ICS 33.050
CCS M 30

团　体　标　准

T/TAF 103-2021

能源物联网设备通信数据安全技术要求和测试方法

The security technical requirement and testing method for communication data of energy networking equipment

2021-12-13 发布　　2021-12-13 实施

电信终端产业协会　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。

本文件由电信终端产业协会提出并归口。

本文件起草单位：中国信息通信研究院、北京时代亿德物联网科技有限公司、百度在线网络技术（北京）有限公司、北京奇虎科技有限公司、郑州信大捷安信息技术股份有限公司、中兴通讯股份有限公司。

本文件主要起草人：国炜、徐晓娜、高媛媛、毛翔、范杰、廖文川、高宏、周易、王敏、张军、王迪、王海棠、郭建领、唐佳伟、张屹、姚一楠、刘献伦、康亮、周继华。

引　　言

近几年，随着国家基础网络的日趋发达，能源物联网入网设备越来越多。然而，能源物联网设备的大量入网也带来了新的问题，入网能源物联网设备通信数据的安全性、有效性如何保障成为了当前能源行业最为关注的问题。能源物联网设备通信数据与国家工业生产及居民日常生活息息相关，如果数据安全得不到有效保障，会对工业生产和日常生活产生重大影响，甚至带来极大危害。

本文件旨在提高能源物联网设备通信数据安全性和可用性，便于能源物联网设备管理，合理利用网络资源，为能源物联网设备企业及相关行业用户起到具体的标准指导作用。

能源物联网设备通信数据安全技术要求和测试方法

1 范围

本文件规定了能源物联网设备的应用场景，在不同应用场景下的安全可靠性能。同时，规范了设备所采集和传输的数据类型及内容定义，以及对这些数据的安全保护技术要求。另外，本文件还包括对设备内的用户数据保护的指令技术要求，以及与上述技术要求对应的相应测试方法。

本文件适用于能源物联网设备。

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。

GM/T 0008-2012 安全芯片密码检测准则

3 术语和定义

下列术语和定义适用于本文件。

3.1

能源物联网设备 energy networking equipment

采集水电气热油等能源数据、计量能源过程执行数据、执行数据上传/接受自管理系统，能进行人机交互，具备数据通信能力的能源设备。

3.2

静态因子 static factor

用于标识能源物联网设备唯一设备编码的UIDI码，总共15位十进制数字，由TAF协会统一下放和管理。

3.3

动态因子 dynamic factor

用于在线验证能源物联网设备特征的信息数据，其中包括了UIDI码，温度，位置信息等特征数据。

3.4

通信模组（模块） communication module (module)

供能源物联网设备上网的集合通信芯片，元器件于一体的通信设备，通常指NB,4G,5G等能入运营商网络的集成模块。

4 缩略语

下列缩略语适用于本文件。

AT：通信模组规定的通讯指令集（Attention）

CNNVD：国家信息安全漏洞库（China National Vulnerability Database of Information Security）

CNVD：国家信息安全漏洞共享平台（China National Vulnerability Database）

IMEI：国际移动设备识别码（International Mobile Equipment Identity）

IP：互联网协议（Internet Protocol）

ITAC：物联网型号分配码（IoT Type Allocation Code）

MAC：媒体存取控制位址（Media Access Control Address）

NB-IoT：窄带物联网（Narrow Band Internet of Things）

NFC：近场通信（Near Field Communication）

RFID：射频识别（Radio Frequency Identification）

TAF：电信终端产业协会（Telecommunication Terminal Industry Forum Association）

UIDI：物联网设备统一编码（Unified IoT Device Identity）

5 能源物联网设备概况

5.1 能源物联网设备应用场景

能源物联网是物联网向水、电、气、暖等能源生产、分配和消费过程的延申，主要是采用传感器技术、嵌入式技术、边缘计算技术、区块链等技术，把能源生产、存储、配送、消费等能源基础设施通过先进信息通信技术、网络技术连接起来，并运行特定的程序，实现智能感知、智能计算、智能处理、智能决策、智能控制的目标。能源物联网主要目标是实现物理互联、信息互通、语义互操作，相比其他的物联网应用场景，能源物联网的特征是实时、智能、安全、可靠、可信、可控。

能源物联网设备典型的应用场景如下：

——水务信息智能管理系统

——充电桩管理系统

——智能燃气管理系统

——热水供应系统

——智能电网系统

能源物联网系统包括硬件部分和相应的软件部分。硬件部分包括电表、水表、气表等对原始数据采集设备，以及数据汇聚设备、服务器等；软件部分可根据实际系统的部署情况及要实现的系统功能所开发的系统软件。

5.2 能源物联网设备端数据分类

能源物联网终端数据通常包括静态因子数据、动态因子数据和过程执行监测数据，具体定义如下：

——静态因子数据：该类数据是与设备属性相关的数据，如设备标识、软硬件名称与版本等；该类数据主要用于设备使用、监测控制、维护等生命周期管理。

——动态因子数据：该类数据包括能源设备设施的周边环境数据，如气温、噪声、水浸、湿度、酸碱度、烟雾、粉尘等；设备状态数据，如设备温度、绝缘强度、倾斜状态、沉降、污秽等。具体数据属性可参见附录 A。这些数据对能源设施的正常运行、故障产生、设备寿命、巡视检修等产生或多或少的影响，也是有效对事故提前预防、报警和事前处理、提高系统运行效率的有利因素。

——过程执行监测数据：这类数据主要和能源用户的消费行为属性相关，是各类、各级用户的精确用能计量数据的基础，具体数据内容可参见附录 B-H。过程执行数据是实现人、设备、系统、服务等多维信息的交互，并提升需求响应互动，也是碳市场交易所需的主要数据来源。

5.3 能源物联网终端功能架构

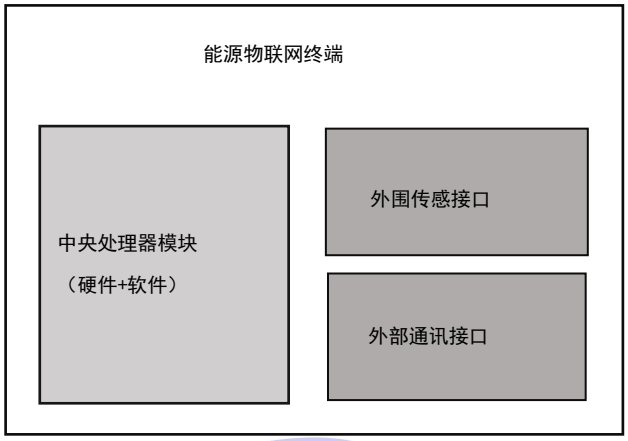

图 1 能源物联网终端功能架构

能源物联网终端是物联网中连接传感网络层和传输网络层，并实现采集数据、向网络层发送数据的设备。它主要的功能是数据采集、数据初步处理、数据加密、数据传输等。

如图 1 所示，能源物联网终端主要由外围传感接口、中央处理模块和外部通讯接口三个部分组成，通过外围传感接口与传感设备连接，如 RFID 读卡器、红外感应器、环境传感器等，将这些传感设备所采集的数据进行读取并通过中央处理模块处理后，按照网络协议，通过外部通讯接口，如蜂窝通信模块（NB-IoT/4G/5G 等）、以太网接口、Wi-Fi、蓝牙等通信协议将数据发送到指定的数据处理平台。

6 总体安全目标

6.1 安全风险

能源物联网系统在每个环节、每个瞬间都会产生海量的数据，这些数据在极大地促进智能感知、内部管控能力一级用户服务效率的同时，面临的主要安全风险是数据被篡改和泄露。

终端在对数据的采集、传输、存储、处理、使用过程中如无法实施有效的控制、或者缺乏一定的安全机制，都会造成数据被篡改或泄露。一旦这些数据被篡改、泄露，将会对整个能源生产、经营管理、用户服务造成极大的影响。

6.2 安全目标

对于能源物联网设备来讲，其面临的终端网络安全漏洞是导致端侧数据被篡改或数据泄露的主要原因，另外由于终端采用的操作系统、嵌入式设备、芯片等各异，通信协议、接口实现方式也不同，出现安全漏洞的几率也大，全面修复漏洞的难度也较大，容易被恶意攻击者用来实现渗透攻击。

因此，在终端侧实现数据存储、使用、传输的机密性和完整性，以及终端设备自身的完整性就显得尤为重要。能源物联网设备通信数据安全目标如下：

a) 能源物联网设备端应具有一定的通信加密机制和验证机制，保证通信数据的机密性和完整性；
b) 能源物联网设备端应具有一定的安全存储机制，保证设备端数据的存储安全；
c) 能源物联网设备端应具备一定的安全传输机制，保证数据传输的机密性、完整性和抗重放性；
d) 能源物联网设备端在软硬件设计上应具有一定的安全机制，保证系统和固件完整性和可用性。

7 安全技术要求

7.1 数据安全要求

7.1.1 静态因子数据安全要求

能源物联网设备标识码应满足以下安全要求：

a) 能源物联网设备应对每个设备标识码（UIDI）进行 MAC 处理后，将处理后的字段连同规范的设备标识码存储在模组的安全区域中，并保证出厂后不可更改；
b) 能源物联网设备应支持使用安全的 AT 指令向模组写入或读取 UIDI；
c) 能源物联网设备的操作系统应具有读取 UIDI 的接口，且该接口不应向非授权认可的第三方应用管理系统开放。

7.1.2 动态因子数据安全要求

能源物联网设备动态因子数据以满足以下安全要求：

a) 能源物联网设备应对动态因子数据进行 MAC 处理后，将处理后的字段连同加密后的动态因子数据存储在模组的安全区域中，并保证不被外部设备更改；
b) 能源物联网设备应支持使用安全的 AT 指令向模组写入或读取加密的动态因子数据。

7.1.3 过程执行监测数据安全要求

能源物联网设备过程执行监测数据应满足以下安全要求：

a) 能源物联网设备应对过程执行监测类数据进行 MAC 处理后，将加密后的过程数据存储在模组的安全区域中，并保证不被更改；
b) 能源物联网设备应支持使用安全的 AT 指令向模组写入或读取加密的过程数据。

7.2 无线通信安全要求

7.2.1 通信模组通用安全要求

能源物联网设备应满足以下无线通信通用安全要求：

a) 在通信双方建立会话前，应进行双向身份验证；
b) 重新建立会话或会话超时，应重新进行身份验证；
c) 应使用加密算法和完整性保护算法保护通信数据安全；
d) 若涉及密钥管理，密钥管理策略应能够保证周期密钥更新、密钥撤销和密钥分发等环节的安全性；
e) 对于关乎民生用能的能源物联网终端设备，应具备两种通信方式，可选范围包括蜂窝通信、红外、蓝牙、Wi-Fi、NFC 等。

7.2.2 蜂窝通信安全要求（如适用）

如能源物联网设备使用蜂窝通信，除应满足7.2.1小节的要求外，还应满足以下安全要求：

a) 蜂窝通信模组应具备不可更改的设备 IMEI 号；
b) 蜂窝通信模组应具备双向鉴权能力。

7.2.3 蓝牙通信安全要求（如适用）

如能源物联网设备使用蓝牙通信，除应满足7.2.1小节的要求外，还应满足以下安全要求：

a) 蓝牙模组应采取措施防止中间人攻击；
b) 使用 BLE4.2 及以上版本协议的模块应使用 LE Secure Connection 模式。

7.2.4 Wi-Fi 通信安全要求（如适用）

如能源物联网设备使用Wi-Fi通信，除应满足7.2.1小节的要求外，还应满足以下安全要求：

应采用WPA3及以上版本协议，采用其他版本时，应通过固定IP、MAC地址过滤等方式保证设备的接入安全和数据传输安全。

7.3 存储安全要求

能源物联网设备数据存储应满足以下安全要求：

a) 能源物联网设备上存储数据时，应采用安全机制以保证其机密性；
b) 能源物联网设备上存储的重要数据（如物联网设备统一编码 UIDI 等）应保存在安全的隔离区域；
c) 数据保护所采用的加密算法应符合相关国家标准和行业标准的要求；
d) 安全存储的密钥应由安全单元进行生成和保护。数据加密应在安全单元内进行。对采用的安全单元应至少满足 GM/T 0008 安全等级 2 级要求，且应具备商用密码产品认证证书。

7.4 传输安全要求

能源物联网设备数据传输应满足以下安全要求：

a) 在传输静态因子、动态因子和过程数据时，应采用数据完整性校验机制保证传输数据的完整性；
b) 在传输静态因子、动态因子和过程数据时，应采用密码机制保证传输数据的机密性；
c) 对于重要数据的传输，应采用有一定强度的加密算法对数据进行加密；
d) 在传输加密数据时，宜采用一次一密的加密传输方式；
e) 传输数据时的加密算法，宜采用国产密码算法；
f) 在传输静态因子、动态因子和过程数据时，应采用一定的机制保证传输数据的抗重放性；
g) 每次传输过程执行数据时，应先将要求的动态因子信息写入到模组的特殊区域内。

7.5 安全认证要求

能源物联网设备应满足以下安全认证要求：

a) 应具备唯一的物联网设备统一编码（UIDI），即静态因子；
b) 应具备用于在线验证能源物联网设备特征的信息数据，即动态因子，动态因子一部分由通信模组提供，一部分由设备提供；
c) 能源物联网设备在通信模组上电后，应读取动态因子并发送给后台安全系统，进行检测和验证；

d) 具有控制台接口的能源物联网设备，应具备认证授权机制（如用户名、口令等方式），禁止未授权访问。

7.6 安全防护与更新要求

7.6.1 系统安全防护要求

能源物联网设备系统应具备安全防护能力，安全防护要求包括但不限于：

a) 应支持系统更新能力；
b) 不应存在已知或在 CNVD、CNNVD 等平台公布 6 个月以上的高危及以上等级漏洞；
c) 应具有防回滚策略，防止系统被恶意降级；
d) 对具备调试功能的设备，应限制调试进程在操作系统中的访问权限和操作权限，防止权限设置过高导致权限滥用；
e) 应采用可信计算等技术，保证系统安全，内部程序采用白名单机制。

7.6.2 系统安全更新要求

能源物联网设备系统应具备安全更新机制，安全更新要求包括但不限于：

a) 应校验系统更新文件的来源和完整性；
b) 系统更新失败时，应保证系统的可用性，避免更新失败导致系统失效。

7.6.3 固件安全更新要求

能源物联网设备固件通过网络或本地接口升级，升级后新版本固件代替原固件，其安全更新要求如下：

a) 应对固件升级包的完整性和来源可靠性进行验证，校验通过后才可以升级；
b) 固件升级失败应保持升级前的固件版本，不允许固件升级到比当前版本号更低的版本；
c) 不应提供用户自主回退机制。

8 测试方法

8.1 数据安全测试

8.1.1 设备标识码安全测试

测试目的	7.1.1 静态因子数据安全
要求	a) 能源设备应对每个设备标识码（UIDI）进行 MAC 处理后，将处理后的字段连同规范的设备标识码存储在模组的安全区域中，并保证出厂后不可更改； b) 能源设备应支持使用安全的 AT 指令向模组写入或读取 UIDI； c) 能源设备的操作系统应具有读取 UIDI 的接口，且该接口不应向非授权认可的第三方系统平台开放。
预置条件	a) 保证设备正常运行； b) 设备具有唯一标识。
测试步骤	a) 使用安全的 AT 指令从模组中读取 UIDI； b) 查看是否读取到 UIDI； c) 以非授权认可的第三方角色从操作系统接口中读取 UIDI，查看读取是否成功。

预期结果	a) 使用 AT 指令从模组中读取的 UIDI； b) 以非授权认可的第三方角色从操作系统接口中读取 UIDI 失败。
实测结果	与预期结果一致
备注	无

8.1.2 动态因子数据安全测试

测试目的	7.1.2 动态因子数据安全
要求	a) 能源设备应对动态因子数据进行 MAC 处理后，将处理后的字段连同加密后的动态因子数据存储在模组的安全区域中，并保证不被更改； b) 能源设备应支持使用安全的 AT 指令向模组写入或读取加密的动态因子数据。
预置条件	a) 保证设备正常运行； b) 设备采集动态因子成功。
测试步骤	使用安全的 AT 指令从模组中读取动态因子。
预期结果	使用 AT 指令从模组中读取的动态因子，其中动态因子数据是加密后的数据。
实测结果	与预期结果一致
备注	无

8.1.3 能源过程执行监测数据安全测试

测试目的	7.1.3 过程执行监测数据安全
要求	a) 能源设备应对过程数据进行 MAC 处理后，将加密后的过程数据存储在模组的安全区域中，并保证不被更改； b) 能源设备应支持使用安全的 AT 指令向模组写入或读取加密的过程数据。
预置条件	a) 保证设备正常运行； b) 设备采集能源过程数据成功。
测试步骤	使用安全的 AT 指令从模组中读取能源过程数据。
预期结果	使用 AT 指令从模组中读取的能源过程数据，其中过程数据是加密后的数据。
实测结果	与预期结果一致
备注	无

8.2 无线通信安全测试

8.2.1 通信模组通用安全测试

测试目的	7.2.1 通信模组通用安全
要求	a) 在通信双方建立会话前，应进行双向身份验证；

	b) 重新建立会话或会话超时，应重新进行身份验证； c) 应使用加密算法和完整性保护算法保护通信数据安全； d) 若涉及密钥管理，密钥管理策略应能够保证周期密钥更新、密钥撤销和密钥分发等环节的安全性； e) 对于关乎民生用能的能源物联网终端设备，应具备两种通信方式，可选范围包括蜂窝通信、红外、蓝牙、Wi-Fi、NFC 等。
预置条件	保证设备正常运行
测试步骤	a) 检查能源物联网设备与其他主体之间在建立会话之前，设备是否对对方进行身份验证，是否为对方提供了验证设备身份的相关支持； b) 检查重新建立会话或会话超时，是否需要重新进行身份验证； c) 查看设备所用通信协议配置信息，是否支持数据加密及完整性保护； d) 检查文档，若涉及密钥管理，查看是否保证密钥更新、密钥撤销和密钥分发等环节的安全性； e) 检查关乎民生用能的能源物联网终端设备，是否具备两种通信方式。
预期结果	a) 能源物联网设备与其他主体之间在建立会话之前，进行了身份验证，并为对方验证其身份提供了相关支持； b) 重新建立会话或会话超时，需要重新进行身份验证； c) 设备所用通信协议支持数据加密及完整性保护； d) 密钥管理方案能保证密钥更新、密钥撤销和密钥分发等环节的安全性； e) 关乎民生用能的能源物联网终端设备具备两种通信方式。
实测结果	与预期结果一致
备注	无

8.2.2 蜂窝通信安全测试（如适用）

测试目的	7.2.2 蜂窝通信安全
要求	a) 蜂窝通信模组应具备不可更改的设备 IMEI 号； b) 蜂窝通信模组应具备双向鉴权能力。
预置条件	a) 保证设备正常运行； b) 设备具备蜂窝通信模组。
测试步骤	a) 查看蜂窝通信模组是否具备 IMEI 号； b) 查看蜂窝通信模组所用协议及其配置是否支持双向鉴权。
预期结果	a) 蜂窝通信模组具备 IMEI 号； b) 蜂窝通信模组所用协议支持双向鉴权。
实测结果	与预期结果一致
备注	无

8.2.3 蓝牙通信安全测试（如适用）

测试目的	7.2.3 蓝牙通信安全
要求	a) 蓝牙模组应采取措施防止中间人攻击； b) 使用 BLE4.2 及以上版本协议的模块应使用 LE Secure Connection 模式。
预置条件	a) 保证设备正常运行；

	b) 设备具备蓝牙通信模组。
测试步骤	a) 尝试构建中间人攻击场景，查看蓝牙通信模组是否可以防止中间人攻击； b) 查看协议配置，若使用 BLE 4.2 及以上版本，查看是否使用 LE Secure Connection 模式。
预期结果	a) 蓝牙通信模块可防止中间人攻击； b) BLE 4.2 及以上版本，开启 LE Secure Connection 模式。
实测结果	与预期结果一致
备注	无

8.2.4 Wi-Fi 通信安全测试（如适用）

测试目的	7.2.4 蓝牙通信安全
要求	应采用 WPA3 及以上版本协议，采用其他版本时，应通过固定 IP、MAC 地址过滤等方式保证设备的接入安全和数据传输安全。
预置条件	a) 保证设备正常运行； b) 设备具备 Wi-Fi 通信模组。
测试步骤	查看能源物联网设备是否使用 WPA3 或以上版本协议，若采用其他版本，查看是否使用固定 IP、MAC 地址过滤方式。
预期结果	设备使用 WPA3 或以上版本协议；或采用其他版本协议时，使用固定 IP、MAC 地址过滤方式。
实测结果	与预期结果一致
备注	无

8.3 存储安全测试

测试目的	7.3 存储安全
要求	a) 能源物联网设备上存储数据时，应采用安全机制以保证其机密性； b) 能源物联网设备上存储的重要数据（如物联网设备统一编码 UIDI 等）应保存在安全的隔离区域； c) 数据保护所采用的加密算法应符合相关国家标准和行业标准的要求； d) 安全存储的密钥应由安全单元进行生成和保护。数据加密应在安全单元内进行。对采用的安全单元应至少满足 GM/T 0008 安全等级 2 级要求，且应具备商用密码产品认证证书。
预置条件	保证设备正常运行
测试步骤	a) 读取能源物联网设备上存储的数据，查看是否使用安全机制保证机密性； b) 查看文档，检查能源物联网设备上存储的重要数据（如 UIDI 等）是否保存在安全的隔离区域内； c) 检查存储数据使用的加密算法是否符合要求； d) 检查安全存储使用的密钥是否由安全单元生成和保护，数据加密是否在安全单元内进行，采用的安全单元是否满足 GM/T 0008 安全等级 2 级要求且具备商用密码产品认证证书。
预期结果	a) 存储的数据为密文形式； b) 存储的重要数据保存在安全的隔离区域；

	c) 使用的加密算法是否符合国家相关法律法规和相关标准要求； d) 安全存储使用的密钥是否由安全单元生成和保护，数据加密在安全单元内进行，采用的安全单元满足 GM/T 0008 安全等级 2 级要求且具备商用密码产品认证证书。
实测结果	与预期结果一致
备注	无

8.4 传输安全测试

测试目的	7.4 传输安全
要求	a) 在传输静态因子、动态因子和过程数据时，应采用数据完整性校验机制保证传输数据的完整性； b) 在传输静态因子、动态因子和过程数据时，应采用密码机制保证传输数据的机密性； c) 对重要数据的传输，应采用有一定强度的加密算法对数据进行加密； d) 在传输加密数据时，应采用一次一密的加密传输方式； e) 传输数据时的加密算法，可采用国产密码算法； f) 在传输静态因子、动态因子和过程数据时，应采用一定的机制保证传输数据的抗重放性； g) 每次传输过程数据时，应先将要求的动态因子信息写入到模组的特殊区域内。
预置条件	保证设备正常运行
测试步骤	a) 检查是否具有传输数据的完整性校验机制； b) 检查数据传输时是否具有密码机制，抓包查看传输的数据是否进行了加密； c) 检查是否具备一次一密的加密传输方式； d) 检查传输数据的加密算法； e) 检查数据传输时是否具备抗重放攻击机制，抓包获取传输的数据被将之重放，检查是否满足抗重放保护要求； f) 检查传输过程数据时，是否将动态因子信息写入到通信模组。
预期结果	a) 具有传输数据的完整性校验机制； b) 数据传输时具有密码机制，抓包查看传输的数据进行了加密； c) 具备一次一密的加密传输方式； d) 传输数据的加密算法符合要求； e) 数据传输时具备抗重放攻击机制，抓包获取传输的数据被将之重放，满足抗重放保护要求； f) 传输过程数据时，将动态因子信息写入到通信模组。
实测结果	与预期结果一致
备注	无

8.5 安全认证测试

测试目的	7.5 安全认证
要求	a) 应具备唯一的物联网设备统一编码（UIDI），即静态因子； b) 应具备用于在线验证能源物联网设备特征的信息数据，即动态因子； c) 能源物联网设备在通信模组上电后，应读取动态因子并发送给后台安

	全系统，进行检测和验证； d) 具有控制台接口的能源物联网设备，应具备认证授权机制（如用户名、口令等方式），禁止未授权访问。
预置条件	保证设备正常运行
测试步骤	a) 检查是否具备唯一的物联网设备统一编码（UIDI）； b) 检查是否具备用于在线验证能源物联网设备特征的信息数据； c) 检查设备在通信模组上电后，是否读取动态因子并发送给后台安全系统进行检测和验证； d) 对具有控制台接口的能源物联网设备，检查是否具备认证授权机制，尝试未授权访问，是否能访问成功。
预期结果	a) 具备静态因子； b) 具备动态因子； c) 设备在通信模组上电后，读取动态因子并发送给后台安全系统进行检测和验证； d) 对具有控制台接口的能源物联网设备，具备认证授权机制，尝试未授权访问，访问失败。
实测结果	与预期结果一致
备注	无

8.6 安全防护与更新测试

8.6.1 系统安全防护测试

测试目的	7.6.1 系统安全防护
要求	a) 应支持系统更新能力； b) 不应存在已知或在 CNVD、CNNVD 等平台公布 6 个月以上的高危及以上等级漏洞； c) 应具有防回滚策略，防止系统被恶意降级； d) 对具备调试功能的设备，应限制调试进程在操作系统中的访问权限和操作权限，防止权限设置过高导致权限滥用； e) 应采用可信计算等技术，保证系统安全，内部程序采用白名单机制。
预置条件	保证设备正常运行
测试步骤	a) 审查是否具备系统更新能力； b) 使用漏扫工具查看是否存在已知或在 CNVD、CNNVD 等平台公布 6 个月以上的高危及以上等级漏洞； 注：对于 6 个月以上仍未公布漏洞修复方法的情况，可采取一定的补救措施，降低安全风险。 c) 检查具有防回滚策略； d) 检查具备调试功能的设备，是否限制调试进程在操作系统中的访问权限和操作权限； e) 检查是否采用可信计算等技术，内部程序采用白名单机制。
预期结果	a) 具备系统更新能力； b) 不存在已知或在 CNVD、CNNVD 等平台公布 6 个月以上的高危及以上等级漏洞； c) 具有防回滚策略； d) 具备调试功能的设备，限制了调试进程在操作系统中的访问权限和操

	作权限； e) 采用可信计算等技术，内部程序采用白名单机制。
实测结果	与预期结果一致
备注	无

8.6.2 系统安全更新测试

测试目的	7.6.2 系统安全更新
要求	a) 应校验系统更新文件的来源和完整性； b) 系统更新失败时，应保证系统可用性，避免更新失败导致系统失效。
预置条件	保证设备正常运行
测试步骤	a) 启动系统更新，检查系统更新前是否对系统更新包、更新版本进行完整性校验并验证来源可靠性； b) 尝试使系统更新失败，验证设备是否恢复到更新前可用的版本。
预期结果	a) 设备能安全更新系统； b) 系统更新失败后，设备保持更新前系统版本。
实测结果	与预期结果一致
备注	无

8.6.3 固件安全更新测试

测试目的	7.6.3 固件安全更新
要求	a) 应对固件升级包的完整性和来源可靠性进行验证，校验通过后才可以升级； b) 固件升级失败应保持升级前的固件版本，不允许固件升级到比当前版本号更低的版本； c) 不应提供用户自主回退机制。
预置条件	保证设备正常运行
测试步骤	a) 在升级服务器中添加用于测试的新版本固件，启动固件升级，检查固件升级前是否对固件升级包、固件升级版本进行完整性校验并验证来源可靠性； b) 尝试写入不正确的固件给设备，使升级失败，验证设备是否恢复到升级前可用的版本； c) 尝试写入比设备当前固件版本更低的固件给设备，验证能否升级成功； d) 检查设备是否给用户提供自主回退版本的机制。
预期结果	a) 设备能安全升级固件，不升级到不安全的固件； b) 固件升级失败后，设备恢复到升级前固件版本； c) 设备无法升级到低版本的固件； d) 设备不能给用户提供自主回退版本的机制。
实测结果	与预期结果一致
备注	无

附 录 A
（资料性）
动态因子

动态因子是每个设备必须上传的数据，设备特征属性在过程执行数据中体现。其具体数据内容见表 A.1。

表 A.1 动态因子属性

数据项	长度（位）	小数位	类型	是否必填项	说明
SN	8 字节	0	HEX	是	模组唯一号
UIDI 码	15	0	BCD	是	每个能源物联网设备从工信部申请的 ITAC 码+本产品流水号。15 位：86+ITAC 码（6）+流水号（6）+校验（1）
通信模组 IMEI 号	15	0	BCD	否	通信模组唯一识别码
模组基站定位信息	10	0	BCD	是	模组在网的基站信息
模组电信号码	13	0	BCD	是	可以在设备上电后提供
北斗位置	10	0	BCD	否	模组北斗位置，如果模组有此功能上传，无此功能填 FF
模组温度	3	2	HEX	否	模组温度，如果模组有此功能上传，无此功能填 FF。第一位最高位是符号，0 代表 0 度以上，1 代表 0 度以下
设备 MCU 编码/系列号	10	0	BCD	否	设备特有编号
设备位置	10	0	BCD	否	北斗位置，如设备有此功能。正在定义长度。
设备温度	3	2	HEX	否	如果模组有此功能上传，无此功能填 FF。第一位最高位是符号，0 代表 0 度以上，1 代表 0 度一下。两位小数
设备电压	4	2	HEX	是	设备的运行电压。单位：V
设备电流	4	2	HEX	是	设备的运行电流。单位：第一位最高位 0 代表 A，1 代表 mA。无小数位。
第二通道通信方式	2	0	BCD	否	00 蓝牙；01 接触卡；02NFC 卡；03 小无线；04WIFI；05 红外。非必要双通道填写 FF。

附 录 B
（资料性）
水表过程执行监测数据

水表过程执行监测数据具体数据内容见表 B.1。

表 B.1 水表过程执行监测数据属性

UIDI	IMEI号	控制信息	读写	方向	长度	小数位	类型	是否必填(否:FF)	内容
15位	15位	上报数据	R	上行	7	0	BCD	是	终端时钟(BCD)年月日时分秒 YYYYMMDDhhmmss
					1	0	BCD	是	信号质量 CSQ：0-31
					2	0	BCD	是	信噪比 SNR：有符号
					2	0	BCD	是	RSRP。有符号整数
					2	2	BCD	是	电源电压值，单位是 0.01V
					1	0	HEX	是	上报周期(日周月年)FF(01 日；02 周；03 月；04 年)
					10	0	BCD	否	北斗位置
					6	0	HEX	是	服务器 IP:HEX
					2	0	HEX	是	服务器端口:HEX
					32	0	ASCII	否	服务器域名:ASCII
					1	0	HEX	否	脉冲当量
					4(工 8)	2	HEX	是	累计正流量:HEX
					4(工 8)	2	HEX	是	累计逆流量:HEX
					4(工 8)	2	HEX	否	累计碳排放量
					4	2	HEX	否	预警剩余量:HEX
					1	0	BCD	否	阀门控制:0：关阀 1：开阀
					2(工 4)	0	HEX	是	阀门电流:HEX
					3	2	HEX	是	水温：有符号 HEX
					3	2	HEX	是	压力：无符号 HEX
					5	2	HEX	否	当前瞬时流量 HEX
					5(工 8)	2	HEX	是	剩余水量 HEX
					5(工 8)	2	HEX	是	累计购水量 HEX
					2	0	HEX	是	购水次数 HEX
					4	0	HEX	否	厂家自定义表状态
					1	0	HEX	否	上报原因 0：定时上报 1：按键上报 2：按键故障上报 3：上电池上报 4：刷卡上报 5：蓝牙上报 6：重发上报 7：欠压上报 8：计量异常上报 9：剩余量低上报 10：机电分离上报 11：上电池上报 12：大流量异常上报
					20	0	ASCII		ICCID：ASCII
					20	-	自定义		预留

附 录 C
（资料性）
充电桩过程执行监测数据

充电桩过程执行监测数据具体数据内容见表 C.1。

表 C.1 充电桩过程执行监测数据属性

UIDI	IMEI号	控制信息	读写	方向	长度	小数位	类型	是否必填(否:FF)	内容
15位	15位	上报数据	R	上行	7	0	BCD	是	终端时钟(BCD)年月日时分秒 YYYYMMDDhhmmss
					1	0	BCD	是	信号质量 CSQ：0-31
					2	0	BCD	是	信噪比 SNR：有符号
					2	0	BCD	是	RSRP。有符号整数
					2	2	BCD	是	电源电压值，单位是 0.01V
					1	0	HEX	是	上报周期(日周月年)FF(01 日；02 周；03 月；04 年)
					10	0	BCD	否	北斗位置
					6	0	HEX	是	服务器 IP:HEX
					2	0	HEX	是	服务器端口:HEX
					32	0	ASCII	否	服务器域名:ASCII
					8	0	BCD	是	充电桩运行编号
					1		BIN	是	充电桩接口
					8	0	BCD	否	用户 ID(消费单回调时需要带上该参数，标示哪个用户消费)
					6	0	BCD	是	电表地址
					4	2	HEX	是	充电前总电能示值
					4	2	HEX	是	充电后总电能示值
					4	2	HEX	是	充电前尖电能示值
					4	2	HEX	是	充电后尖电能示值
					4	2	HEX	是	充电前峰电能示值
					4	2	HEX	是	充电后峰电能示值
					4	2	HEX	是	充电前平电能示值
					4	2	HEX	是	充电后平电能示值
					4	2	HEX	是	充电前谷电能示值
					4	2	HEX	是	充电后谷电能示值
					4	2	HEX	是	本次充电金额
					4	2	HEX	是	本次充电总服务费
					3	4	HEX	否	尖电价
					3	4	HEX	否	尖服务费单价
					3	2	HEX	否	尖电量
					4	4	HEX	否	尖金额
					4	4	HEX	否	尖服务费金额
					3	4	HEX	否	峰电价
					3	4	HEX	否	峰服务费单价
					3	2	HEX	否	峰电量
					4	2	HEX	否	峰金额
					4	2	HEX	否	峰服务费金额
					3	4	HEX	否	平电价
					3	4	HEX	否	平服务费单价
					3	2	HEX	否	平电量
					4	2	HEX	否	平金额
					4	2	HEX	否	平服务费金额
					3	4	HEX	否	谷电价

表 C.1　充电桩过程执行监测数据属性（续）

UIDI	IMEI号	控制信息	读写	方向	长度	小数位	类型	是否必填(否:FF)	内容
					3	4	HEX	否	谷服务费单价
					3	2	HEX	否	谷电量
					4	2	HEX	否	谷金额
					4	2	HEX	否	谷服务费金额
					7	0	BCD	是	充电开始时间 YYYYMMDDHHmmss
					7	0	BCD	是	充电结束时间
					1	0	BCD	否	停止充电模式 1:恒压 2:恒流
					1	0	BCD	否	充电桩状态 1:未停机 2:停机
					1	0	BCD	否	停止充电原因
					1	0	BCD	否	当前 soc XX%
					20	0	ASCII		ICCID:ASCII
					20	-	自定义		预留

附 录 D
（资料性）
燃气过程执行监测数据

燃气过程执行监测数据具体数据内容见表 D.1。

表 D.1 燃气过程执行监测数据属性

UIDI	IMEI 号	控制信息	读写	方向	长度	小数位	类型	是否必填(否:FF)	内容
15 位	15 位	上报数据	R	上行	7	0	BCD	是	终端时钟(BCD)年月日时分秒 YYYYMMDDhhmmss
					1	0	BCD	是	信号质量 CSQ：0-31
					2	0	BCD	是	信噪比 SNR：有符号
					2	0	BCD	是	RSRP。有符号整数
					2	2	BCD	是	电源电压值，单位是 0.01V
					1	0	HEX	是	上报周期(日周月年)FF(01 日；02 周；03 月；04 年)
					10	0	BCD	否	北斗位置
					6	0	HEX	是	服务器 IP:HEX
					2	0	HEX	是	服务器端口:HEX
					32	0	ASCII	否	服务器域名:ASCII
					4(工 8)	2	HEX	是	当前工况累计气量： 无符号整数(HEX)，数值扩大 100 倍用于保留 2 位小数。
					4(工 8)	2	HEX	是	当前标况累计气量： 无符号整数(HEX)，数值扩大 100 倍用于保留 2 位小数。
					4(工 8)	2	HEX	是	当前碳累计排放量
					2	1	HEX	否	声速： 有符号整数(HEX)，数值扩大 10 倍用于保留 1 位小数。
					2	2	HEX	是	温度： 有符号整数(HEX)，数值扩大 100 倍用于保留 2 位小数。0x7FFF 表示温度异常；
					2	2	HEX	是	压力： 无符号整数(HEX)，数值扩大 100 倍用于保留 2 位小数。
					4	2	HEX	是	预警剩余量： 有符号整数(HEX)，数值扩大 100 倍用于保留 2 位小数。
					2	0	BCD	否	(BCD)当日最大瞬时流量时间
					2(工 4)	2	HEX	否	当日最大标况瞬时流量： 无符号整数(HEX)，数值扩大 100 倍用于保留 2 位小数。
					2(工 4)	2	HEX	否	当日最大工况瞬时流量： 无符号整数(HEX)，数值扩大 100 倍用于保留 2 位小数。
					4	-	-	-	保留
					4	0	HEX	否	表状态
					4	2	HEX	否	NB 网络信号强度： RSRP：有符号整数 2(HEX)； SNR：符号整数 2(HEX)。
					4	-	-	-	表厂自定义表状态
					1	-	-	-	供电类型
					2	2	HEX	否	主电电池电压
					1	0	BCD	否	主电电量百分比

表 D.1 燃气过程执行监测数据属性（续）

UIDI	IMEI号	控制信息	读写	方向	长度	小数位	类型	是否必填(否:FF)	内容
					1	0	BCD	否	上报方式:无符号整数（HEX） 0：自动定时 1：手动按键 5：欠压上报 9：计量异常上报 14：上电池上告 15：大流量异常上报 16：微小流泄露上报 17：反向走气上报 18：拆表上报 20：多天不用气上报 31：预警剩余量上报 32：温度传感器异常上报 33：压力传感器异常上报 34：温度超限上报 35：压力超限上报
					20	0	ASCII		ICCID：ASCII
					20	-	自定义		预留

附 录 E
（资料性）
热水过程执行监测数据

热水过程执行监测数据具体数据内容见表 E.1。

表 E.1 热水过程执行监测数据属性

UIDI	IMEI 号	控制信息	读写	方向	长度	小数位	类型	是否必填(否:FF)	内容
15 位	15 位	上报数据	R	上行	7	0	BCD	是	终端时钟(BCD)年月日时分秒 YYYYMMDDhhmmss
					1	0	BCD	是	信号质量 CSQ：0-31
					2	0	BCD	是	信噪比 SNR：有符号
					2	0	BCD	是	RSRP。有符号整数
					2	2	BCD	是	电源电压值，单位是 0.01V
					1	0	HEX	是	上报周期(日周月年)FF(01 日；02 周；03 月；04 年)
					10	0	BCD	否	北斗位置
					6	0	HEX	是	服务器 IP:HEX
					2	0	HEX	是	服务器端口:HEX
					32	0	ASCII	否	服务器域名:ASCII
					5(工 8)	2	HEX	是	累计热量 HXE 带单位
					5(工 8)	2	HEX	是	累计冷量 HXE 带单位
					5(工 8)	2	HEX	否	瞬时流量 HXE 带单位
					5(工 8)	2	HEX	否	功率 HXE 带单位
					5(工 8)	2	HEX	否	累计正流量 HXE 带单位
					5(工 8)	2	HEX	否	累计逆流量 HXE 带单位
					5(工 8)	2	HEX	否	累计碳排放量
					3	0	HEX	否	累计工作时间 HXE
					1	0	HEX	否	阀门控制:0：关阀 1：开阀
					3	2	HEX	是	进水温度：有符号 HEX
					3	2	HEX	是	回水温度：有符号 HEX
					2	2	HEX	是	压力：无符号 HEX
					1	0	HEX	否	状态字 HEX
					20	0	ASCII	否	ICCID：ASCII
					20	-	自定义		预留

附 录 F
（资料性）
电能表过程执行监测数据

电能表过程执行监测数据单相具体数据内容见表 F.1。

表 F.1 电能表过程执行监测数据单相

UIDI	设备分类编码	IMEI 号	控制信息	读写	方向	长度	小数位	类型	是否必填（否:FF）	内容
15 位	110101 设备大类 + 设备中类 + 设备小类	15 位	上报数据	R	上行	7	0	BCD	是	终端时钟(BCD)年月日时分秒
						1	0	BCD	是	信号质量 CSQ：0-31
						2	0	BCD	是	信噪比 SNR：有符号
						2	0	BCD	是	RSRP。有符号整数
						2	2	BCD	是	电源电压值，单位是 0.01V
						1	0	HEX	是	上报周期
						10	0	BCD	否	北斗位置
						6	0	HEX	是	服务器 IP:HEX
						2	0	HEX	是	服务器端口:HEX
						32	0	ASCII	否	服务器域名:ASCII
						6	0	BCD	否	电能表通信地址 字节串
						6	0	BCD	是	电能表表号 字节串
						6	0	BCD	否	电能表客户编号 字节串 Octet String
						6	0	HEX	是	电能表额定电压
						6	0	HEX	是	电能表基本电流
						6	0	HEX	否	电能表最大电流
						6	0	HEX	否	电能表最小电流
						6	0	HEX	否	电能表转折电流
						4	0	HEX	否	电能表有功准确度等级
						4	0	HEX	否	电能表无功准确度等级
						4	0	HEX	否	电能表有功常数 Double-long-unsigned 单位:imp/kWh 换算:0
						4	0	HEX	否	电能表无功常数 Double-long-unsigned 单位:imp/kvarh 换算:0
						4	0	HEX	是	电能表电压互感器变比 单位:无 换算:无
						4	0	HEX	是	电能表电流互感器变比单位:无 换算:无
						2	1	HEX	是	电能表 A 相电压 Long-unsigned 单位:V 换算:-1
						4	3	HEX	是	电能表 A 相电流 Double-long 单位:A 换算:-3
						4	3	HEX	否	电能表零线电流 Double-long 单位:A 换算:-3
						4	1	HEX	是	电能表有功总功率 Double-long 单位:W 换算:-1
						2	3	HEX	是	电能表总功率因数 Long 单位:无 换算:-3
						2	1	HEX	否	电能表温度 Long 单位:℃ 换算:-1
						4	2	HEX	是	电能表当前组合有功总电能 Double-long 单位:kWh 换算:-2
						4	2	HEX	是	电能表当前组合有功费率 1 电能 Double-long 单位:kWh 换算:-2
						4	2	HEX	是	电能表当前组合有功费率 2 电能 Double-long 单位:kWh 换算:-2
						4	2	HEX	是	电能表当前组合有功费率 3 电能 Double-long 单位:kWh 换算:-2

表 F.1　电能表过程执行监测数据单相（续）

UIDI	设备分类编码	IMEI 号	控制信息	读写	方向	长度	小数位	类型	是否必填(否:FF)	内容
						4	2	HEX	是	电能表当前组合有功费率 4 电能 Double-long 单位:kWh 换算:-2
						4	2	HEX	是	电能表当前正向有功总电能 Double-long-unsigned 单位:kWh 换算:-2
						4	2	HEX	是	电能表当前正向有功费率 1 电能 Double-long-unsigned 单位:kWh 换算:-2
						4	2	HEX	是	电能表当前正向有功费率 2 电能 Double-long-unsigned 单位:kWh 换算:-2
						4	2	HEX	是	电能表当前正向有功费率 3 电能 Double-long-unsigned 单位:kWh 换算:-2
						4	2	HEX	是	电能表当前正向有功费率 4 电能 Double-long-unsigned 单位:kWh 换算:-2
						4	2	HEX	是	电能表当前反向有功总电能 Double-long-unsigned 单位:kWh 换算:-2
						4	2	HEX	是	电能表当前反向有功费率 1 电能 Double-long-unsigned 单位:kWh 换算:-2
						4	2	HEX	是	电能表当前反向有功费率 2 电能 Double-long-unsigned 单位:kWh 换算:-2
						4	2	HEX	是	电能表当前反向有功费率 3 电能 Double-long-unsigned 单位:kWh 换算:-2
						4	2	HEX	是	电能表当前反向有功费率 4 电能 Double-long-unsigned 单位:kWh 换算:-2
						4	2	HEX	否	电能表累计碳排量 Double-long 单位:Kg 换算:-2
						4	2	HEX	否	电能表累计二氧化碳排量 Double-long 单位:Kg 换算:-2
						4	2	HEX	是	剩余购电量 单位:kWh 换算:-2
						4	2	HEX	是	累计购电量 单位:kWh 换算:-2
						2	0	HEX	是	购电次数 单位:次 换算:0
						20	0	HEX	否	集成电路卡识别码 ICCID：ASCII
						30	-	-	否	预留

电能表过程执行监测数据三相具体数据内容见表 F.2。

表 F.2　电能表过程执行监测数据三相

UIDI	设备分类编码	IMEI 号	控制信息	读写	方向	长度	小数位	类型	是否必填(否:FF)	内容
15 位	110101 设备大类 + 设备中类 + 设备小类	15 位	上报数据	R	上行	7	0	BCD	是	终端时钟(BCD)年月日时分秒
						1	0	BCD	是	信号质量 CSQ：0-31
						2	0	BCD	是	信噪比 SNR：有符号
						2	0	BCD	是	RSRP。有符号整数
						2	2	BCD	是	电源电压值，单位是 0.01V
						1	0	HEX	是	上报周期
						10	0	BCD	否	北斗位置
						6	0	HEX	是	服务器 IP:HEX
						2	0	HEX	是	服务器端口:HEX
						32	0	ASCII	否	服务器域名:ASCII
						6	0	BCD	否	电能表通信地址 字节串 Octet String
						6	0	BCD	是	电能表表号 字节串 Octet String
						6	0	BCD	否	电能表客户编号 字节串 Octet String
						6	0	HEX	是	电能表额定电压 Visible String

表 F.2　电能表过程执行监测数据三相（续）

UIDI	设备分类编码	IMEI 号	控制信息	读写	方向	长度	小数位	类型	是否必填（否:FF）	内容
						6	0	HEX	是	电能表基本电流 Visible-String
						6	0	HEX	否	电能表最大电流 Visible-String
						6	0	HEX	否	电能表最小电流 Visible-String
						6	0	HEX	否	电能表转折电流 Visible-String
						4	0	HEX	是	电能表有功准确度等级 Visible-String
						4	0	HEX	是	电能表无功准确度等级 Visible-String
						4	0	HEX	是	电能表有功常数 Double-long-unsigned 单位:imp/kWh 换算:0
						4	0	HEX	是	电能表无功常数 Double-long-unsigned 单位:imp/kvarh 换算:0
						4	0	HEX	是	电能表电压互感器变比 单位:无 换算:无
						4	0	HEX	是	电能表电流互感器变比单位:无 换算:无
						2	1	HEX	是	电能表 A 相电压 Long-unsigned 单位:V 换算:-1
						2	1	HEX	是	电能表 B 相电压 Long-unsigned 单位:V 换算:-1
						2	1	HEX	是	电能表 C 相电压 Long-unsigned 单位:V 换算:-1
						4	3	HEX	是	电能表 A 相电流 Double-long 单位:A 换算:-3
						4	3	HEX	是	电能表 B 相电流 Double-long 单位:A 换算:-3
						4	3	HEX	是	电能表 C 相电流 Double-long 单位:A 换算:-3
						4	3	HEX	是	电能表零线电流 Double-long 单位:A 换算:-3
						4	1	HEX	是	电能表有功总功率 Double-long 单位:W 换算:-1
						4	1	HEX	是	电能表 A 相有功功率 Double-long 单位:W 换算:-1
						4	1	HEX	是	电能表 B 相有功功率 Double-long 单位:W 换算:-1
						4	1	HEX	是	电能表 C 相有功功率 Double-long 单位:W 换算:-1
						2	3	HEX	是	电能表总功率因数 Long 单位:无 换算:-3
						2	3	HEX	是	电能表 A 相功率因数 Long 单位:无 换算:-3
						2	3	HEX	是	电能表 B 相功率因数 Long 单位:无 换算:-3
						2	3	HEX	是	电能表 C 相功率因数 Long 单位:无 换算:-3
						2	1	HEX	否	电能表温度 Long 单位:℃ 换算:-1
						4	2	HEX	是	电能表当前组合有功总电能 Double-long 单位:kWh 换算:-2
						4	2	HEX	是	电能表当前组合有功费率 1 电能 Double-long 单位:kWh 换算:-2
						4	2	HEX	是	电能表当前组合有功费率 2 电能 Double-long 单位:kWh 换算:-2
						4	2	HEX	是	电能表当前组合有功费率 3 电能 Double-long 单位:kWh 换算:-2
						4	2	HEX	是	电能表当前组合有功费率 4 电能 Double-long 单位:kWh 换算:-2

表 F.2　电能表过程执行监测数据三相（续）

UIDI	设备分类编码	IMEI号	控制信息	读写	方向	长度	小数位	类型	是否必填(否:FF)	内容
						4	2	HEX	是	电能表当前正向有功总电能 Double-long-unsigned 单位:kWh 换算:-2
						4	2	HEX	是	电能表当前正向有功费率 1 电能 Double-long-unsigned 单位:kWh 换算:-2
						4	2	HEX	是	电能表当前正向有功费率 2 电能 Double-long-unsigned 单位:kWh 换算:-2
						4	2	HEX	是	电能表当前正向有功费率 3 电能 Double-long-unsigned 单位:kWh 换算:-2
						4	2	HEX	是	电能表当前正向有功费率 4 电能 Double-long-unsigned 单位:kWh 换算:-2
						4	2	HEX	是	电能表当前反向有功总电能 Double-long-unsigned 单位:kWh 换算:-2
						4	2	HEX	是	电能表当前反向有功费率 1 电能 Double-long-unsigned 单位:kWh 换算:-2
						4	2	HEX	是	电能表当前反向有功费率 2 电能 Double-long-unsigned 单位:kWh 换算:-2
						4	2	HEX	是	电能表当前反向有功费率 3 电能 Double-long-unsigned 单位:kWh 换算:-2
						4	2	HEX	是	电能表当前反向有功费率 4 电能 Double-long-unsigned 单位:kWh 换算:-2
						4	2	HEX	是	电能表当前 A 相正向有功电能 Double-long-unsigned 单位:kWh 换算:-2
						4	2	HEX	是	电能表当前 B 相正向有功电能 Double-long-unsigned 单位:kWh 换算:-2
						4	2	HEX	是	电能表当前 C 相正向有功电能 Double-long-unsigned 单位:kWh 换算:-2
						4	2	HEX	是	电能表当前 A 相反向有功电能 Double-long-unsigned 单位:kWh 换算:-2
						4	2	HEX	是	电能表当前 B 相反向有功电能 Double-long-unsigned 单位:kWh 换算:-2
						4	2	HEX	是	电能表当前 C 相反向有功电能 Double-long-unsigned 单位:kWh 换算:-2
						4	2	HEX	否	电能表累计碳排量 Double-long 单位:Kg 换算:-2
						4	2	HEX	否	电能表累计二氧化碳排量 Double-long 单位:Kg 换算:-2
						4	2	HEX	是	剩余购电量 单位:kWh 换算:-2
						4	2	HEX	是	累计购电量 单位:kWh 换算:-2
						2	0	HEX	是	购电次数 单位:次 换算:0
						20	0	HEX	否	集成电路卡识别码 ICCID：ASCII
						30	0	HEX	-	预留

附 录 G
（资料性）
光伏发电数据

光伏发电数据具体数据内容见表 G.1。

表 G.1 光伏发电数据

UIDI	IMEI 号	控制信息	读写	方向	长度	小数位	类型	是否必填（否:FF）	内容
15 位	15 位	上报数据	R	上行	7	0	BCD	是	终端时钟(BCD)年月日时分秒 YYYYMMDDhhmmss
					1	0	BCD	是	信号质量 CSQ：0-31
					2	0	BCD	是	信噪比 SNR：有符号
					2	0	BCD	是	RSRP。有符号整数
					2	2	BCD	是	电源电压值，单位是 0.01V
					1	0	HEX	是	上报周期(日周月年)FF(01 日；02 周；03 月；04 年)
					10	0	BCD	否	北斗位置
					6	0	HEX	是	服务器 IP:HEX
					2	0	HEX	是	服务器端口:HEX
					32	0	ASCII	否	服务器域名:ASCII
					8	0	HEX	是	组件 ID/序列号
					1	0	HEX	是	组件状态 On/off 达到一定输出电压或电流，即认为组件在工作
					2	0	HEX	是	组件面积 m2
					4	2	HEX	是	输出电流 A
					4	2	HEX	是	输出电压 V
					4	2	HEX	是	输出功率 W
					2	2	HEX	是	环境温度° C
					2	2	HEX	是	组件温度° C
					2	1	HEX	是	辐照度 W/m^2
					1	0	BCD	是	组件效率%
					2	2	HEX	是	当日累计发电量 KWh
					4	2	HEX	是	当月累计发电量 KWh
					4	2	HEX	是	当年累计发电量 KWh
					5	2	HEX	是	总累计发电量 KWh
					2	1	BCD	是	组件方位角 度
					2	1	BCD	是	组件倾斜角 度
					2	2	HEX	是	开路电压 V
					2	2	HEX	是	短路电流 A
					1	0	BCD	是	组件二极管状态 On/off
					20	0	ASCII	是	ICCID：ASCII
					30	-	-	-	预留（自定义）

附 录 H
（资料性）
风力发电数据

风力发电数据具体数据内容见表 H.1。

表 H.1 风力发电数据

UIDI	IMEI号	控制信息	读写	方向	长度	小数位	类型	是否必填(否:FF)	内容
15位	15位	上报数据	R	上行	7	0	BCD	是	终端时钟(BCD)年月日时分秒 YYYYMMDDhhmmss
					1	0	BCD	是	信号质量 CSQ：0-31
					2	0	BCD	是	信噪比 SNR：有符号
					2	0	BCD	是	RSRP。有符号整数
					2	2	BCD	是	电源电压值，单位是 0.01V
					1	0	HEX	是	上报周期
					10	0	BCD	否	北斗位置
					6	0	HEX	是	服务器 IP:HEX
					2	0	HEX	是	服务器端口:HEX
					32	0	ASCII	否	服务器域名:ASCII
					6	0	HEX	是	风机编号
					8	0	HEX	是	天气
					1	0	HEX	是	风速
					2	0	HEX	是	风向
					6	2	HEX	是	发电量
					6	2	HEX	是	上网电量
					6	2	HEX	是	购网电量
					4	0	HEX	是	等效利用小时数
					4	2	HEX	是	本机用电量
					2	0	HEX	否	场用电率
					2	0	HEX	否	场损率
					2	0	HEX	否	送出线损率
					2	0	HEX	否	风能利用系数
					4	0	HEX	是	风机功率
					3	2	HEX	是	温度
					2	0	HEX	是	振动
					2	0	HEX	是	转速
					2	0	BCD	是	正常运行机组数
					2	0	BCD	是	停机数
					2	2	HEX	是	报警内容
					4	2	HEX	是	平均风速
					4	2	HEX	是	有效风时数
					1	0	HEX	是	空气密度
					20	0	ASCII	是	ICCID：ASCII

电信终端产业协会团体标准

能源物联网设备通信数据安全技术要求和测试方法

T/TAF 103-2021

*

电信终端产业协会印发
地址：北京市西城区新街口外大街 28 号
电话：010-82052809
电子版发行网址：www.taf.org.cn