ICS ##.###.##

P ##

CGAS

团　　体　　标　　准

T/CGAS ###-20##

物联网智能燃气表数据安全规范

Specification for data security of IoT smart gas meter

（征求意见稿）

####-##-## 发布　　####-##-## 实施

中国城市燃气协会 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》给出的规则起草。

本文件的内容包括范围、规范性引用文件、术语和定义、安全技术框架、主站安全技术、智能燃气表安全技术、数据格式、检测要求及附录。

本文件由中国城市燃气协会提出并归口。

本文件起草单位：

本文件起草人：

物联网智能燃气表数据安全规范

1　范围

本文件规定了物联网智能燃气表系统中安全技术框架、主站安全技术、智能燃气表安全技术、数据格式及检测要求。

本文件适用于采用物联网技术的智能燃气表。

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/T 22239 信息安全技术 网络安全等级保护基本要求

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

GB/T 39786 信息安全技术 信息系统密码应用基本要求

GB/T 41816-2022 物联网 面向智能燃气表应用的物联网系统技术规范

GM/Z 0001

3　术语和定义

下列术语和定义适用于本文件。

3.1

主站 master station

物联网智能燃气表的管理中心，管理数据传输、处理、应用及安全，由管理系统和通信设备的集合构成。提供业务逻辑运算与定制化展示、数据收发与通信、数据保存与安全处理、系统运维等相关管理功能。

3.2

物联网联接管理平台 IoT connectivity management platform

联结通讯网络和主站的功能实体，提供联接管理、设备管理、用户识别卡管理及业务使用等功能。

3.3

物联网智能燃气表 IoT smart gas meter

利用物联网通信技术的燃气计量仪表，表具可以和主站通信。

3.4

安全单元（SE）security element

具有密钥管理、加解密、数据处理及安全存储功能的芯片单元。

3.5

表号 meter number

按照一定规则编制要求生产，在燃气表出厂时设置的唯一编码。

3.6

公钥 public key

非对称密码算法中可公开的密钥。

3.7

私钥 private key

非对称密码算法中只能由拥有者使用的不公开密钥。

[来源：GB/T 25069-2022,3.580]

3.8

非对称密码算法 asymmetric cryptography algorithm

加密和解密使用不同密钥的密码算法。其中一个密钥(公钥)可以公开，另一个密钥(私钥)必须保密，且由公钥求解私钥是计算不可行的。

3.9

国密算法 State Commercial cryptography algorithm

由国家密码管理部门组织制定的以国家标准形式颁布的商用密码算法。

3.10

数字签名 digital signature

签名者使用私钥对待签名数据的杂凑值做密码运算得到的结果，该结果只能用签名者的公钥进行验证，用于确认待签名数据的完整性、签名者身份的真实性和签名行为的抗抵赖性。

3.11

重放攻击 replay attacks

攻击者通过记录通信会话，以便日后某个时刻重放整个或部分会话的主动攻击方式。

[来源：GB/T 25069-2022,3.78]

3.12

防重因子 anti-replay factor

为了保证报文不可重放，而引入的可使通信内容变化的报文数据段。

3.13

抗抵赖性 non-repudiation

也称不可否认性，证明一个已经发生的操作行为无法否认的性质。

[来源：GB/T 25069-2022,3.321]

3.14

密钥管理系统 Key Management System，KMS

是专门为安全单元设计开发的软硬件系统集，用于管理各类密钥的产生、存储、备份、恢复及销毁等功能，实现密钥的全生命周期的安全管理。包括 KMS 发行程序、KMS 数据库服务器、发行读写器、SAM 卡等。

3.15

消息鉴别码 message authentication code,MAC

消息鉴别码算法的比特串。

[来源：GB/T 25069-2022,3.660]

4 安全技术框架

4.1 总体框架

数据安全包括主站对设备接入的身份认证、数据采用的安全保护机制、密钥的安全管理；智能燃气表对数据的安全管理；以及主站和智能然气表之间数据交互的安全机制。总体框架如图1。

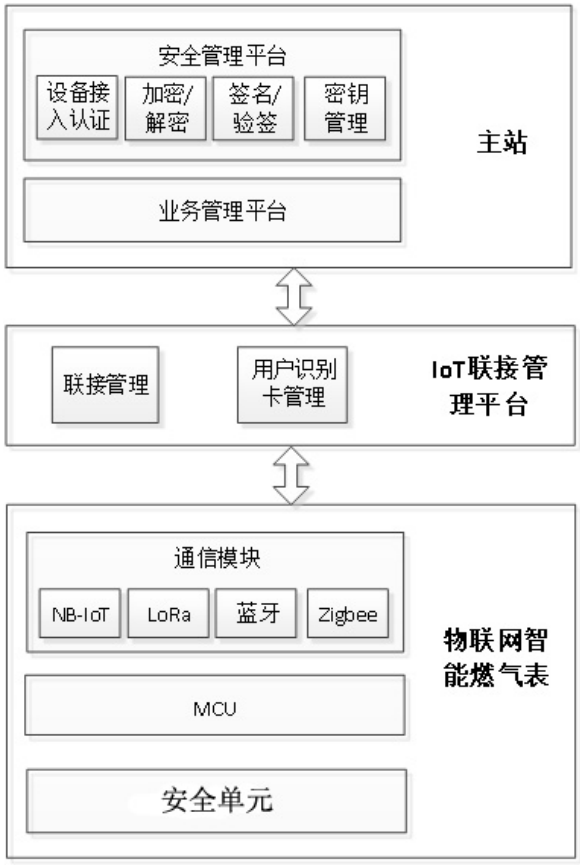

图1 总体框架

4.1.1 主站

负责燃气表的注册、安全接入，数据的加密、解密、签名、验签运算，密钥和敏感数据的安全存储和管理。

4.1.2 IoT 联接管理平台

负责燃气表的联接管理和用户识别卡管理，并且负责燃气表和主站之间数据的透传。

4.1.3 物联网智能燃气表

由微控制单元（MCU）、通信模块和安全单元构成。安全单元负责燃气表关键数据的安全存储，上行数据的加密、完整性计算、签名等操作，下行数据的解密、完整性校验、数字签名等操作。

4.2 核心参数

4.2.1 安全单元证书

安全单元证书用于标识安全单元，即燃气表身份的、符合 X.509 DER 格式的唯一数字证书。安全单元证书是由国家授权 CA 签发或自建、每一个燃气表安全单元在初始化时以安全方式将该证书以及对应私钥导入。

4.2.2 主站证书

4.2.2.1　数字证书是由CA签发的绑定实体身份信息和公钥信息的数据结构，其本身并不含有私钥，所以使用证书进行签名的说法欠精准，建议修改措辞。

4.2.2.2　需要澄清SE初始化写入的是“主站证书的公钥”还是完整的“主站证书”，从后文证书发行来看，SE中导入的是完整的主站证书。

4.2.3　数据上报根密钥

数据上报根密钥为对称密钥，安全单元使用该密钥产生数据上报时的会话密钥。会话密钥的产生可以包括随机数、时间戳等信息。

4.2.4　数据下传根密钥

数据下传根密钥为对称密钥，主站使用该密钥产生数据下传时的会话密钥。会话密钥的产生可以包括随机数、时间戳等信息。

4.2.5　SE 密钥更新密钥

SE密钥更新密钥为对称密钥，主站使用该密钥产生SE时的会话密钥。会话密钥的产生可以包括随机数、时间戳等信息。

4.3　分级要求

4.3.1　数据分级原则

物联网智能燃气表数据安全分为基本级和增强级两类。处理一般性数据时应满足基本级安全要求，处理重要数据、敏感信息以及涉及重要安全问题的数据时应该满足增强级安全要求。具体可根据身份、行为和能力三个属性进行评估，如下：

a）　身份属性明确数据主体身份，依据为身份完整性，具体包括智能燃气表硬件设备、引导程序、配置文件、操作系统等不被篡改。

b）　行为属性明确数据行为特性，依据为安全性（密钥信息、加密强度），可用性（燃气表状态、计量准确度、时间延迟），可靠性（丢包率、误码率、故障率）等。

c）　能力属性明确数据能力等级，依据为安全能力，包括数据完整性保护能力、数据保密性能力，数据容错能力，数据泄露补救能力等。

4.3.2　基本级数据安全

基本级数据主要为智能燃气表状态数据，包括但不限于状态监测与统计、燃气表提示信息、报警信息。

基本级数据传输时主站应对燃气表进行身份认证，并保证数据的可用性和完整性。

4.3.3　增强级数据安全

a）　增强级数据主要为智能燃气表配置数据和控制对象数据，包括但不限于阀门控制、充值、计费、调价、参数配置、密钥更新。

b） 增强级数据应存储在安全单元内且满足一定权限后才能对数据进行修改、删除等操作，数据传输时应采用非对称算法实现燃气表端与主站的双向身份认证，并采用具有一定强度的加密算法保证数据的保密性和抗抵赖性。

5 主站安全技术

5.1 主站框架

主站包括安全管理平台和业务管理平台，安全管理平台由CA系统、设备接入认证系统以及KMS系统组成。主站框架如图2。

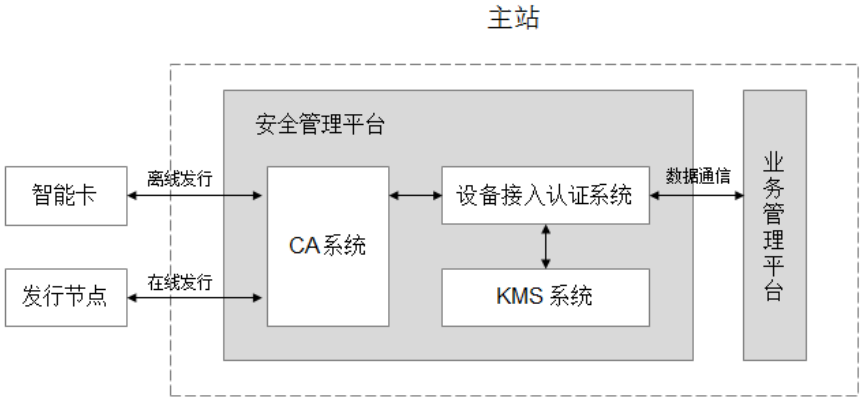

图2 主站框架

5.1.1 CA 系统

负责发行燃气表或者主站证书，支持离线发行以及在线发行两种方式，支持对证书的全生命周期管理。

5.1.2 设备接入认证系统

负责对接入燃气表进行身份鉴别，具备对数据的加解密以及签名验签能力。

5.1.3 KMS 系统

支持对密钥的全生命周期管理。

5.2 通用要求

主站中使用的密码技术应遵循相关国家标准和行业标准；主站中使用的密码产品、密码服务如加密机、加密卡、KMS 系统、CA 等应符合法律法规的相关要求。

5.3 安全机制

密钥及证书需存储于加密设备和 KMS 系统中，待加密、待签名的数据通过加密设备加密、签名后，下传到智能燃气表；待解密、待验签的数据通过加密设备解密、验签后发送到主站业务管理平台。

5.3.1 证书发行

可通过符合国密要求的 CA 系统发行燃气表或者主站证书。CA 系统应对证书生命周期进行管理。证书发行支持在线和离线两种方式。

a） 在线发行：发行系统与发行节点通过双向身份认证，建立发行系统、发行节点、安全单元的安全通道。发行系统将安全单元证书和主站证书下发到发行节点，发行节点把证书发行到燃气表安全单元。

b） 离线发行：安全单元证书、主站证书存储在智能卡等安全载体中，终端私钥在初始化阶段通过安全方式从智能卡中导入到安全单元中，同时导入安全单元证书和主站证书。

5.3.2 接入认证

a） 主站与燃气表正式数据传输前，需要通过双向身份认证。

b） 燃气表用自身私钥签名上行数据，主站收到数据后使用燃气表的公钥验签。主站使用主站私钥签名下行数据，燃气表收到数据后使用主站的公钥验签。若失败，则接入认证不通过。

c） 若主站内的安全管理平台与业务平台部署在不同的网络域，应通过证书或者账号密码实现接入认证。

5.3.3 数据传输

a） 主站与智能燃气表在通过双向身份认证后，可协商出会话密钥。会话密钥为对称密钥，具备有限的生命周期。在会话密钥的生命周期结束后，主站与智能燃气表需再次双向身份认证并重新协商会话密钥。一般上下文交互报文可采用会话密钥进行加密传输。

b） 关键数据的上行报文，燃气表可使用自身安全单元私钥进行签名后上传，主站使用智能燃气表的安全单元证书进行验签。

c） 关键数据的下行报文，主站可使用私钥进行签名后下传，智能燃气表使用主站安全单元证书进行验签。

d） 数据的传输报文添加序号、随机数、时间戳等新鲜性标识，防止数据重放攻击。

e） 由于物联网终端资源的限制，每个终端设备可利用一对公私钥实现加密、解密、签名及验签操作。

f） 燃气表注册、燃气数据上传以及燃气表数据指令下传安全流程中的数据传输内容详见附录 A。

5.3.4 密钥管理

a） 密钥采用根密钥、工作密钥、业务密钥三级密钥体制，工作密钥由根密钥进行加密保护，业务密钥由随机数生成并直接对业务数据进行加密保护，生成业务密钥的随机数由工作密钥进行加密传输。在典型的燃气物联网系统中，根密钥为加密设备中最高级别的密钥，工作密钥为主站私钥，业务密钥为会话密钥。

b） 主站使用加密设备及 KMS 系统进行密钥的全生命周期管理，包括密钥的生成、存储、分发、导入、导出、使用、备份、恢复、归档、销毁等环节。加密设备宜采用双机部署，保障密钥管

理系统的热冗余以及高可用性。

6 智能燃气表安全技术

6.1 智能燃气表组成

智能燃气表由通信单元、人机交互单元、计量传感单元、阀控单元、主控单元以及安全单元组成，见图 3。

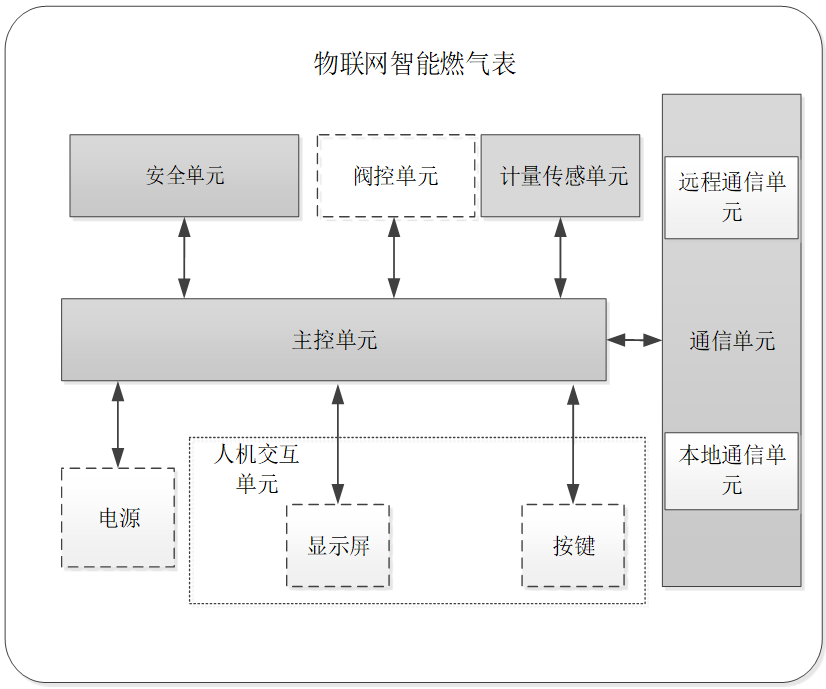

图 3 智能燃气表组成

6.2 安全相关方说明

6.2.1 智能燃气表制造系统

在智能燃气表生产过程中，“燃气表制造系统”需要和智能燃气表进行通信，完成智能燃气表身份信息、参数的初始化工作。

6.2.2 智能燃气表现场维护系统

智能燃气表在出厂后，“燃气表现场维护系统”通过燃气表的本地通信单元和燃气表进行包括但不限于数据读取、参数设置等操作。

6.2.3 燃气公司运营管理系统

“燃气公司运营管理系统”应能够处理来自智能燃气表的数据，进行数据管理，并提供智能燃气表管理的相关操作接口。

注：本文给出的安全相关方从功能方面给出说明，实际应用中安全相关方的名称可以与本文给出的不一致。

6.3 安全技术

6.3.1 安全机制

6.3.1.1 智能燃气表生命周期管理

a） 智能燃气表应具有“厂内模式”和“出厂模式”两种生命周期状态。

b） 智能燃气表生命周期状态应存储在安全单元中，由安全单元提供专用接口进行修改。

c） 在“厂内模式”下，“燃气表制造系统”有权限将智能燃气表生命周期状态修改为“出厂模式”。

d） 在“出厂模式”下，需要有“燃气公司运营管理系统”合法签名的指令才能将智能燃气表生命周期状态修改回“厂内模式”。

6.3.1.2 智能燃气表标识信息保护

智能燃气表标识信息应存储在安全单元中，且仅在智能燃气表处于“厂内模式”下可以修改。

6.3.1.3 敏感数据保密

远程通信时需要对敏感数据采用安全单元进行加密，保证敏感数据在传输过程中不被非法窃听。敏感数据可由制造商与用户共同商定。

6.3.1.4 关键操作权限认证

关键操作权限认证应符合以下要求：

a） 智能燃气表中与法定计量相关参数（不可任意修改的参数，如累积量）的修改、充值、调价及由主站进行阀门的控制，属于关键操作。

b） 智能燃气表经安全单元和主站认证成功后，才执行关键操作。认证失败后，则拒绝执行。

c） 智能燃气表的关键参数应存储在安全单元的内部安全存储区中，由安全单元执行对关键参数的修改动作。

d） 认证过程中，应要根据不同的场景，设定安全要求，并使用相应的安全等级的密码技术进行安全加固。

e） 当要求具备“不可否认性”时，应使用数据签名进行合法性验证。

f） 当未要求具备“不可否认性”时，可使用消息鉴别码（MAC）进行合法性验证。

g） 在“厂内模式”下，智能燃气表生产厂商具有修改表内的关键参数、标识信息等数据的权限。

h） 在“出厂模式”下，关键操作应由“燃气公司运营管理系统”认证的指令进行执行，或由“燃气表现场维护工具”在“燃气公司运营管理系统”授权认证的情况下进行执行。

6.3.2 安全功能

6.3.2.1 通用要求

智能燃气表应符合以下要求：

a） 应支持采用国家密码管理机构核准的密码算法，宜采用国密标准 SM2、SM3、SM4 以及 SM9 算法；

b） 应使用安全单元实现安全存储、数据加/解密、身份认证等安全控制功能；

c） 应支持多种文件类型：透明二进制文件、记录文件、密钥文件；

d） 应支持多种安全访问方式和权限；

e） 安全单元应支持安全数据传输，保证数据的保密性、完整性、抗抵赖性；

f） 应支持侵入式、半侵入式和非侵入式防护机制。

g） 安全单元在出厂时应完成初始化，包括加载固件、预置根密钥、导入主站公钥及相应的安全单元证书。

h） 初始化时应为安全单元设置唯一设备可信标识，标识一旦写入应不可修改。

6.3.2.2 累积量保护

a） 在安全单元中应配置具有累积量计算器，用于计算并存储累积量。安全单元提供该计算器的增量值接口给智能燃气表的“计量传感单元”。智能燃气表的“计量传感单元”在累积量数据更新时，传递增量值给安全单元进行累积量计算。

b） 累积量计数器在智能燃气表“出厂模式”下应单向增长。

6.3.2.3 指令防重放

为了防止攻击者重复发送一个接收方已接收的通信数据，协议报文中应引入防重因子，防重因子可设计单向递增或递减特性，智能燃气表通过检测主站下发报文中防重因子特性来实现指令防重，应实现以下要求：

a） 智能燃气表生成的报文应不会重复；

b） 智能燃气表应能够识别并过滤掉重放的报文；

c） 发送数据时，防重因子应由安全单元直接生成并打包到待发送数据中；

d） 接收数据时，防重因子应由安全单元直接从接收到的数据中提取，进行维护和检查。

7 数据格式

7.1 通信协议

7.1.1 概述

本文件通信协议是基于TCP、UDP、CoAP、HTTP/HTTPS等网络传输协议，对终端设备到数据采集系统间的应用层通信协议进行了规范。本协议缺省高字节在前，即大端格式。

7.1.2 帧格式

帧是数据信息传输的基本单元，帧应包含起始符、数据帧总长度、控制字、数据标识码、数据域、CRC校验码和结束符，具体内容见表1。

表 1 帧格式定义表

名称	字节数	备注	
起始符	1	固定常量 0x68，标识一帧信息的开始	
数据帧总长度	2	从（包含）数据帧总长度到（包含）结束符之间的字节数。	
协议代码	1	1 字节 Hex 码，取值范围 0~255	
协议版本	1	1 字节 Hex 码，取值范围 0~255	
控制字	1	Bit7	指令交互类型，值分为 1 和 0。 1：上行指令，指远传表向采集系统发出的指令； 0：下行指令，指采集系统向远传表发出的指令。
		Bit6	有后续帧标识，1：有后续帧；0：无后续帧；
		Bit5 | Bit0	指令控制码
数据域	n	内容根据控制字和数据标识码而变化。	
CRC 校验码	2	从（包含）数据帧总长度到（包含）数据域，CRC16 校验。	
结束符	1	固定常量 0x16，标识一帧的结束。	

7.1.3 通信指令

7.1.3.1 注册上行指令

由终端设备发起，用于终端设备与采集系统交换注册信息，注册帧上行指令如表 2 所示。

表 2 注册上行帧格式

项目	说 明
运算规则	报文采用的运算，明文+MAC
功能控制字	注册请求上行报文
计数器	报文计数器
报文随机数	上行报文随机数
燃气表号	BCD 码
安全单元 ID	ID 标识
密钥信息	报文密钥
附加报文	注册包携带的附加报文，密文或者明文格式。
MAC	MAC 认证码

其中附加报文由表端 MCU 提供，明文原文内容如表 3：

表 3 明文原文内容

项目	说 明
RSRP	信号接收功率，无线信号强度的关键参数。有符号整数。
SINR	信号与干扰加噪声比。有符号整数。

ECL	ECL 覆盖等级。有符号整数。
CellId	BCD 码，最多 12 位，不足高位补 0。
REAL_NEARFCN	实际接入频点。无符号整数。
IMEI	BCD 码，15 位，不足高位补 0，模组号
IMSI	BCD 码，长度不足 15 位，高位补 0，移动用户识别码

7.1.3.2　注册下行指令

注册帧下行指令如表 4 所示。

表 4 注册下行帧格式

项目	说　明
运算规则	报文采用的运算，密文+签名
功能控制字	注册请求下行报文。带附加报文。
同步计数器	报文计数器
报文随机数	报文随机数
密钥信息	报文加密对称密钥索引
附加报文	注册应答报文携带的附加报文，密文或者明文格式。
MAC	MAC认证码。MAC认证错误的报文将被丢弃。

7.1.3.3　数据对象推送（上行）指令

上行报文的数据格式，如表 5：

表 5 指令上行报文的数据格式

项目	说　明	产生方
运算规则	报文采用的运算	安全单元
功能控制字	普通上行报文	安全单元
计数器	报文计数器	安全单元
报文随机数	上行报文随机数	安全单元
数据报文	报文密文或者明文格式	表端MCU-->安全单元
MAC	MAC认证码	安全单元

普通上行报文，可包含多个控制对象

表 6 指令普通上行报文控制对象

项目	长度	说　明
数据对象个数	1	请求的数据对象个数
1数据对象ID	2	参考附录 数据对象标志码
1数据对象	X1	
2数据对象ID	2	参考附录 数据对象标志码
2数据对象	X2	
……		
N数据对象ID	2	参考附录 数据对象标志码
N数据对象	Xn	

7.1.3.4　数据对象访问请求（下行）指令

普通下行报文的数据格式，如表 7：

表 7 请求指令普通下行报文数据格式

项目	说　明	生成方
运算规则	报文采用的运算	安全服务
功能控制字	普通下行功能控制	安全服务
计数器	报文计数器	安全服务
报文随机数	上行报文随机数	安全服务
数据报文	报文密文或者明文格式	采集服务-->安全服务
MAC或签名	MAC认证码或签名数据	安全服务

普通下行报文，安全单元解析后明文返回给远传表，报文可包含多个目标数据对象：

表 8 请求普通下行报文目标数据对象

项目	长度	说　明
数据对象个数	1	操作的数据对象个数
1数据对象ID	2	参考附录 数据对象标志码
1数据对象	X1	写、读命令包含，读命令不包含
2数据对象ID	2	参考附录 数据对象标志码
2数据对象	X2	写、读命令包含，读命令不包含
……		
N数据对象ID	2	参考附录 数据对象标志码
N数据对象	Xn	写、读命令包含，读命令不包含

7.1.3.5　数据对象访问应答（上行）指令

上行报文的数据格式，如表 9：

表 9 应答指令上行报文数据格式

项目	说　明	产生方
运算规则	报文采用的运算	安全单元
功能控制字	普通上行报文	安全单元
同步计数器	报文计数器	安全单元
报文随机数	上行报文随机数	安全单元
数据报文	报文密文或者明文格式	表端MCU-->安全单元
MAC	MAC认证码	安全单元

上行报文，安全服务明文返回给采集服务，报文可包含多个目标数据对象见表 10：

表 10 读应答数据对象

项目	长度	说　明
数据对象个数	1	请求的数据对象个数
1数据对象ID	2	参考附录 数据对象标志码
1数据对象	X1	参考附录 数据对象标志码

2数据对象ID	2	参考附录 数据对象标志码
2数据对象	X2	参考附录 数据对象标志码
……		
N数据对象ID	2	参考附录 数据对象标志码
N数据对象	Xn	参考附录 数据对象标志码

7.1.3.6 安全单元访问请求（下行）指令

下行报文的数据格式，如表 11：

表 11 请求下行报文数据格式

项目	说 明	生成方
运算规则	报文采用的运算	安全服务
功能控制字	功能控制字	安全服务
同步计数器	报文计数器	安全服务
报文随机数	上行报文随机数	安全服务
数据报文	报文密文或者明文格式	采集服务-->安全服务
MAC或签名	MAC认证码或签名数据	安全服务

7.1.3.7 安全单元访问应答（上行）指令

上行报文的数据格式，如表 12：

表 12 应答指令上行报文数据格式

项目	说 明	产生方
运算规则	报文采用的运算	安全单元
功能控制字	功能控制字	安全单元
同步计数器	报文计数器	安全单元
报文随机数	上行报文随机数	安全单元
数据报文	报文密文或者明文格式	表端MCU-->安全单元
MAC	MAC认证码	安全单元

7.1.3.8 结束通信（下行）指令

下行报文的数据格式，如表 13：

表 13 结束通信指令下行报文数据格式

项目	说 明	生成方
运算规则	报文采用的运算	安全服务
功能控制字	普通下行功能控制	安全服务
同步计数器	报文计数器	安全服务
报文随机数	上行报文随机数	安全服务
数据报文	报文密文或者明文格式	采集服务-->安全服务
MAC或签名	MAC认证码或签名数据	安全服务

其中，数据报文的内容格式如表14：

表14 结束通信指令下行报文内容格式

项目	长度	说　明
数据对象个数	1	操作的数据对象个数
1数据对象ID	2	参考附录 数据对象标志码
1数据对象	X1	参考附录 数据对象标志码
2数据对象ID	2	参考附录 数据对象标志码
2数据对象	X2	参考附录 数据对象标志码
……		
N数据对象ID	2	参考附录 数据对象标志码
N数据对象	Xn	参考附录 数据对象标志码

7.2 配置数据

7.1.1 配置数据描述

燃气表使用的配置参数信息，燃气表初装后使用配置参数的默认初值进行处理，后期采集系统可根据实际情况进行远程更新。

7.1.2 基础数据格式

基础数据格式见下表 15：

表 15 技术数据格式

数据项	备注
注册报文密钥信息	
IP 地址版本	
IPv4 地址	针对中国电信。建议厂商根据订单要求的运营商，在生产时灵活配置
IPv6 地址	
端口号	端口
APN	针对中国电信。建议厂商根据订单要求的运营商，在生产时灵活配置。
定时上传周期类型	
定时上传周期值	
定时上传时间点	
多天不用气关阀门限	
多天不通信关阀参数	
过流报警关阀使能	
过流门限	
微小流报警使能	
最大预留量	开户前预留气量
管道防拆使能	
直通报警使能	

外部报警使能	
逆流报警使能	

7.3 状态数据

7.3.1 状态数据描述

状态数据用于记录燃气表运行、计量等动态信息，按照业务要求上传频率定时上报主站。

7.3.2 状态数据格式

状态数据格式见下表 16：

表 16 状态数据格式

数据项	长度	备注
表内时钟	6字节	
运行状态	4字节	无符号整数，不足4字节，高字节补0
累计气量	6字节	数值扩大10倍以保留1位小数。
工况累计气量	6字节	数值扩大10倍以保留1位小数。
标况累计气量	6字节	数值扩大10倍以保留1位小数。
工况瞬时流量	4字节	数值扩大1000倍以保留3位小数。单位：m^3/h。
标况瞬时流量	4字节	数值扩大1000倍以保留3位小数。单位：m^3/h。
燃气温度	2字节	数值扩大100倍以保留2位小数，有符号整数
燃气压力	4字节	单位：Pa，无符号整数；若压力异常则上报FFFFFFFF
主电电压	2字节	数值扩大1000倍以保留3位小数。
声速	2字节	单位：m/s，例如365表示365m/s，异常则返回0xFFFF
结算状态	1字节	0--未透支；1--透支
阀门状态	1字节	1表示阀门关
异常状态	1字节	0表示无异常；1表示有异常

7.4 控制对象数据

7.4.1 控制对象描述

用于燃气表与主站通讯，主站向燃气表下达控制指令。

7.4.2 控制对象数据格式

控制对象数据格式见下表 17：

表 17 控制对象数据格式

数据项	长度	备注
解锁阀门	1	
关阀并上锁	1	
普通关阀	1	

8　检测要求

8.1　主站安全检测

8.1.1　证书发行检测

审查智能燃气表主站制造商提交的文件，检查证书是否由符合国密要求的 CA 系统颁发，证书发行是否满足在线发行和离线发行要求，核对审查结果是否符合 5.3.1 的要求。

8.1.2　接入认证检测

审查智能燃气表主站制造商提交的文件，验证确认主站能够提供安全措施控制数据的本地或远程访问，核对审查结果是否符合5.3.2的要求。

8.1.3　数据传输检测

审查智能燃气表主站制造商提交的文件，确认主站是否通过会话密钥加密方式实现保密通信，对会话密钥生命周期及重新协商等进行说明，核对审查结果是否符合5.3.3的要求。

8.1.4　密钥管理检测

审查智能燃气表主站制造商提交的文件，确认主站采用的密钥体制、加密设备及应用，核对审查结果是否符合5.3.4的要求。

8.2　智能燃气表安全检测

8.2.1　试验环境

智能燃气表试验应在下列条件下进行：

a）　温度：20.0℃±5.0℃；

b）　相对湿度：35%～85%；

c）　大气压：86kPa～106kPa；

d）　磁场：除地磁场外应无其他磁场干扰；

e）　气体介质：可使用空气或者其他气体进行试验。气体中应无游离水或油等杂质存在。使用空气作为检测介质时，在任何条件下都不应出现由空气中水蒸气所引起的凝结。

8.2.2　安全单元检测

8.2.2.1　智能燃气表生命周期管理检测

审查智能燃气表制造商提交的文件，检查燃气表生命周期状态是否存储在安全单元中，验证燃气表状态是否需在权限保护下切换，核对审查结果是否符合6.3.1.1的要求。

8.2.2.2　智能燃气表标识信息保护检测

审查智能燃气表制造商提交的文件，检查智能燃气表标识信息存储位置及修改条件，核对审查结果是否符合6.3.1.2的要求。

8.2.2.3　敏感数据保密检测

审查智能燃气表制造商提交的文件，确认智能燃气表在远程通信时，对敏感数据采用安全单元进行加密，核对审查结果是否符合6.3.1.3的要求。

8.2.2.4　关键操作权限认证检测

审查智能燃气表制造商提交的文件，确认智能燃气表关键操作权限认证设计；验证关键操作权限是否与厂商声明一致，核对检查结果是否符合6.3.1.4的要求。

8.2.3　安全功能检测

8.2.3.1　通用要求检测

审查智能燃气表制造商提交的文件，确认已获得行业认可的安全单元资质证书，或已取得国家密码管理部门颁发的硬件密码产品资质证书，检查确认安全单元存储、密码算法、文件类型、访问方式、传输方式、初始化方式、初始化完成的内容等是否满足6.3.2.1的要求。

8.2.3.2 累积量保护检测

审查智能燃气表制造商提交的文件，确认智能燃气表安全单元是否配置有累积量计算器，以及其功能、接口，核对检查结果是否符合6.3.2.2的要求。

8.2.3.3　指令重放检测

审查智能燃气表制造商提交的文件，验证确认协议报文设计引入了防重因子，核对审查结果是否符合6.3.2.3的要求。

8.3　数据格式检测

8.3.1　通信指令检测

8.3.1.1　注册指令检测

注册指令检测进行如下试验：

a)　启动主站和智能燃气表运转工作；

b)　按照智能燃气表制造商提供的方法或工具，触发智能燃气表注册功能，使用抓包工具抓取通信交互数据包，核对测试结果是否符合 7.1.1、7.1.2、7.1.3.1、7.1.3.2 的要求。

8.3.1.2　数据对象推送检测

数据对象推送检测进行如下试验：

a） 启动主站和智能燃气表运转工作；

b） 按照智能燃气表制造商提供的方法或工具，触发智能燃气表上报功能，使用抓包工具抓取通信交互数据包，核对测试结果是否符合 7.1.1、7.1.2、7.1.3.3 的要求。

8.3.1.3 数据对象访问检测

数据对象访问检测进行如下试验：

a） 启动主站和智能燃气表运转工作；

b） 按照智能燃气表制造商提供的数据对象访问信息，触发主站向智能燃气表下发指令，进行多次、多个数据对象访问以及开/关阀要求，核对试验结果是否符合 7.1.1、7.1.2、7.1.3.4、7.1.3.5、7.1.3.8、7.3、7.4 的要求。

8.3.1.4 安全单元访问检测

安全单元访问检测进行如下试验：

a） 启动主站和智能燃气表运转工作；

b） 按照智能燃气表制造商提供的安全单元访问信息，触发主站向智能燃气表下发指令，进行安全单元访问，核对试验结果是否符合 7.1.1、7.1.2、7.1.3.6、7.1.3.7 的要求。

8.3.2 配置数据格式检测

配置数据格式检测进行如下试验：

a） 智能燃气表初装后，检查智能燃气表当前使用的配置参数信息，确认符合 7.2 的要求；

b） 智能燃气表正常连接至主站后，参照表 15 的数据项内容，从主站向智能燃气表下发指令，进行配置数据的更新，使用抓包工具抓取通信交互数据包，核对测试结果是否符合 7.2 的要求。

附录 A

（规范性附录）

安全业务流程

A.1 智能燃气表注册

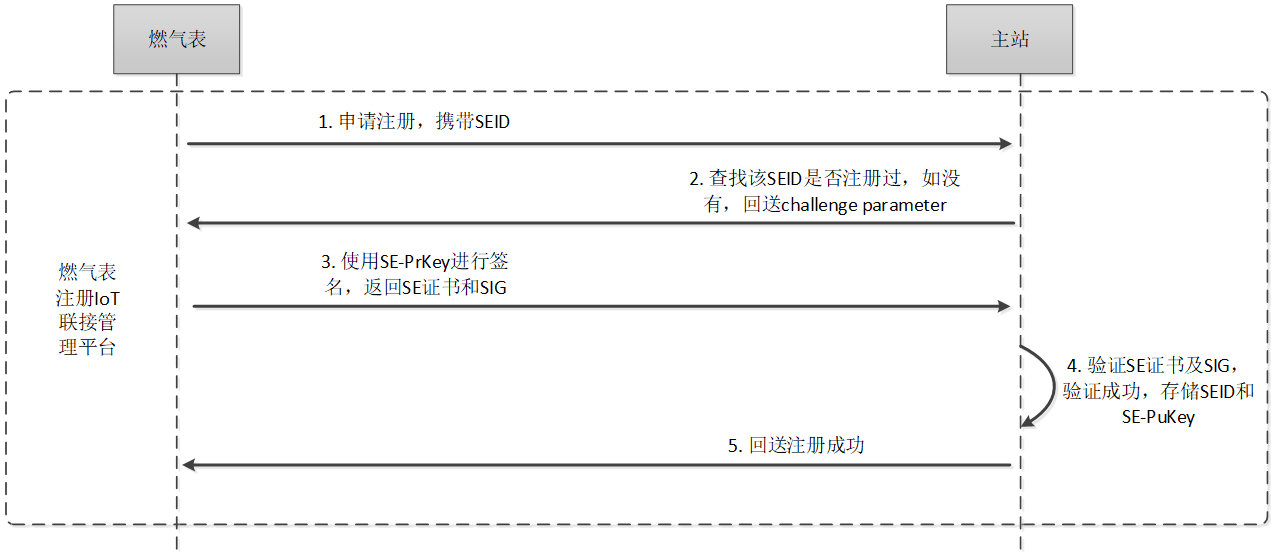

图 3 燃气表向 IoT 联接管理平台注册流程图

流程说明：

a） 燃气表通过网络向主站申请注册，携带 SEID；

b） 主站查找该燃气表号是否注册过，如未注册，向燃气表 SE 回送 challenge parameter；

c） 燃气表 SE 用安全单元证书私钥进行签名，并将安全单元证书和签名发送到主站；

d） 主站使用安全单元证书公钥数字签名，并使用根证书验证安全单元证书，确定燃气表 SE 的真实性，验证成功，则注册成功；

e） 主站向燃气表回送注册成功。

注：如未注册成功，燃气表需要重新申请注册。

A.2 智能燃气表数据上报

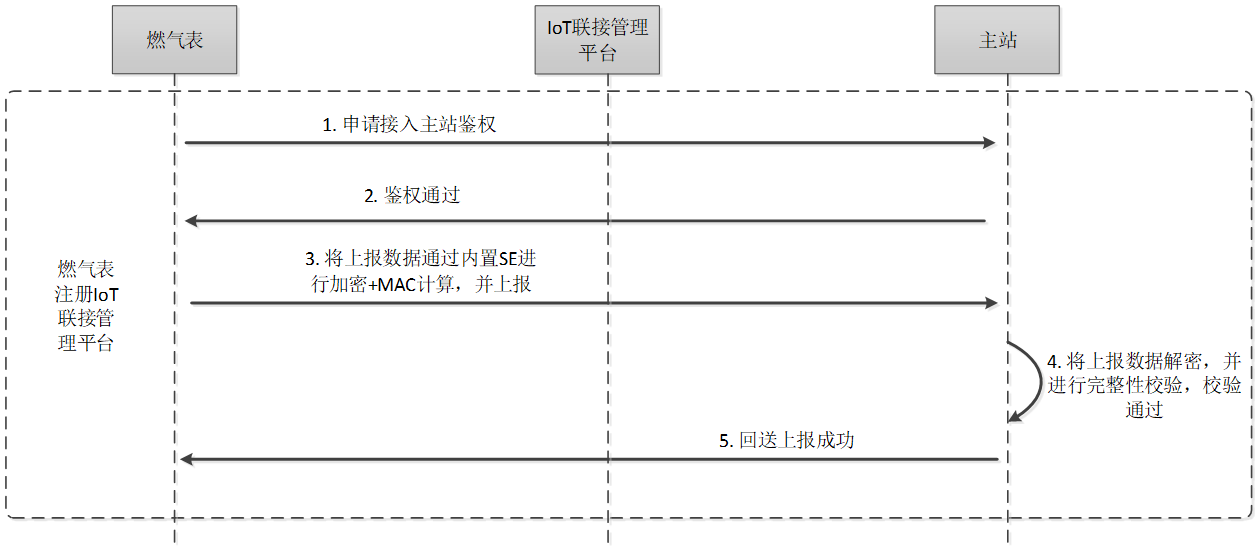

图4 燃气表向主站上报数据流程图

流程说明：

a） 燃气表向主站申请接入鉴权，IoT 联接管理平台鉴权通过后，燃气表可以向主站上报数据；

b） 燃气表将需要上报的数据通过内置安全单元（SE）进行加密+MAC 或加密+签名运算，然后发送到主站；

c） 主站解密上报数据，并进行完整性校验；

d） 主站向 SE 回送上报成功状态。

A.3 主站数据下传

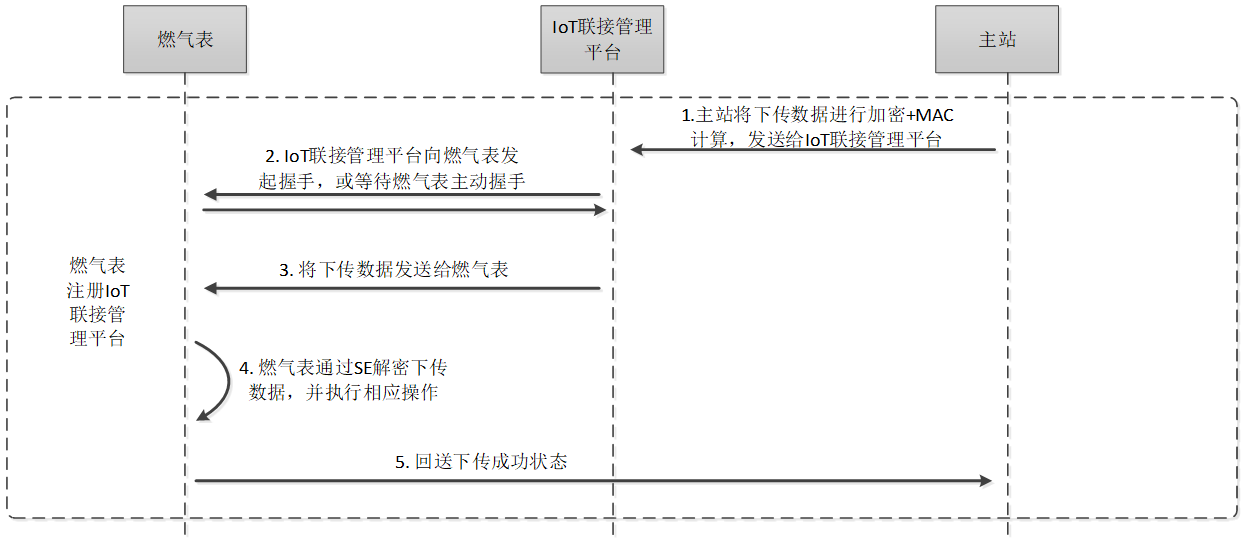

图5 主站向燃气表下传数据流程图

流程说明：

a） 主站将需要下传给燃气表的数据，包括阀门控制、模组升级、校时下传、初始化、SE 密钥更新等，进行加密+MAC 或加密+签名计算，并发送到 IoT 联接管理平台；

b） IoT 联接管理平台和燃气表握手，或等待燃气表的主动握手，握手成功后，将下传数据发送给燃气表；

c） 燃气表将接收到的数据发送到内置 SE 进行解密和完整性校验计算，SE 判断解密后的数据，如果是本身处理，如密钥更新，则处理成功后，回送燃气表成功状态；如果数据需要交给燃气表处理，如阀门控制，则将解密后数据返送到燃气表；

d） 向主站回送下传数据成功状态。

附 录B

（资料性附录）

数据对象标志码

B.1 状态数据对象标志码

下表给出了远传表状态数据对象标志码。

状态数据：仅用于上报或者读取，不能够被远程修改的数据。

状态数据对象标志码

数据对象ID	数据对象名称	长度	数据格式		
0x0001	表全貌信息（膜式表）	104	触发事件上报代码，4 字节。参考附录 录触发事件上报代码		
			表内时钟，6 字节 BCD 码，如{0x14,0x02,0x22,0x12,0x01,0x02}表示 14 年 2 月 22 日 12 时 1 分 2 秒。		
			运行状态，2 字节 HEX，无符号整数。格式详见“运行状态”数据对象。		
			累计气量，4 字节 HEX。数值扩大 10 倍以保留 1 位小数。		
			主电电压，2 字节。数值扩大 1000 倍以保留 3 位小数。		
			最近 5 条日汇总气量记录，（3 + 4） * 5 = 35 字节。3 字节年月日 BCD 码+4 字节日冻结数据（4 字节，数值扩大 10 倍以保留 1 位小数），总共 5 条		
			最近一条每日用气明细记录，3 + 2 * 24=51 字节。3 字节年月日 BCD 码，包含 24 小时用气增量数值（2 字节，数值扩大 100 倍以保留 2 位小数）。		
0x0002	表全貌信息（超声波表）	117	触发事件上报代码，4 字节。参考附录 录触发事件上报代码		
			表内时钟，6 字节 BCD 码，如{0x14,0x02,0x22,0x12,0x01,0x02}表示 14 年 2 月 22 日 12 时 1 分 2 秒。		
			运行状态，3 字节 HEX，无符号整数。格式详见“运行状态（超声波表）”数据对象。		
			工况累计气量，4 字节 HEX。数值扩大 10 倍以保留 1 位小数。为上报时实时累计气量，从远传表用气量信息文件获取。		
			标况累计气量，4 字节 HEX。数值扩大 10 倍以保留 1 位小数。为上报时实时累计气量，从远传表用气量信息文件获取。		
			燃气温度。2 字节 HEX。数值扩大 100 倍以保留 2 位小数，有符号整数；若温感异常则上报-9999		
			燃气压力。4 字节 HEX。单位：Pa，无符号整数；若压力异常则上报 FFFFFFFF		
			声速。2 字节 HEX。单位：m/s，例如 365 表示 365m/s，异常则返回 0xFFFF		
			主电电压，2 字节。数值扩大 1000 倍以保留 3 位小数。		
			最近 5 条日汇总气量记录，（3 + 4） * 5 = 35 字节。3 字节年月日 BCD 码+4 字节日冻结数据（4 字节，数值扩大 10 倍以保留 1 位小数），总共 5 条，标况上报。		
			最近一条每日用气明细记录，3 + 2 * 24=51 字节。3 字节年月日 BCD 码，包含 24 小时用气增量数值（2 字节，数值扩大 100 倍以保留 2 位小数），标况上报。		
0x1001	运行状态	2	BYTE0	BIT0~1	主电量状态，0 表示电量正常，1 表示电量低（碱

					电版本低于欠压值 1）,2 表示电量不足（碱电版本低于欠压值 2）。
				BIT2~3	备电状态，0 表示电量正常，1 表示电量不足，2 表示电量低，3 表示掉电。
				BIT4	阀门状态（开、关）,1 表示阀门关
				BIT5	远传表被强制命令关阀（阀门处于锁定状态）
				BIT6	计量异常（如磁干扰等计量传感器异常）
				BIT7	异常大流量状态。0 表示无异常；1 表示有异常
			BYTE1	BIT0	异常微小流量状态。0 表示无异常；1 表示有异常
				BIT1	外部报警。0 表示无报警；1 表示有报警
				BIT2~3	多天不用天气状态： 0 表示多天不用气状态正常 1 表示一级多天不用气状态 2 表示二级多天不用气状态
				BIT4	多天不通信告警 0 正常 1 告警
				BIT5	开户状态 0 未开户；1 已开户
				BIT6	管道防拆状态 0：未拆除状态；1 ：被拆除状态
				BIT7	备用
0x1003	运行状态（超声波表）	3	BYTE0	BIT0~1	主电量状态，0 表示电量正常，1 表示电量低（碱电版本低于欠压值 1）,2 表示电量不足（碱电版本低于欠压值 2）。
				BIT2~3	备电状态，0 表示电量正常，1 表示电量不足，2 表示电量低，3 表示掉电。
				BIT4	阀门状态（开、关）,1 表示阀门关
				BIT5	远传表被强制命令关阀（阀门处于锁定状态）
				BIT6	计量异常（如超声波计量模组等计量传感器异常）
				BIT7	异常大流量状态。0 表示无异常；1 表示有异常
			BYTE1	BIT0	异常微小流量状态。0 表示无异常；1 表示有异常
				BIT1	外部报警。0 表示无报警；1 表示有报警
				BIT2~3	多天不用天气状态： 0 表示多天不用气状态正常 1 表示一级多天不用气状态 2 表示二级多天不用气状态
				BIT4	多天不通信告警 0 正常 1 告警
				BIT5	开户状态 0 未开户；1 已开户
				BIT6	管道防拆状态 0：未拆除状态；1 ：被拆除状态
				BIT7	逆流状态：0 表示无异常；1 表示有异常
			BYTE2	BIT0	温度状态：0 表示无异常；1 表示有异常
				BIT1	压力状态：0 表示无异常；1 表示有异常
				BIT2	阀门故障报警（直通），0 表示无异常；1 表示

					有异常
				BIT3	累积量结算类型，0 表示标况结算，1 表示工况结算
				BIT4~BIT7	保留
0x1002	结算状态	1	BIT0	透支状态：0--未透支；1--透支	
			BIT1	剩余量状态：0--剩余量未用完；1--剩余量用完	
			BIT2~BIT7	未定义	
0x2001	主电电压	2	HEX 码，无符号整数。数值扩大 1000 倍以保留 3 位小数		
0x2003	表内时钟	6	BCD 码，如{0x14,0x02,0x22,0x12,0x01,0x02}表示 14 年 2 月 22 日 12 时 1 分 2 秒。		
0x2005	累计气量	6	无符号整数。数值扩大 10 倍以保留 1 位小数。		

B.2 控制数据对象标志码

下表给出了远传表控制数据对象标志码。

控制信息：只写数据对象，请求方通过写结果判定是否控制成功。

控制数据对象标志码

数据对象 ID	数据对象名称	长度	数据格式
0x3001	解锁阀门	1	1 字节常量 0x01
0x3002	关阀并上锁	1	1 字节常量 0x01
0x3003	普通关阀	1	1 字节常量 0x01
0x3004	通信结束	22	结束原因，2 字节 HEX：0x0000，正常结束；非 0,异常结束。
			系统时钟，6 字节 BCD 码，如{0x14,0x02,0x22,0x12,0x01,0x02}表示 14 年 2 月 22 日 12 时 1 分 2 秒。终端可使用改数据对象进行时间校时。
			剩余气量，HEX，4 字节无符号整数，扩大 100 倍以保留 2 位小数
			透支状态，1 字节 HEX，0——未透支；1——透支。
			余量状态，1 字节 HEX，0——余量正常；1——余量不足。
			单价，HEX，4 字节无符号整数，扩大 100 倍以保留 2 位小数。
			剩余金额，HEX，4 字节有符号整数，扩大 100 倍以保留 2 位小数。该字段用于界面展示。金额表使用。

B.3 触发事件上报代码

下表给出了触发事件上报代码。

触发代码	事件说明
00 00 00 00	定时自动上报
00 00 00 01	长按键上报
00 00 00 02	连续不用气触发上报
00 00 00 03	红外触发
00 00 00 99	外部报警
80 01 00 06	电源电压欠压值
80 01 00 07	电源供电
80 01 00 09	阀门故障
80 01 00 10	时钟电池欠压
80 01 00 11	磁干扰
80 01 00 12	异常流量超大流量
80 01 00 13	异常流量超小流量
80 01 00 14	拆盖报警
80 01 00 15	倾斜报警
80 01 00 16	阀门强制开启
80 01 00 17	掉电上报
80 01 00 18	3D 防拆报警
80 01 00 19	计量异常
80 01 00 20	传感器故障
80 01 00 21	管道防拆
80 01 00 22	逆流报警
80 01 00 23	外部报警器连接异常
80 01 00 24	声速异常报警
80 01 00 25	压力异常报警