证，适用于高安全等级场景；
c）基于令牌的认证：可支持一次性密码（OTP）或更安全的多因素认证（MFA），以提高认证强度。
7.1.3 主站平台管理端的登录，对管理员及进行关键操作的人员宜采用双因素认证.

7.2 访问控制

7.2.1 应实施基于角色的访问控制（RBAC）机制，依据用户角色（如系统管理员、运维人员、监控员）分配最小必要权限。
7.2.2 访问控制策略应清晰定义，并实现以下控制：
a）角色权限分配：权限应与角色关联，用户通过被授予角色来获得权限；
b）权限细化：应能对不同角色设置对设备数据（如实时数据、历史数据、配置参数、控制指令）的读、写、执行等不同级别的操作权限；
c）默认拒绝：新注册用户或未配置权限的资源默认应拒绝访问。
7.2.3 对于复杂的、动态的授权决策需求，可结合基于属性的访问控制（ABAC）模型，综合考虑用户属性、资源属性、环境条件等因素。

7.3 会话管理与审计

7.3.1 认证成功后建立的会话应具有合理的超时时间，并具备防重放攻击机制。
7.3.2 所有身份认证尝试（成功与失败）、权限变更、关键数据访问及控制指令下发等操作应被完整记录，日志应受到保护，防止非授权删除和篡改，为安全审计提供依据。

8 数据留存与销毁

8.1 数据留存

8.1.1 应制定数据留存策略，明确不同类型数据（如设备运行数据、告警日志、用户操作日志）的保存期限。安全事件审计数据的存储时间不应少于90天。
8.1.2 重要数据（如工艺参数、安全告警）和敏感数据（如控制指令记录）应采取安全可靠的备份措施，至少制作两份备份，并异地保存，以确保数据的可用性和完整性。
8.1.3 承载数据的存储介质（如硬盘、闪存）应定期进行状态检查与维护。对于磁性载体，宜每满2年进行一次抽样机读检验；对于光盘，宜每满4年进行一次抽样检验，发现问题应及时采取数据恢复或迁移措施。

8.2 数据销毁

8.2.1 应建立数据销毁策略和操作规程，明确销毁触发条件（如超过留存期限、设备报废、业务终止）和审批流程。
8.2.2 数据销毁应彻底，确保数据不可恢复。销毁方法应根据介质类型和数据敏感级别选择：
a）逻辑删除：对于非敏感数据，可进行覆盖写入或执行安全擦除命令；
b）物理销毁：对于存储敏感数据的介质，在报废或转作他用时，应采用物理消磁、破碎等方式彻底销毁。
8.2.3 数据销毁过程应记录日志，内容包括销毁时间、数据类型、销毁方法、操作人员及审批信息。涉及敏感数据的销毁，应有监督机制。
8.2.4 数据销毁活动，特别是批量销毁或涉及重要、敏感数据的销毁，应进行安全风险评估

9 安全审计与运维

9.1 安全审计

9.1.1 系统应记录详细的安全审计日志，内容至少包括：用户登录/登出、权限变更、关键控制指令下发、数据传输失败、密钥更新、系统配置更改及安全告警事件。
9.1.2审计日志本身应受到保护，防止未授权的读取、修改和删除。

9.2 安全运维

9.2.1 应制定并执行定期的安全运维计划，包括对系统漏洞的扫描、评估与修复。对数据传输安全性的测试可参照GB/T 37025规定的方法执行。
9.2.2 每12个月宜对系统中使用的数据传输协议、加密算法和核心组件进行一次安全审定，及时发现并修复潜在的安全漏洞。
9.2.3 宜建立安全威胁预警机制，对系统运行状态进行实时监控，对频繁登录失败、异常流量、非工作时间访问等异常行为进行检测和告警。

10 应急处置

10.1 安全事件响应

当发生数据泄露、系统遭受网络攻击等安全事件时，应立即启动应急处置预案，其措施包括但不限于：阻断受影响的通信链路、隔离异常设备或系统模块，并启动安全事件追溯与分析机制。

10.2 应急控制与恢复

10.2.1 智能调压器应具备远程应急控制能力，如在确保安全认证的前提下，支持远程锁定或安全关闭，防止恶意操控。恢复操作需经过严格的身份验证与审批流程。
10.2.2 应制定业务连续性计划，确保在安全事件发生后，能尽快恢复系统的正常功能，并将对燃气供应的影响降至最低。
10.2.3 安全事件处理完毕后，应进行复盘总结，完善安全防护措施和应急预案。