ICS 35.020

# Q/GDW

国 家 电 网 有 限 公 司 企 业 标 准

Q/GDW 12186—2021

# 输变电设备物联网通信安全规范

Communication security standard for the internet of things for power transmission and transformation equipment

2021-12-06 发布　　2021-12-06 实施

国家电网有限公司　　发 布

# 目　　次

# 前　言

为规范输变电场景下感知层设备接入管理信息大区与互联网大区时的通信安全防护要求，制定本标准。

本标准由国家电网有限公司设备管理部提出并解释。

本标准由国家电网有限公司科技部归口。

本标准起草单位：国网河北省电力有限公司电力科学研究院、国网河北省电力有限公司、南瑞集团有限公司、国网江苏省电力有限公司、国网四川省电力公司、国网安徽省电力有限公司、国网天津市电力公司、国网浙江省电力有限公司、国网信息通信产业集团有限公司、北京国网富达科技发展有限责任公司、保定天威新域科技发展有限公司。

本标准主要起草人：张克谦、常硕、贾骏、高树国、穆文喆、岳国良、邵进、冯笑、程阳、韦小刚、练永兵、曾军、申金平、乔国华、何瑞东、路艳巧、刘金锁、王晔、郭靓、屠正伟、郑鹏超、高方玉、胡成博、秦剑华、李旭旭、罗磊、赵常威、钱宇骋、冯军基、文清丰、成敬周、许飞、师璞、田如钢、王伟、贾晓峰、高艳海、邵洪林、赵振华、田源、姚陶、刘海峰、宋敬良、段泽龙、吕红志、王鹏、金春雷、汪苑、徐欢、陆莎、王朝兴、陈国广、徐春晖。

本标准首次发布。

本标准在执行过程中的意见或建议反馈至国家电网有限公司科技部。

# 输变电设备物联网通信安全规范

## 1 范围

本标准规定了输变电场景下传感终端、涉控终端、移动作业终端、视频装置、汇聚节点、边缘物联代理等感知层设备接入公司管理信息大区与互联网大区的通信安全要求。

本标准适用于输变电设备物联网的通信安全防护。

## 2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 22239 信息安全技术网络安全等级保护基本要求

GM/T 0002 SM4分组密码算法

GM/T 0009 SM2密码算法使用规范

GM/T 0044 SM9标识密码算法

Q/GDW 11712 电网资产统一身份编码技术规范

Q/GDW 12021 输变电设备物联网节点设备无线组网协议

Q/GDW 12082 输变电设备物联网无线传感器通用技术规范

## 3 术语和定义

下列术语和定义适用于本文件。

3.1

**输变电设备物联网** Internet of Things for power transmission and transformation equipment

以实现输变电设备状态信息感知、互联互通及智能化应用的物联网。

[Q/GDW 12021，定义3.1]

3.2

**接入节点** access node

输变电设备物联网的感知层中的通信主设备，具备边缘计算、自组网和终端接入的功能。

[Q/GDW 12021，定义3.2]

3.3

**汇聚节点** sink node

输变电设备物联网感知层中的通信中继设备，具备自组网和终端接入的功能。

[Q/GDW 12021，定义3.3]

3.4

**传感终端** sensor terminal

输变电设备物联网感知层中的终端设备，可实现对输变电设备运行状态感知，并通过无线或者有线方式接入汇聚节点或接入节点，可分为IP化传感终端与非IP化传感终端。

[Q/GDW 12021，定义3.4]

3.5

**涉控终端** involved control terminal

输变电设备物联网感知层中的终端设备，执行物联网指令，控制辅助设备启停等物理动作，并通过无线或者有线方式接入汇聚节点或接入节点。例如电机控制器、空调控制终端、水泵控制终端、通风除湿控制终端等。

3.6

**边缘物联代理** IoT edge agent

对各类智能传感器、智能业务终端进行统一接入、数据解析和实时计算的装置或组件。

3.7

**物联安全接入网关（高端型）** IoT security access gateway（high-end models）

一种采用SSAL、SSL VPN等技术实现对物联网终端或边缘物联代理的身份认证、网络访问控制和传输通道加密，保障电力物联网终端接入安全的防护设备。

3.8

**物联安全接入网关（低端型）** IoT security access gateway（low-end models）

一种融合SSAL、SSL VPN安全接入与基于双主机电路交换的网闸隔离两种安全防护措施的隔离网关设备，主要部署于变电站内部，用于无线终端本地接入变电站管理信息大区网络。

3.9

**信息安全网络隔离装置（逻辑型）** information security network isolation device（logic）

一种用于国家电网有限公司管理信息大区对外隔离的专用安全防护设备，可提供逻辑强隔离状态下的跨边界代理访问服务。

3.10

**信息安全网络隔离装置（网闸型）** information security network isolation device（GAP）

一种用于国家电网有限公司管理信息大区对外隔离的专用安全防护设备，可提供基于双主机电路交换的网闸隔离功能。

3.11

**安全芯片** security chip

包含操作系统和加解密运算单元的集成电路，可以实现安全存储、数据加/解密、身份认证、存取权限控制、网络通道加密传输等安全控制功能。

3.12

**数字证书** digital certificate

一个经证书授权中心签名的包含公开密钥拥有者信息以及公开密钥的文件。

3.13

**可信根** root of trust

接入设备的基础安全组件，通常为一组隐式的可信函数，系统或设备的其余部分可使用这些函数确保其安全性，是设备制造商建立可信的基础。

## 4 缩略语

下列缩略语适用于本文件。

APN：接入点（Access Point Name）

IBC：基于标识的密码体系（Identity-Based Cryptography）

ID：身份标识（Identifier）

IPSec：互联网安全协议（Internet Protocol Security）
SSAL：国家电网有限公司安全应用层（State Grid Secure Application Layer）
SSL：安全套接字协议（Secure Sockets Layer）

## 5 总体防护

### 5.1 防护架构

输变电设备物联网通信安全总体防护架构如图1所示，感知层、网络层、平台层和应用层的防护策略分别为：

a) 感知层设备包括传感终端、涉控终端、移动作业终端、视频装置以及汇聚节点、接入节点、视频接入主机等，输变电设备物联网典型传感终端与典型涉控终端参见附录A。感知层应通过身份认证、访问控制、数据加密、自身监测和日志审计等措施对仿冒接入、非法控制、数据泄漏和数据篡改等风险进行防控。感知层设备至少应有唯一身份标识，涉控终端、移动作业终端与站内无线视频装置应采用身份认证、数据加密、自身监测的安全防护策略，汇聚节点对接传感终端时应采用访问控制、自身监测的安全防护策略，汇聚节点对接涉控终端时应采取身份认证、访问控制、自身监测的安全防护策略，边缘物联代理应采用身份认证、数据加密、访问控制、自身监测、安全管理、日志审计等安全防护策略；
b) 网络层接入有光纤专网和无线两种方式，无线接入分为无线APN专网、公司无线专网与无线公网三种方式。网络层的安全防护应符合GB/T 22239规定。采用光纤专网接入时，边缘物联代理经过防火墙接入平台层，应与平台层进行双向身份认证与数据加密。管理信息大区通过物联安全接入网关（高端型）和信息安全网络隔离装置（网闸型）接入至平台层，互联网大区通过物联安全接入网关（高端型）接入至平台层。终端应与物联安全接入网关 （高端型）进行双向身份认证和数据加密，对仿冒接入和数据泄漏等风险进行防控；
c) 平台层汇集物联采集数据，实现物联网设备管理、边缘计算配置和海量数据存储，其安全防护应符合GB/T 22239规定；
d) 应用层对物联网感知数据进行高级分析与应用，实现信息共享和辅助决策，其安全防护应符合GB/T 22239规定。

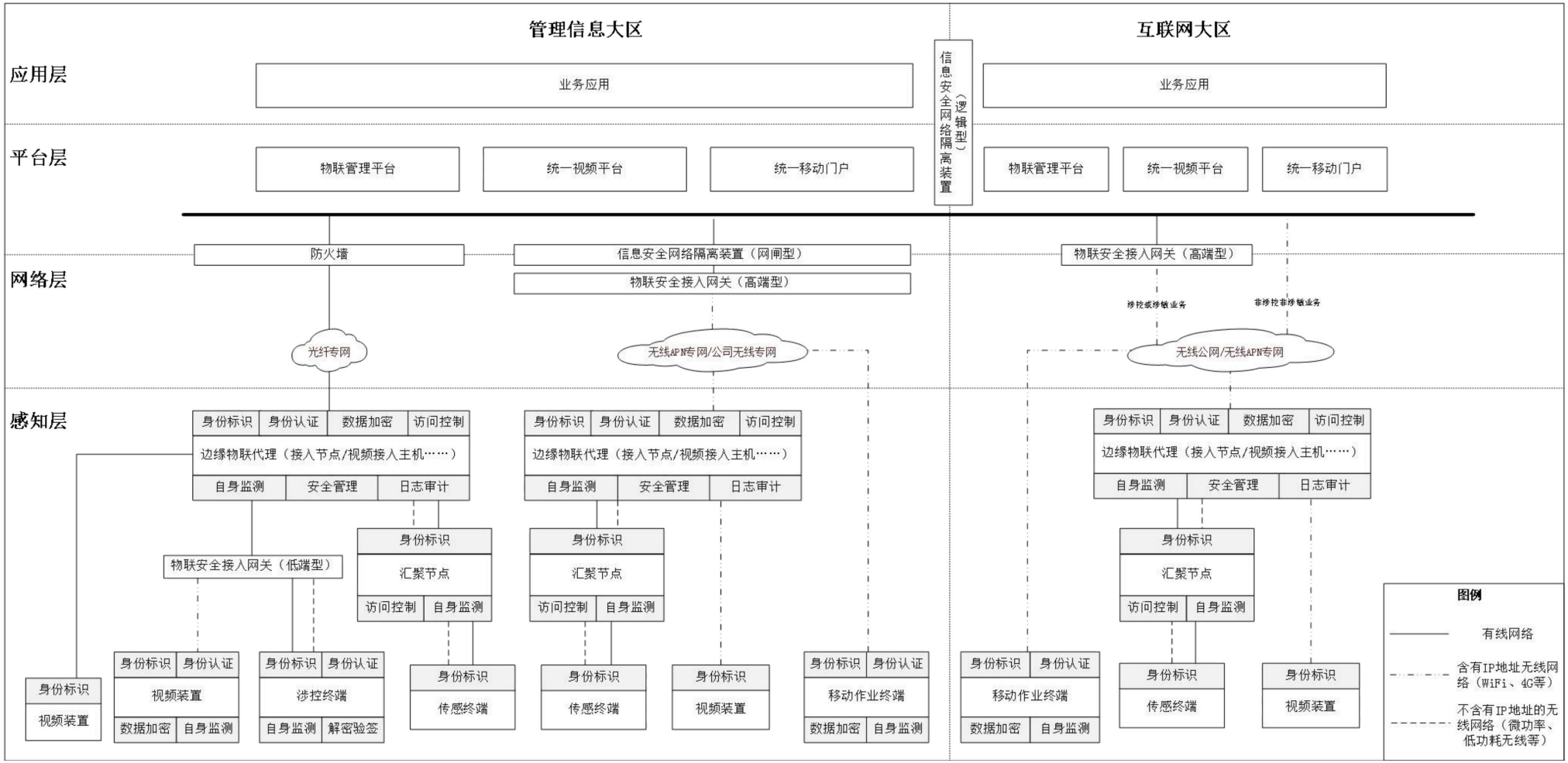



图 1　输变电设备物联网总体防护架构

### 5.2 数据安全

针对商密数据、企业重要数据、一般数据三种数据应分别采取以下防护策略：

a) 商密数据包含电网拓扑接线图等数据，此类数据含有坐标信息，禁止在互联网大区数据库中存储；

b) 重要数据包含线路台账、人员台账等基础信息数据，此类数据可存储于互联网大区数据库中服务于业务应用，存储时间应少于3个月。当脱离互联网大区对外提供时，应采取数据脱敏、数字水印和数据审计等措施；

c) 一般数据包含监控数据、巡检数据、作业数据、灾害数据等普通业务数据，此类数据针对不同应用需求，可采取适当灵活的安全措施，无存储时间要求。

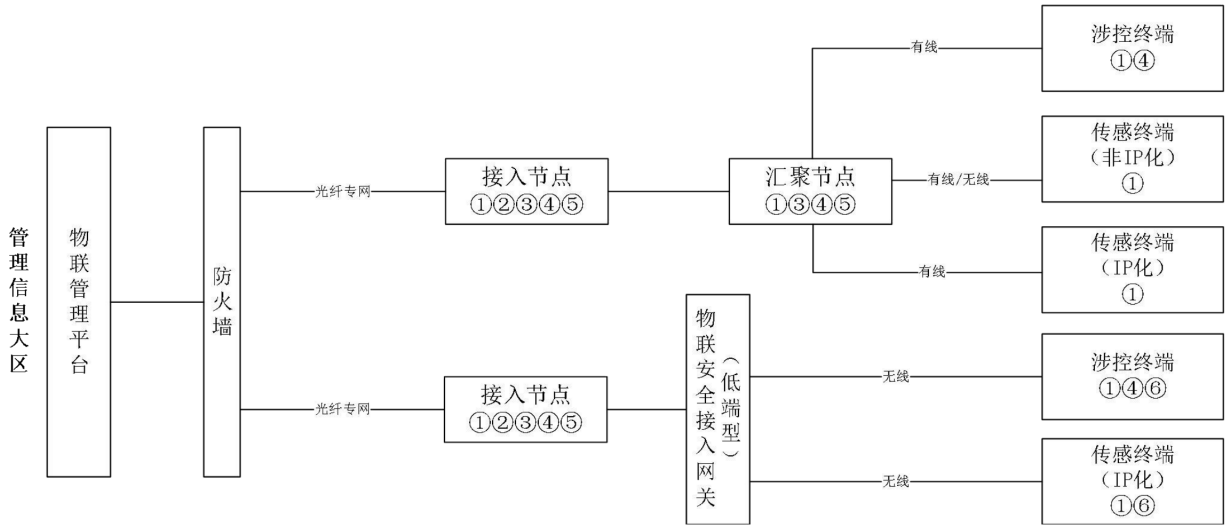
### 5.3 跨区通信安全

管理信息大区与互联网大区应通过信息安全网络隔离装置（逻辑型）进行逻辑隔离，可双向部署以实现双向数据交换。

## 6 传感终端与涉控终端光纤专网接入场景安全要求

### 6.1 典型架构

光纤专网接入方式主要适用于变电站、换流站等站内接入管理信息大区的场景，其典型接入架构及安全要求见图2。非IP化传感终端，如：温湿度、水浸、水位、形变等输变电设备物联网传感终端（见表 A.1 ），可通过汇聚节点/接入节点接入管理信息大区；涉控终端（见表 A.2）和IP化传感终端，应通过物联安全接入网关（低端型）接入管理信息大区。




序号说明：

①——表示在接入节点的网络中应具有唯一网络身份标识；

②——表示接入节点北向通信时应与物联管理平台进行双向身份认证，并对传输数据进行加密；

③——表示应具备访问控制功能；

④——表示应具备对自身软硬件安全监测的功能；

⑤——表示应具备安全管理与日志审计的功能；

⑥——表示在接入时应使用安全芯片、TF加密卡或加密模块等方式与物联安全接入网关进行双向身份认证，并对传输数据进行加密。

注：此图中仅有通过无线连接的涉控终端与IP化传感终端经过物联安全接入网关（低端型）接入。

图 2 传感终端与涉控终端光纤专网接入场景典型架构

### 6.2 通用要求

感知层设备在接入节点的网络中应具有唯一网络身份标识，身份标识编码的构成、使用及维护应符合Q/GDW 12082中附录B的规定。

### 6.3 接入要求

#### 6.3.1 身份认证与数据加密

经过物联安全接入网关（低端型）的涉控终端与IP化传感终端在接入时应满足以下要求：

a) 应使用安全芯片、TF卡或加密模块等方式通过物联安全接入网关（低端型）接入至接入节点；
b) 应采用国产密码算法和公司统一密码基础设施签发的数字证书，基于公司SSAL、SSL VPN或IPSec VPN协议，实现双向认证和数据加密，并满足公司物联安全接入网关对接技术要求，宜采用SM2密码算法或SM9密码算法，算法分别见GM/T 0009和GM/T 0044，认证流程（以SM9为例）参见附录C；
c) 传输数据加密时，应使用国密对称算法SM1或SM4，加密密钥应协商获得，不应采用固定密钥。SM1算法使用硬件接口加解密，SM4算法采用GM/T 0002的密码算法。

#### 6.3.2 自身监测

涉控终端应具备对自身软硬件安全监测的功能，满足GB/T 22239中6.1.4.5的要求，发现系统程序或引导程序的可信性受到破坏的事件并告警，参见附录D.1。

#### 6.3.3 解密验签

应用层对控制命令进行加密，涉控终端应具备对控制指令进行解密的功能，加密密钥协商获得，不应采用固定密钥，宜采用GM/T 0002规定的国密对称SM4密码算法

### 6.4 汇聚节点接入要求

#### 6.4.1 汇聚节点分类

对于具备边缘计算功能的汇聚节点，应满足本章节的要求。对于只具备数据汇聚转发功能、不具备边缘计算功能的汇聚节点不做要求。

#### 6.4.2 访问控制

汇聚节点在访问控制方面应包含但不限于以下功能：

a) 支持传感终端与涉控终端的访问控制，应拒绝未授权的传感终端与涉控终端接入请求；
b) 终止认证超时的涉控终端会话；
c) 终止超过规定次数认证失败的涉控终端建立会话，并记录身份信息。

#### 6.4.3 自身监测

汇聚节点应具备对自身软硬件安全监测的功能，满足GB/T 22239中6.1.4.5的要求，应发现系统程序或引导程序的可信性受到破坏的事件并告警，参见附录D.1。

### 6.5 接入节点接入要求

#### 6.5.1 身份认证与数据加密

接入节点通过光纤专网接入公司管理信息大区时应采用国产密码算法和公司统一密码基础设施签发的数字证书进行双向认证，对传输数据进行加密，加密密钥协商获得，不应采用固定密钥，应使用国密对称算法SM1或SM4。SM1算法使用硬件接口加解密，SM4算法采用GM/T 0002的密码算法。

#### 6.5.2 访问控制

接入节点应具备控制用户访问接入节点中应用软件和用户数据等资源的功能，应满足GB/T 22239中7.1.4.2的要求，参见附录D.2。

#### 6.5.3 自身监测

接入节点应具备对自身软硬件安全监测的功能，宜满足GB/T 22239中7.1.4.6的要求，可基于可信根对设备的引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行告警，并将验证结果形成审计记录送至物联管理平台，参见附录D.4。

### 6.5.4 安全管理

接入节点对于本地及远程配置的安全管理应包含但不限于以下功能：

a) 具备安全策略管理和日志审计等功能；
b) 具备查阅和配置认证、访问控制和数据安全传输策略等功能；
c) 具备查阅和管理日志的功能。

### 6.5.5 日志审计

接入节点的安全事件日志应包含但不限于以下信息：

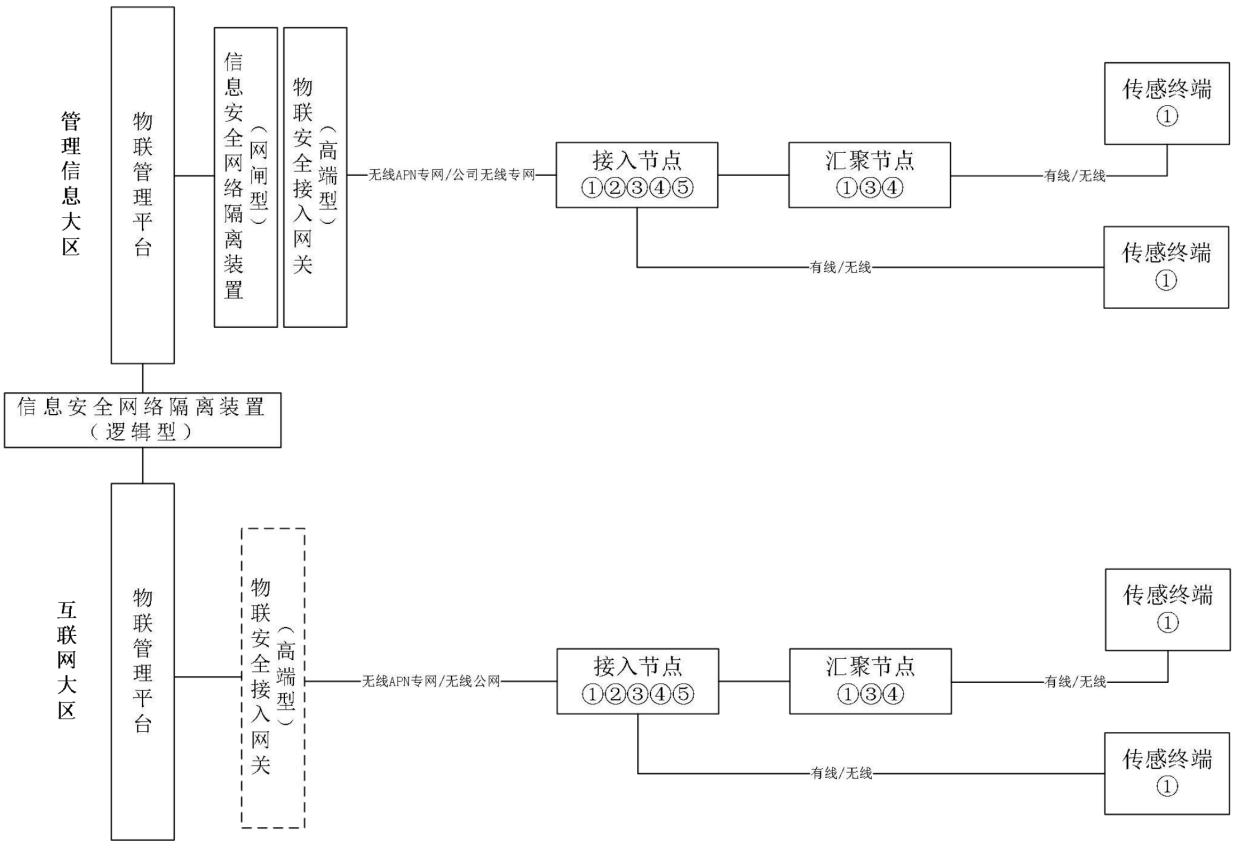
a) 记录授权认证成功和失败事件；
b) 记录接入设备认证成功和失败事件；
c) 记录系统入侵告警事件；
d) 满足GB/T 22239中7.1.3.5的要求，参见附录D.3。

## 7 传感终端无线接入场景安全要求

### 7.1 典型架构

无线接入包括无线APN专网、公司无线专网与无线公网三种方式。

公司无线专网接入方式主要适用于接入管理信息大区的输电场景；无线公网接入方式适用于通过公网接入互联网大区的输电场景；无线APN专网接入方式适用于以上两者。其典型接入架构和安全防护要求见图3。



序号说明：

①——表示在接入节点的网络中应具有唯一网络身份标识；
②——表示接入节点应使用安全芯片或TF加密卡与物联安全接入网关（高端型）进行双向身份认证，并对传输数据进行加密；
③——表示应具备访问控制功能；
④——表示应具备对自身软硬件安全监测的功能；
⑤——表示应具备安全管理与日志审计的功能。
注：互联网大区非涉控非涉敏业务可不通过物联安全接入网关（高端型）接入平台层。

**图 3　传感终端无线接入场景典型架构**

## 7.2　通用要求

感知层设备在接入节点的网络中应具有唯一网络身份标识，身份标识编码的构成、使用及维护应符合Q/GDW 12082中附录B的规定。

## 7.3　汇聚节点接入要求

### 7.3.1　汇聚节点分类

对于具备边缘计算功能的汇聚节点，应满足本章节的要求。对于只具备数据汇聚转发功能、不具备边缘计算功能的汇聚节点不作要求。

### 7.3.2　访问控制

汇聚节点在访问控制方面应包含但不限于以下功能：

a) 支持传感终端的访问控制，应拒绝未授权的传感终端接入请求；
b) 终止认证超时的传感终端会话；
c) 终止超过规定次数认证失败的传感终端建立会话，并记录身份。

### 7.3.3　自身监测

汇聚节点应具备对自身软硬件安全监测的功能，满足GB/T 22239中6.1.4.5的要求，应发现系统程序或引导程序的可信性受到破坏的事件并告警，参见附录D.1。

## 7.4　接入节点接入要求

### 7.4.1　身份认证与数据加密

接入节点接入至物联管理平台时应满足以下要求：

a) 管理信息大区应使用安全芯片或TF加密卡通过物联安全接入网关（高端型）接入至平台层；
b) 互联网大区涉及涉控或涉敏业务时应使用安全芯片或TF加密卡通过物联安全接入网关（高端型）接入至平台层；
c) 应采用国产密码算法和公司统一密码基础设施签发的数字证书，基于公司SSAL、SSL VPN或IPSec VPN协议，实现双向认证和数据加密；
d) 传输数据加密时，应使用国密对称算法SM1或SM4，加密密钥应协商获得，不应采用固定密钥。SM1算法使用硬件接口加解密，SM4算法采用GM/T 0002的密码算法。

### 7.4.2　访问控制

接入节点应具备控制用户访问接入节点中应用软件和用户数据等资源的功能，应满足GB/T 22239中7.1.4.2的要求，参见附录D.2。

### 7.4.3　自身监测

接入节点应具备对自身软硬件安全监测的功能，宜满足GB/T 22239中7.1.4.6的要求，可基于可信根对设备的引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行告警，并将验证结果形成审计记录送至物联管理平台，参见附录D.4。

### 7.4.4　安全管理

接入节点对于本地及远程配置的安全管理应包含但不限于以下功能：

a) 具备安全策略管理和日志审计等功能；
b) 具备查阅和配置认证、访问控制和数据安全传输策略等功能；
c) 具备查阅和管理日志的功能。

#### 7.4.5 日志审计

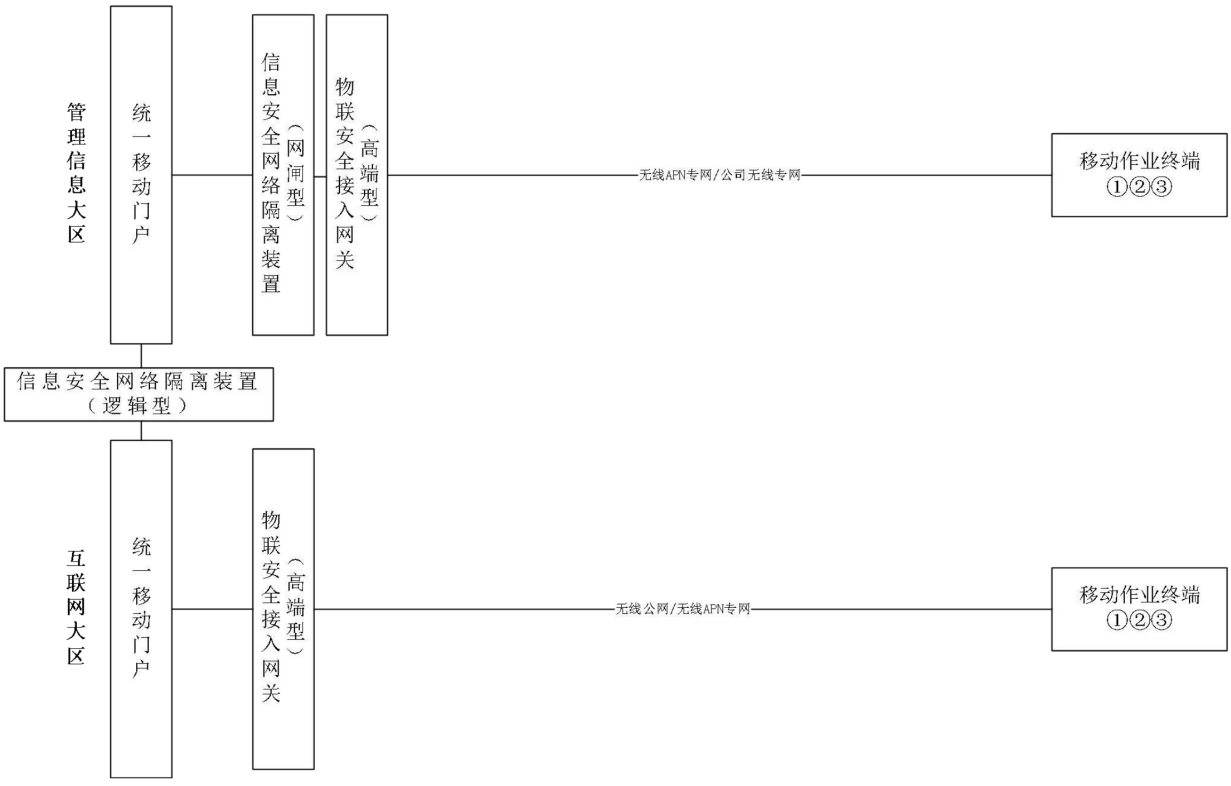
接入节点的安全事件日志应包含但不限于以下信息：

a) 记录授权认证成功和失败事件；
b) 记录接入设备认证成功和失败事件；
c) 记录系统入侵告警事件；
d) 满足GB/T 22239中7.1.3.5的要求，参见附录D.3。

## 8 移动作业终端接入场景安全要求

### 8.1 典型架构

移动作业终端通过无线APN专网、公司无线专网或无线公网经过物联安全接入网关（高端型）接入管理信息大区或互联网大区，其典型接入架构和安全防护要求见图4。




序号说明：

①——表示在公司网络中应具有唯一网络身份标识；
②——表示移动作业终端应使用TF加密卡与物联安全接入网关（高端型）进行双向身份认证，并对传输数据进行加密；
③——表示应具备对自身软硬件安全监测的功能。

图 4 移动作业终端接入场景典型架构

### 8.2 移动作业终端接入要求

#### 8.2.1 身份标识

移动作业终端在公司网络中应具有唯一网络身份标识，身份标识编码的构成、使用及维护应符合Q/GDW 12082中附录B的规定。

#### 8.2.2 身份认证与数据加密

移动作业终端在接入时应满足以下要求：

a) 应使用TF加密卡通过物联安全接入网关（高端型）接入至平台层；
b) 应采用国产密码算法和公司统一密码基础设施签发的数字证书，基于公司SSAL、SSL VPN或IPSec VPN协议，实现双向认证和数据加密，并满足公司物联安全接入网关对接技术要求；
c) 传输数据加密时，应使用国密对称算法SM1或SM4，加密密钥应协商获得，不应采用固定密钥。SM1算法使用硬件接口加解密，SM4算法采用GM/T 0002的密码算法。

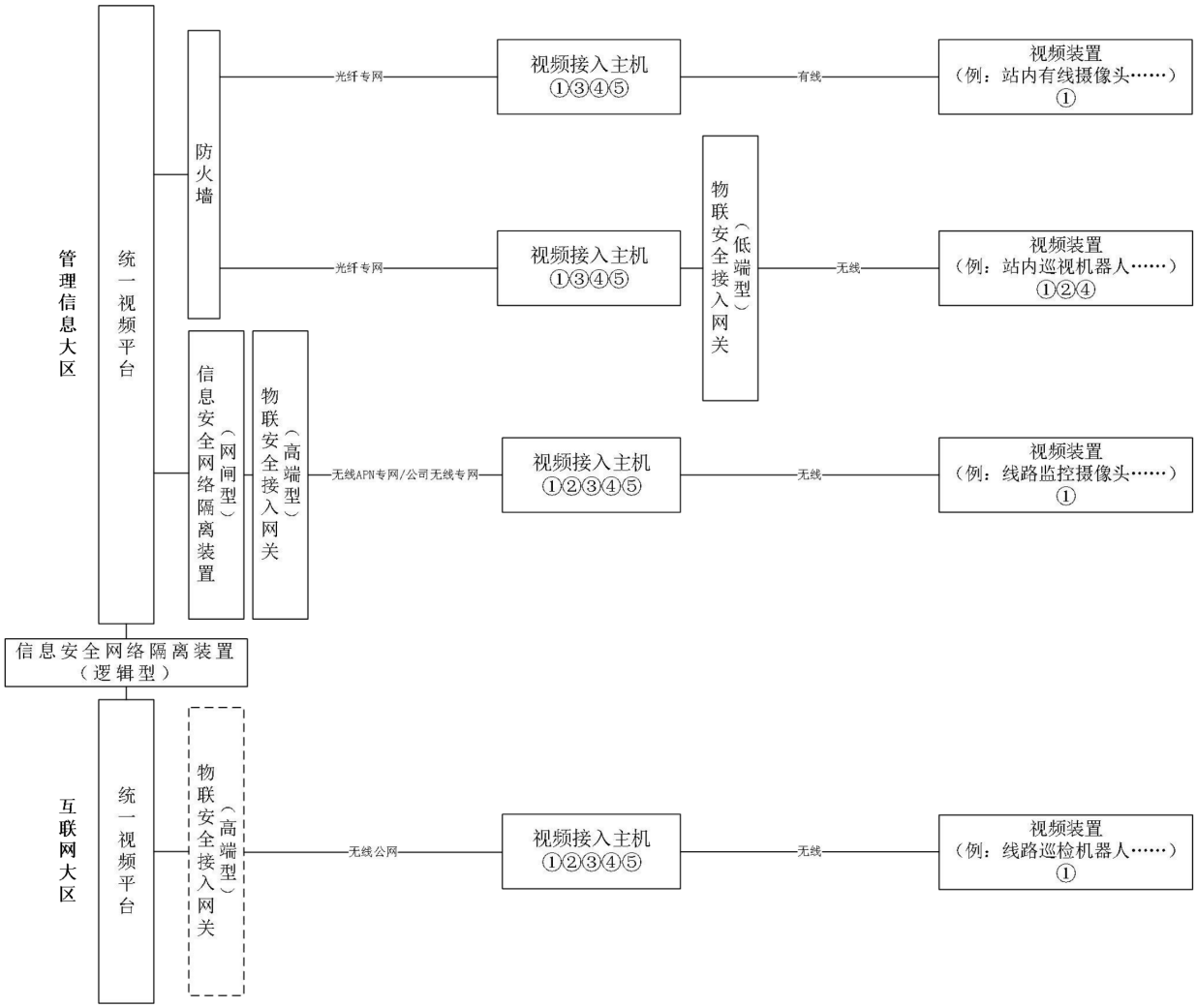
#### 8.2.3 自身监测

移动作业终端应具备对自身软硬件安全监测的功能，满足GB/T 22239中6.1.4.5的要求，发现系统程序或引导程序的可信性受到破坏的事件并告警，参见附录D.1。

## 9 视频装置接入场景安全要求

### 9.1 典型架构

视频装置在监测监控类业务场景中均有应用，例如摄像头、机器人、无人机、智能穿戴设备等，根据视频装置部署的地理位置、连接方式的不同，视频接入主机与视频装置应遵循不同的安全防护要求。其典型接入架构和安全防护要求见图5。




序号说明：

①——表示在视频接入主机的网络中应具有唯一网络身份标识；

②——表示视频接入主机或视频装置应使用安全芯片、TF加密卡或加密模块与物联安全接入网关进行双向身份认证，并对传输数据进行加密；

③——表示应具备访问控制功能；

④——表示应具备对自身软硬件安全监测的功能；

⑤——表示应具备安全管理与日志审计的功能。

注：互联网大区非涉控非涉敏业务可不通过物联安全接入网关（高端型）接入平台层。

**图 5　视频装置接入场景典型架构**

## 9.2　通用要求

感知层设备在视频接入主机的网络中应具有唯一网络身份标识，身份标识编码的构成、使用及维护应符合Q/GDW 12082中附录B的规定。

## 9.3　站内无线视频装置接入要求

### 9.3.1　身份认证与数据加密

站内无线视频装置在接入视频接入主机时应满足以下要求：

d)　应使用安全芯片、TF卡或加密模块通过物联安全接入网关（低端型）接入至视频接入主机；

e)　应采用国产密码算法和公司统一密码基础设施签发的数字证书，基于公司SSAL、SSL VPN或IPSec VPN协议，实现双向认证和数据加密，并满足公司物联安全接入网关对接技术要求；

f) 传输数据加密时，应使用国密对称算法SM1或SM4，加密密钥应协商获得，不应采用固定密钥。SM1算法使用硬件接口加解密，SM4算法采用GM/T 0002的密码算法。

#### 9.3.2 自身监测

站内无线视频装置应具备对自身软硬件安全监测的功能，满足GB/T 22239中6.1.4.5的要求，发现系统程序或引导程序的可信性受到破坏的事件并告警，参见附录D.1。

### 9.4 视频接入主机接入要求

#### 9.4.1 身份认证与数据加密

通过无线APN专网、公司无线专网或无线公网接入方式的视频接入主机在接入平台层时应满足以下要求：

a) 管理信息大区应使用安全芯片或TF卡通过物联安全接入网关（高端型）接入至平台层；
b) 互联网大区涉及涉控或涉敏业务的视频接入主机应使用安全芯片或TF卡通过物联安全接入网关（高端型）接入至平台层；
c) 应采用国产密码算法和公司统一密码基础设施签发的数字证书，基于公司SSAL、SSL VPN或IPSec VPN协议，实现双向认证和数据加密，并满足公司物联安全接入网关对接技术要求；
d) 传输数据加密时，应使用国密对称算法SM1或SM4，加密密钥应协商获得，不应采用固定密钥。SM1算法使用硬件接口加解密，SM4算法采用GM/T 0002的密码算法。

#### 9.4.2 访问控制

视频接入主机应具备控制用户访问自身设备中应用软件和用户数据等资源的功能，应满足GB/T 22239中7.1.4.2的要求，参见附录D.2。

#### 9.4.3 自身监测

视频接入主机应具备对自身软硬件安全监测的功能，宜满足GB/T 22239中7.1.4.6的要求，可基于可信根对设备的引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行告警，并将验证结果形成审计记录送至物联管理平台，参见附录D.4。

#### 9.4.4 安全管理

视频接入主机对于本地及远程配置的安全管理应包含但不限于以下功能：

a) 具备安全策略管理和日志审计等功能；
b) 具备查阅和配置认证、访问控制和数据安全传输策略等功能；
c) 具备查阅和管理日志的功能。

#### 9.4.5 日志审计

视频接入主机的安全事件日志应包含但不限于以下信息：

a) 记录授权认证成功和失败事件；
b) 记录接入设备认证成功和失败事件；
c) 记录系统入侵告警事件；
d) 满足GB/T 22239中7.1.3.5的要求，参见附录D.3。

# 附 录 A
（资料性附录）
# 输变电设备物联网典型传感终端与典型涉控终端

输变电设备物联网典型传感终端和典型涉控终端分别见表A.1和表A.2。

**表 A.1 典型传感终端**

| 序号 | 名称 |
|---|---|
| 1 | 温/湿度传感器 |
| 2 | 水浸/水位传感器 |
| 3 | 形变传感器 |
| 4 | 烟感传感器 |
| 5 | 避雷器泄漏电流传感器 |
| 6 | 局部放电传感器 |
| 7 | 电流传感器 |
| 8 | 风偏传感器 |
| 9 | 绝缘子泄漏电流传感器 |
| 10 | 杆塔倾斜角传感器 |
| 11 | 气象传感器 |
| 12 | 有害气体/可燃气体传感器 |
| 13 | 断路器机械特性传感器 |
| 14 | 倾角传感器 |
| 15 | 测流传感器 |
| 16 | 气象传感器 |
| 17 | 振动传感器 |
| 18 | 舞动传感器 |
| 19 | 门磁传感器 |
| 20 | 压力传感器 |
| 21 | 油气压力传感器 |
| 22 | 氢气浓度传感器 |
| 23 | 导线运动监测球 |
| 24 | 拉力传感器 |
| 25 | 位移传感器 |
| 26 | 距离传感器 |

**表A.2 典型涉控终端**

| 序号 | 名称 |
|---|---|
| 1 | 电机控制器 |
| 2 | 空调控制终端 |
| 3 | 水泵控制终端 |
| 4 | 通风除湿控制终端 |

# 附 录 B
（资料性附录）
基于 IBC 体系的轻量级接入认证流程及报文示例

## B.1 接入认证流程

### B.1.1 流程概述

本接入认证方法适用于感知层设备间的通信，轻量级接入认证主要基于IBC标识认证体系实现，不使用数字证书，去中心化认证，降低现场实施难度，提高实体身份认证效率。以国密SM9为例，安全接入流程分为两个阶段，此处的“密钥生成中心”应使用公司统一密码基础设施，流程见图B.1。

### B.1.2 私钥申请

此阶段交互主体双方为终端与密钥生成中心或者对端（汇聚、接入）与密钥生成中心。私钥申请流程如下：

a) 终端或对端（汇聚、接入）向密钥生成中心发送申请系统参数报文；
b) 密钥生成中心收到后发送系统参数，终端收到后保存系统参数；
c) 终端或对端（汇聚、接入）预置密钥生成中心公钥（密钥生成中心标识），随机生成一个SM4密钥，用密钥生成中心公钥对SM4密钥进行加密，与终端或对端（汇聚、接入）的设备ID一起作为私钥申请报文发送给密钥生成中心；
d) 密钥生成中心收到报文后拿到终端或对端（汇聚、接入）的设备ID，并用密钥生成中心私钥解析出SM4密钥；检测终端或对端（汇聚、接入）设备ID是否合法，检测通过后（设备ID+有效期）作为设备公钥，计算设备私钥；用获取到的SM4密钥对设备私钥进行加密，并用密钥生成中心私钥对加密后的数据签名，与有效期一起发送给终端或对端（汇聚、接入）；
e) 终端或对端（汇聚、接入）收到应答报文，验签成功后用SM4密钥解密，得到私钥和有效期，（设备ID+有效期）为公钥，这样终端或对端（汇聚、接入）就得到与自身设备ID相关的公私钥对。

### B.1.3 认证协商

此阶段交互主体双方为终端与对端（汇聚、接入）。认证协商流程如下：

a) 终端将自身设备ID和私钥有效期一起发给对端，对端（汇聚、接入）收到后将终端设备ID和有效期组合成终端公钥；
b) 对端（汇聚、接入）将自身设备ID和私钥有效期一起发送给终端，终端收到将对端（汇聚、接入）的设备ID和有效期组合成对端（汇聚、接入）公钥；
c) 终端选取随机数r1,用对端（汇聚、接入）公钥对r1加密，然后用终端私钥对加密数据签名作为申请报文发送给对端（汇聚、接入）；
d) 对端（汇聚、接入）收到申请报文后首先用终端公钥验签，通过后用对端（汇聚、接入）私钥解密出r1；对端（汇聚、接入）选取随机数r2，用终端公钥对r2加密，然后用对端（汇聚、接入）私钥对加密数据签名作为应答报文发送给终端；
e) 终端收到应答报文后首先用对端（汇聚、接入）公钥验签，通过后用终端私钥解解密出r2；终端计算r1与r2的异或值，并对其进行散列，将散列结果作为确认报文发送给对端（汇聚、接入）；
f) 对端（汇聚、接入）收到确认报文后对r1、r2作同样操作，计算后与确认报文中作对比，如果一致就完成认证协商过程。

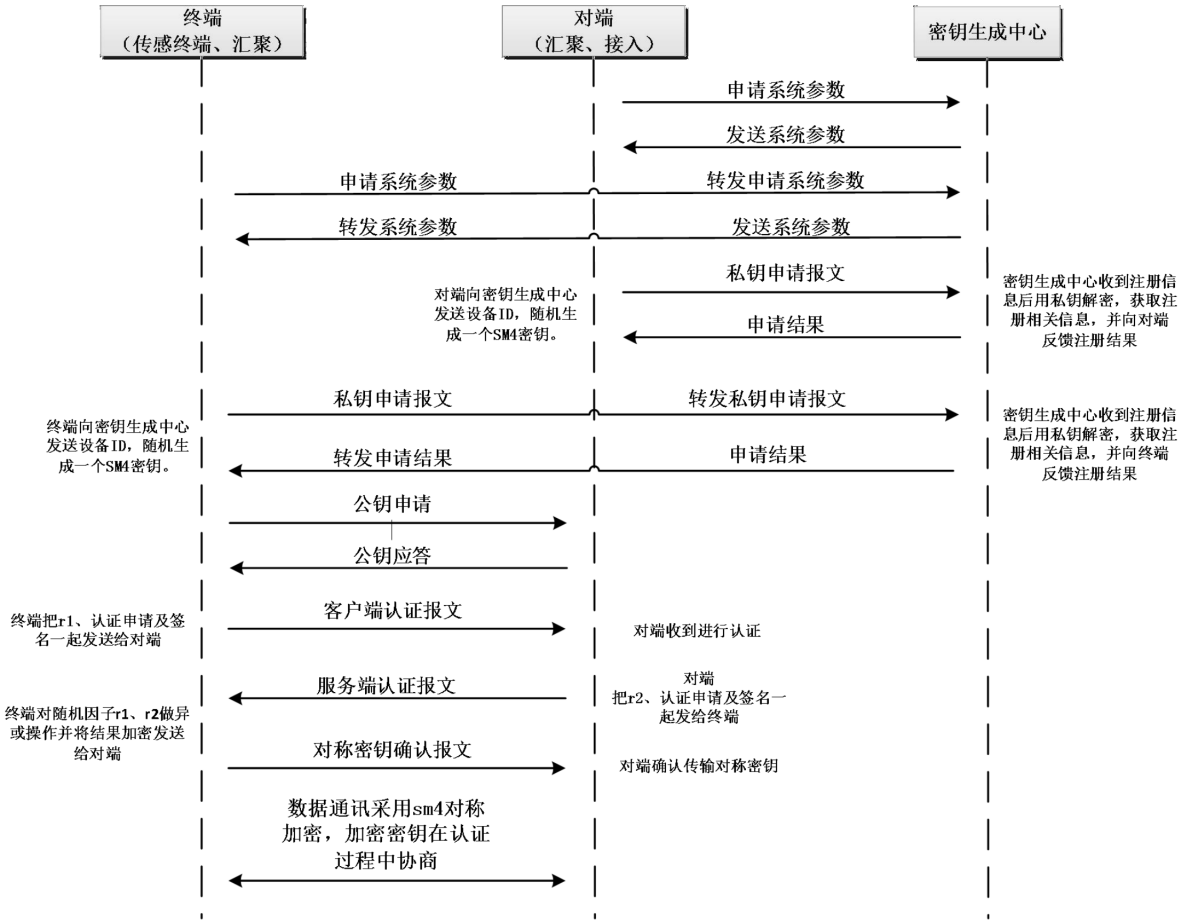



图 B.1　基于 IBC 体系的轻量级接入认证流程

## B.2　身份认证报文格式示例

身份认证报文格式示例见表B.1～B.10：

表B.1　参数申请报文

| 名称 | 长度 | 内容 | 说明 |
|---|---|---|---|
| 类型 | 1 | 1 | 参数申请 |
| 子类型 | 1 | 1 | 请求 |
| 长度 | 2 | 5+m | 报文总长度（网络序） |
| 标识长度 | 1 | ID 长度 | 不超过 32 |
| 标识 | m | ID | 注册设备唯一标识，长度不超过 32 |

表B.2　参数应答报文

| 名称 | 长度 | 内容 | 说明 |
|---|---|---|---|
| 类型 | 1 | 1 | 参数申请 |
| 子类型 | 1 | 2 | 应答 |
| 长度 | 2 | 197+m | 报文总长度（网络序） |
| 标识长度 | 1 | ID 长度 | 不超过 32 |
| ID | m | ID | 注册设备唯一标识，长度不超过 32 |

表B.2 （续）

| 名称 | 长度 | 内容 | 说明 |
|---|---|---|---|
| 签名主公钥 | 64 | 签名主公钥 | 明文发送 |
| 加密主公钥 | 128 | 加密主公钥 | 明文发送 |

表B.3 私钥申请报文

| 名称 | 长度 | 内容 | 说明 |
|---|---|---|---|
| 类型 | 1 | 2 | 私钥申请 |
| 子类型 | 1 | 1 | 请求 |
| 长度 | 2 | 5+m+n | 报文总长度（网络序） |
| 标识长度 | 1 | ID 长度 | 不超过 32 |
| ID | m | ID | 注册设备唯一标识，长度不超过 32 |
| E(SM4key) | n | 应答时用于 SM4 加密的 16 字节密钥 | SM4 加密密钥由终端生成,此密钥仅用于私钥申请阶段 |

表B.4 私钥应答报文

| 名称 | 长度 | 内容 | 说明 |
|---|---|---|---|
| 类型 | 1 | 2 | 私钥申请 |
| 子类型 | 1 | 2 | 应答 |
| 长度 | 2 | 297+m | 报文总长度（网络序） |
| 标识长度 | 1 | ID 长度 | 不超过 32 |
| ID | m | ID | 注册设备唯一标识，长度不超过 32 |
| 有效期 | 4 | 4 字节时间戳 | 密钥申请有效时间，网络序 |
| E(DS+DE) | 192 | 用户签名私钥和用户加密私钥，使用 SM4 加密 | 前 64 个字节为用户签名私钥<br>后 128 个字节为用户加密私钥<br>合并后用 SM4 加密 |
| 签名 | 96 | 对数据（ID\|\|有效期\|\|E(DS+DE)）签名 | 用本端签名私钥对对数据（ID\|\|有效期\|\|E(DS+DE)）的签名 |

表B.5 公钥申请报文

| 名称 | 长度 | 内容 | 说明 |
|---|---|---|---|
| 类型 | 1 | 3 | 公钥申请 |
| 子类型 | 1 | 1 | 请求 |
| 长度 | 2 | 9+m | 报文总长度（网络序） |
| 标识长度 | 1 | ID 长度 | 不超过 32 |
| ID | m | ID | 请求方设备唯一标识，长度不超过 32 |
| 有效期 | 4 | 4 字节时间戳 | 密钥申请有效时间（网络序） |

表B.6 公钥应答报文

| 名称 | 长度 | 内容 | 说明 |
|---|---|---|---|
| 类型 | 1 | 3 | 公钥申请 |

表B.6 （续）

| 名称 | 长度 | 内容 | 说明 |
|---|---|---|---|
| 子类型 | 1 | 2 | 应答 |
| 长度 | 2 | 9+m | 报文总长度（网络序） |
| 标识长度 | 1 | ID 长度 | 不超过 32 |
| ID | m | ID | 应答方设备唯一标识，长度不超过 32 |
| 有效期 | 4 | 4 字节时间戳 | 密钥申请有效时间（网络序） |

表B.7 认证申请报文

| 名称 | 长度 | 内容 | 说明 |
|---|---|---|---|
| 类型 | 1 | 4 | 表示协商过程 |
| 子类型 | 1 | 1 | 请求 |
| 长度 | 2 | 213+m | 报文总长度（网络序） |
| 标识长度 | 1 | ID 长度 | 不超过 32 |
| ID | m | ID | 请求方设备唯一标识，长度不超过 32 |
| 随机数 r1 | 112 | 16 字节随机数 r1 的加密密文 | 选取 16 字节随机数 r1,用应答方公钥对其加密 |
| 签名 | 96 | 对数据（ID\|\|随机数密文）签名 | 用本端签名私钥对对数据（ID\|\|随机数密文）的签名 |

表B.8 认证应答报文

| 名称 | 长度 | 内容 | 说明 |
|---|---|---|---|
| 类型 | 1 | 4 | 表示协商过程 |
| 子类型 | 1 | 2 | 应答 |
| 长度 | 2 | 213+m | 报文总长度（网络序） |
| 标识长度 | 1 | ID 长度 | 不超过 32 |
| ID | m | ID | 应答方设备唯一标识，长度不超过 32 |
| 随机数 r2 | 112 | 16 字节随机数 r2 的加密密文 | 选取 16 字节随机数 r2,用请求方公钥对其加密 |
| 签名 | 96 | 对数据（ID\|\|申请时间\|\|有效期\|\|随机数）签名 | 用本端签名私钥对对数据（ID\|\|申请时间\|\|有效期\|\|随机数）的签名 |

表B.9 认证确认报文

| 名称 | 长度 | 内容 | 说明 |
|---|---|---|---|
| 类型 | 1 | 4 | 表示协商过程 |
| 子类型 | 1 | 3 | 确认 |
| 长度 | 2 | 37+m | 报文总长度（网络序） |
| 标识长度 | 1 | ID 长度 | 不超过 32 |
| ID | m | ID | 请求方设备唯一标识，长度不超过 32 |
| r1⊕r2 | 32 | 对异或的结果进行 hash | 对异或的结果进行 hash |

表B.10　数据传输报文

| 名称 | 长度 | 内容 | 说明 |
|---|---|---|---|
| 类型 | 1 | 5 | 表示数据传输 |
| 子类型 | 1 | 1 | 数据传输 |
| 长度 | 2 | 5+m | 报文总长度（网络序） |
| 数据 | m | 加密数据 | 传输数据用协商出的对称密钥加密 |

# 附 录 C
（资料性附录）
网络安全等级保护基本要求节选

## C.1 第一级安全要求-可信验证

可基于可信根对计算设备的系统引导程序、系统程序等进行可信验证，并在检测到其可信性受到破坏后进行报警。

[来源：GB/T 22239，6.1.4.5]

## C.2 第二级安全要求-访问控制

本项要求包括：

a) 应对登录的用户分配账户和权限；
b) 应重命名或删除默认账户，修改默认账户的默认口令；
c) 应及时删除或停用多余的、过期的账户，避免共享账户的存在；
d) 应授予管理用户所需的最小权限，实现管理用户的权限分离。

[来源：GB/T 22239，7.1.4.2]

## C.3 第二级安全要求-安全审计

本项要求包括：

a) 应在网络边界、重要网络节点进行安全审计，审计覆盖到每个用户，对重要的用户行为和重要的安全事件进行审计；
b) 审计记录应包括事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；
c) 应对审计记录进行保护，定期备份，避免受到未预期的删除、修改或覆盖等。

[来源：GB/T 22239，7.1.3.5]

## C.4 第二级安全要求-可信验证

可基于可信根对计算设备的系统引导程序、系统程序、重要配置参数和应用程序等进行可信验证，并在检测到其可信性受到破坏后进行报警，并将验证结果形成审计记录送至安全管理中心。

[来源：GB/T 22239，7.1.4.6]

# 输变电设备物联网通信安全规范

## 编　制　说　明

# 目　　次

## 1 编制背景

本标准依据《国家电网有限公司关于下达2019年第二批技术标准制修订计划的通知》（国家电网科〔2019〕807号）的要求编制。

为支撑输变电设备物联网业务应用，明确输变电物联终端接入管理信息大区和互联网大区的安全防护要求，保障网络分区和业务应用安全，制定本标准。

本标准编制的主要目的是规范输变电场景下感知层设备接入管理信息大区与互联网大区时的通信安全防护要求。

## 2 编制主要原则

本标准编制的主要原则如下：

a) 贯彻国家现行的法律、法规和文件要求；

b) 参考信息通信安全和输变电设备物联网领域现行相关的国家标准、行业标准和企业标准。

本标准项目计划名称为“输变电设备物联网技术规范 第3部分：安全通信”，因与计划内容不相符，经编写组与专家商定，更名为“输变电设备物联网通信安全规范”。

## 3 与其他标准文件的关系

本标准与相关技术领域的国家现行法律、法规和政策保持一致。

本标准不涉及专利、软件著作权等知识产权使用问题。

## 4 主要工作过程

2019年7月，项目启动，召开标准编制启动会。

2019年8月，成立编写组，制定工作计划。本标准项目计划名称为“输变电设备物联网技术规范 第3部分：安全通信”，因与计划内容不相符，经编写组与专家商定，本标准更名为“输变电设备物联网通信安全规范”。

2019年9月，完成标准大纲编写，组织召开大纲研讨会，确定标准主要内容。

2019年10月，完成标准初稿编写，组织召开标准讨论会。

2020年10月，完成标准征求意见稿编写，采用研讨会、邮件等方式广泛、多次在全国范围内征求意见。

2020年11月，修改形成标准送审稿。

2020年11月，公司设备管理技术标准专业工作组（TC04）组织召开了标准审查会，审查组的审查结论为：修改后以技术标准形式报批。

2020年11月，修改形成标准报批稿。

## 5 标准结构和内容

本标准按照《国家电网公司技术标准管理办法》（国家电网企管〔2018〕222号文）的要求编写。

本标准的主要结构和内容如下：

本标准主题章分为5章，由总体防护、传感终端与涉控终端光纤专网接入场景安全要求、传感终端无线接入场景安全要求、移动作业终端接入场景安全要求和视频装置接入场景安全要求五部分组成。本标准根据输变电环境的特殊性与复杂性，输变电场景下感知层设备接入管理信息大区与互联网大区时的通信安全防护作出规范性要求。第5章介绍了输变电设备物联网通信安全总体防护架构，第6章规范了传感终端与涉控终端光纤专网接入场景安全要求，第7章规范了传感终端无线接入场景安全要求，第8章规范了移动作业终端接入场景的安全要求，第9章规范了视频装置接入场景的安全要求。第5章为总体描述，第6章、第7章、第8章、第9章这4章是并列结构，能够为第5章提供详细描述。

## 6 条文说明

本标准第2章中，引用的GB/T 22239信息安全技术网络安全等级保护基本要求为本标准最低要求，根据业务系统自身的安全防护等级，可参照此引用标准的更高等级要求。

本标准第5章中，总体防护为输变电物联网通信安全的通用标准，未全面覆盖特殊的业务场景，特殊业务场景应遵循专用规范。

本标准第9章中，站内巡检机器人存在多种接入方法。本标准的接入架构为典型架构，其他接入方式的设备也应满足本标准相关要求。