ICS 29.020

Q/GDW

国家电网公司企业标准

Q/GDW 377—2009

电力用户用电信息采集系统安全防护技术规范

power user electric energy data acquire system safety protection specification

2009-12-07发布　　2009-12-07实施

国家电网公司　发布

目　　次

前　言

按照坚强智能电网建设的总体要求，保证智能电网建设规范有序推进，实现电力用户用电信息采集系统建设“全覆盖、全采集、全预付费”的总体目标，规范统一用电信息采集系统及主站、采集终端、通信单元的功能配置、型式结构、性能指标、通信协议、安全认证、检验方法、建设及运行管理等。在国家电网公司“电力用户用电信息采集系统建设研究”项目研究成果基础上，国家电网公司营销部组织对国内外采集系统建设应用现状进行调研和分析，并充分结合通信技术、微处理器技术、制造工艺等技术的发展，全面梳理国内外用电信息采集系统相关技术标准，制定了《电力用户用电信息采集系统》系列标准。

本部分是《电力用户用电信息采集系统》系列标准之一，本部分规定了系统的安全防护技术规范。

本部分由国家电网公司营销部提出；

本部分由国家电网公司科技部归口。

本部分起草单位：中国电力科学研究院、国网电力科学研究院、国网信通公司、江西省电力公司、福建电力有限公司、北京市电力公司

本部分主要起草人：章欣、周宗发、赵兵、杜新纲、葛得辉、郑安刚、吕英杰、陈刚、王一蓉、李建新、李连兴、张松

电力用户用电信息采集系统安全防护技术规范

1 适用范围

本部分规定了电力用户用电信息采集系统的信息安全防护技术要求，主要从边界、主站、采集信道、采集设备、应用和密钥管理方面全面分析并规范了电力用户用电信息采集系统安全防护技术和设备功能性能要求。

本部分适用于电力用户用电信息采集系统建设中各环节的安全防护、信息传输和身份认证。

2 规范性引用文件

下列文件中的条款通过本部分的引用而成为本部分的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本部分，然而，鼓励根据本部分达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本部分。

GB 15853.3—1999 信息技术-安全技术-实体鉴别第 3 部分：使用非对称签名的机制（ISO/IEC 9798-3：1997）

GB/T 17903.2—1999 信息技术-安全技术-抗抵赖第 2 部分：使用对称技术的机制（ISO/IEC 13888-2：1997）

GB/T 17903.3—1999 信息技术-安全技术-抗抵赖第 3 部分：使用非对称技术的机制（ISO/IEC 13888-3：1997）

GB/T 22239—2008 信息安全技术 信息系统安全等级保护基本要求

Q/GDW 365—2009 智能电能表信息交换安全认证技术规范

Q/GDW376.1-2009 电力用户用电信息采集系统通信协议：主站与采集终端通信协议

《电力二次系统安全防护总体方案》

《信息安全等级保护管理办法》（公通字［2007］43 号）

《国家电网公司信息化“SG186”工程安全防护总体方案（试行）》

《网络与信息系统安全隔离实施指导意见》

《国家电网公司信息机房设计及建设规范》

《国家电网公司信息机房管理规范》

《密码术语》

3 术语和定义

3.1

安全模块 Security Module

安全模块是含有操作系统和加解密逻辑单元的集成电路，可以实现安全存储、数据加/解密、双向身份认证、存取权限控制、线路加密传输等安全控制功能。

3.2

密码机 Cryptography Machine

能够独立完成加/解密和密钥管理功能的设备。

3.3

密码算法　Cryptographic Algorithm

描述密码处理过程的一组运算规则或规程。

3.4

SM1 算法　SM1 Cryptographic Algorithm

SM1 算法是由国家密码管理局批准的一种商用密码分组标准对称算法。

3.5

认证　Certification

验证一个称谓的系统实体身份的过程。

3.6

明文　PlainText

待加密的数据。

3.7

密文　Ciphertest

加密后的数据。

3.8

加密　Encryption

对数据进行密码变换以产生密文的过程。

3.9

解密　Decryption

加密过程对应的逆过程。

3.10

密钥　Key

控制密码变换操作的关键信息或参数。

3.11

消息鉴别码算法　Message Authentication Code Algorithm

带密钥的密码杂凑算法，可用于数据源鉴别。

3.12

消息鉴别码　Message Authentication Code（MAC）

消息鉴别码算法的输出。

3.13

分散因子　Diffusion Factor

密钥分散是上级的密钥与本级特征相结合形成本级密钥，与本级特征有关的业务代码，密钥学称之为分散因子。

3.14

密钥信息　Key Information

密钥信息是与密钥相关的一些信息标识。

3.15

公钥基础设施　Public Key Infrastructure（PKI）

用公钥密码技术建立的普遍适用额基础设施，为用户提供证书管理和密钥管理等安全服务。

3.16

认证机构　Certification Authority（CA）

产生、签发和注销数字证书的第三方机构，也可以为用户生成密钥。

3.17

证书注册中心　Registration Authority（RA）

接收公钥证书的申请、注销和查验申请材料的机构。

3.18

数字证书（或证书）　Digtal Certificate

数字证书是经一个权威的、可信赖的、公正的第三方机构证书认证中心（CA）数字签名的包含公开密钥拥有者信息以及公开密钥的文件。

3.19

目录服务器　Directory Service

分布在网络中的各种节点或服务器提供的分布式数据库服务，它们可以存储像证书和 CRL 这样的信息。

3.20

RSA　Rivest-Shamir-Adleman algorithm

一种基于大整数因子分解问题的公钥密码算法，在本技术规范中用于数字签名和数据加密。

3.21

公钥　Public Key

非对称密码算法中可以公开的密钥。

3.22

私钥　Private Key

非对称密码算法中只能由拥有者使用的密钥。

3.23

随机数　Random Number

不可预测的时变参数。

3.24

椭圆曲线密码算法　Elliptic Curve Cryptography（ECC）Alogrithm

基于有限域上的椭圆曲线离散对数问题密码算法。

3.25

对称密钥算法　Symmetric Cryptographic

加/接密使用相同密钥的密码算法。

3.26

非对称密码算法　asymmetric cryptographic algorithm

加解密使用不同密钥的算法。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。

3.27

虚拟专用网络　Virtual Private Network（VPN）

通过一个公用网络（可以是服务提供者 IP、帧中继、ATM 主干网、Internet 等广域网）建立一个临时的安全的连接，是一条穿过混乱的公用网络的安全、稳定的隧道。

4　安全技术要求

4.1　总体要求

4.1.1　安全防护总体要求

用电信息采集系统是营销管理业务应用系统的基础数据源的提供者，为确保系统的安全性和保密

性，安全防护工作首先应做到统一规划，全面考虑。

根据《电力二次系统安全防护总体方案》、《电力行业信息系统安全等级保护定级工作指导意见》和《国家电网公司信息化“SG186”工程安全防护总体方案》等相关规定，结合用电信息采集系统的实际应用情况，依据“分区、分级、分域”防护方针，将电力用户用电信息采集系统部署在国家电网公司管理信息大区，具体如图 4-1 所示。

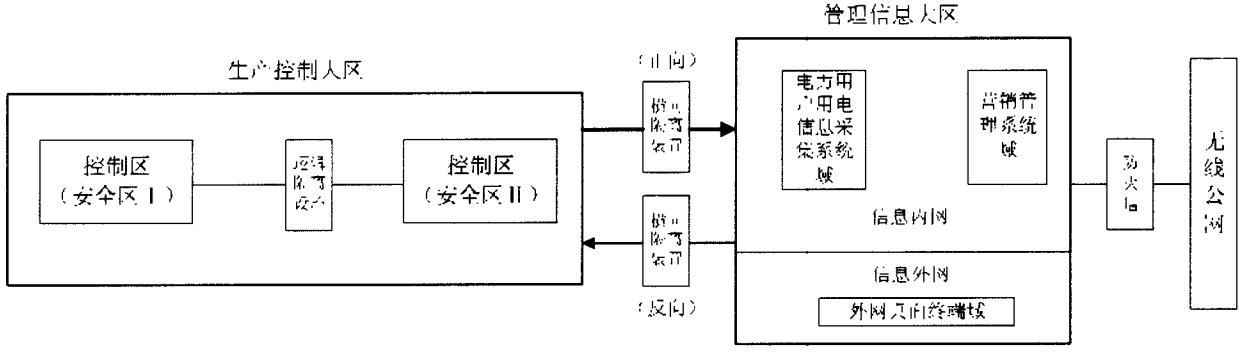

图 4-1　电力用户用电信息采集系统所属分区

将电力用户用电信息采集系统部署在国家电网公司管理信息大区的信息内网，在信息内网中独立成域（如图 4-2 所示），按照三级防护原则进行安全防护设计。

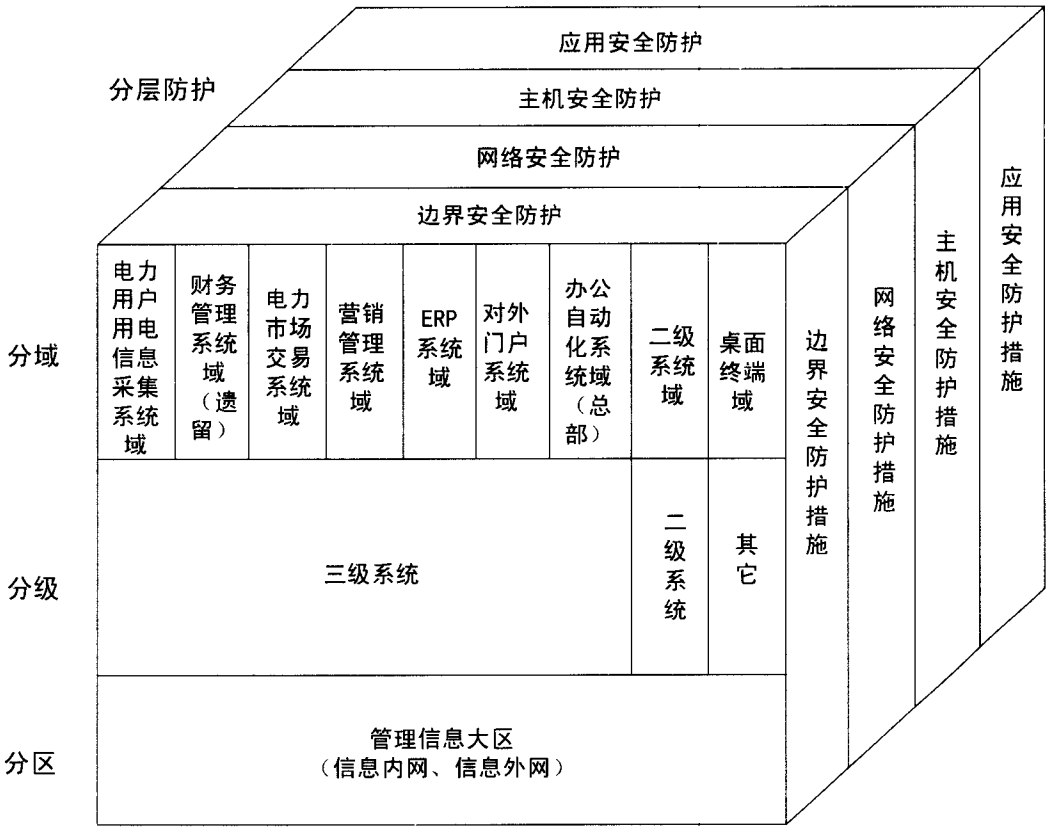

图 4-2　用电信息采集系统安全防护架构示意图

系统的安全防护应积极采用各种先进技术，如虚拟交换网络、防火墙技术、加密技术、网络管理技术等，在系统的各个层面（操作系统、数据库系统、应用系统、网络系统等）加以防范；另外，在系统日常运行管理中，要加强规范管理、严格执行安全管理制度。

在不同主站系统之间建立远程安全加密信道及身份认证、网络边界防护、隔离装置等安全措施，为应用系统提供数据源认证、抗回放、数据加密、数据完整性验证等多种安全功能，有效抵抗窃取网络信息、篡改网络数据、网络重放攻击，确保发送电力数据的加密性，保证充值数据的安全性或通过网络诱骗防止内部网络信息等攻击。

4.1.2 安全防护体系建设的总体目标

防止信息网络瘫痪、防止应用系统破坏、防止业务数据丢失、防止篡改网络数据、保证数据传输的机密性、保证数据存储的安全性、防止企业信息泄密、防止终端病毒感染、防止有害信息传播、防止恶意渗透攻击，以确保信息系统安全稳定运行，确保业务数据安全。

4.1.3 安全防护体系建设遵循的策略

信息内外网间采用逻辑强隔离设备进行隔离；信息系统间的远程传输采用网络加密系统保证远程数据传输的安全性和完整性、对终端和用户身份进行严格认证，保证用户身份的唯一性和真实性。信息系统划分为边界、网络环境、主机系统、应用系统四个层次进行安全防护设计，以实现层层递进，纵深防御，系统的物理安全和数据安全依照 GB/T 22239-2008《信息安全技术 信息系统安全等级保护基本要求》中第三级基本要求实施。

4.2 安全防护框架

4.2.1 集中式主站部署方式

集中式主站部署是指每省（自治区、直辖市）仅部署一套主站系统，一个统一的通信接入平台，直接采集全省（直辖市）范围内的所有现场终端和表计，集中处理信息采集、数据存储和业务应用。下属的各地市公司不设立单独的主站，用户统一登录到省公司主站，授权使用数据和执行本地区范围内的运行管理职能。

4.2.2 分布式主站部署方式

分布式主站部署是指在全省（自治区、直辖市）各地市公司分别部署一套主站系统，独立采集本地区范围内的现场终端和表计，实现本地区信息采集、数据存储和业务应用。省公司从各地市抽取相关的数据，完成省公司的汇总统计和全省应用。

4.2.3 防护框架

无论是分布式主站部署方式还是集中式主站部署方式，对安全防护的整体框架是相同的，都需要分别对边界、主站、信道、采集设备、应用系统进行防护，以满足整个系统的安全防护需求。

4.2.4 部署策略

在各主站系统内部署病毒防护中心，在所有的计算机终端、服务器上部署防病毒客户端，以防止恶意代码、病毒威胁及黑客攻击。

在各主站系统边界处部署两套防火墙系统，以实现边界隔离和边界策略保护。

在服务器上部署服务器安全增强系统以增强服务器的安全性，保证服务器数据的安全。

在系统内部署一套安全审计系统，对各服务器和终端的操作行为进行监控。

网络入侵检测系统部署在主站系统的核心交换机上。

采用漏洞扫描系统提供定期对终端、服务器漏洞的扫描，并及时打补丁，漏洞扫描系统部署在各网省公司主站系统内。

在各主站系统处部署两台高速主机密码机，在专变终端、集中器和用户电能表处部署安全模块，实现应用层数据完整性、机密性、可用性和可靠性保护。

4.3 边界防护

4.3.1 边界描述

边界安全防护关注如何对进出该边界的数据流进行有效的检测和控制。国家电网公司网络边界归为信息外网第三方边界、信息内网第三方边界、信息内外网边界、信息内网纵向上下级单位边界及横向域

间边界五类。电力用户用电信息采集系统部署在信息内网，其边界可划分成信息内网第三方边界、信息内外网边界、信息内网纵向上下级单位边界及横向域间边界四类。如图 4-3 所示。

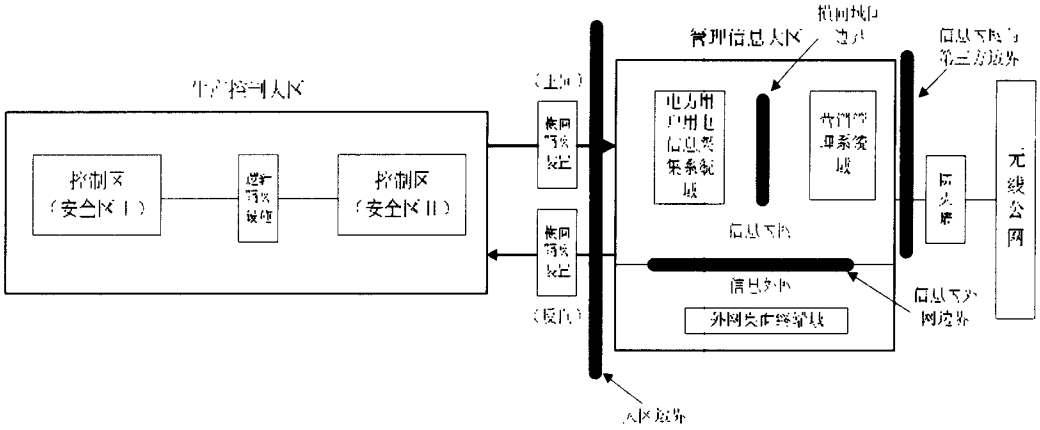

图 4-3　电力用户用电信息采集系统边界示意图

电力用户用电信息采集系统边界描述如表 4-1：

表 4-1　电力用户用电信息采集系统边界

边界类型	边　界　描　述
信息内网与第三方边界	电力用户用电信息采集系统与无线公网之间的边界
信息内外网边界	电力用户用电信息采集系统与信息外网之间的边界
信息内网纵向上下级单位边界	公司总部、网省公司、地市公司之间的边界
信息内网横向域间边界	电力用户用电信息采集系统域与信息内网其他安全域间（如营销管理系统等）的边界

4.3.2　信息内网第三方边界安全防护

信息内网第三方边界指信息内网与其他第三方网络连接所形成的网络边界，相关安全防护措施根据《国家电网公司信息化“SG186”工程安全防护总体方案》内容主要包括：边界网络访问控制、信息入侵检测、防御隐性边界。具体安全防护措施和实现的功能如表 4-2 所示。

表 4-2　系统信息内网第三方边界安全防护

信息内网第三方边界安全防护内容	安全防护措施实现形式	配　置　方　式	实　现　效　果
边界网络访问控制	防火墙	仅允许开放与其他第三方网络之间确定的地址间通讯，在防火墙上限制并发连接及各主要服务类型的传输优先级；	保护信息内网的应用不被来自第三方网络的病毒或恶意人员攻击；
信息入侵检测	入侵检测系统	将信息内网第三方边界的流量映射至入侵检测探头所在的交换机端口进行入侵监测；	检测发现隐藏于流经边界正常信息流中的入侵行为；
防御隐性边界	专用的防非法外联系统桌面终端安全管理系统	信息内网采用管理手段结合专用技术措施	防止信息内网主机非法外联互联网，并对其行为进行定位、阻断
远程接入控制	VPN 设备	以 IPSec 协议为基础，在网络上构建加密隧道；基于 IP 地址或数字证书，统一管理和设置安全策略	实现 IP 包加密、信息完整性认证、信源和信宿鉴别

根据电力用户用电信息采集系统实际应用情况，电力用户用电信息采集系统与无线公网之间的边界应划归为信息内网第三方边界，应采用 VPN 技术来保证远程数据接入的安全防护。终端通过本地号码或免费号码拨入服务提供商（ISP），然后 ISP 的接入服务器 （Net Access Server，NAS）发起一条隧道连接到电力网。对于专用的 APN，电力公司内部应建立一台 Radius 认证服务器，由电力公司为终端分配帐号和密码。当终端接入企业内部网时，需要通过 Radius 认证，确认用户身份后，才分配 IP 地址。

4.3.3 信息内外网边界安全防护

信息内外网边界应当采用国家电网公司专用逻辑强隔离设备进行安全防护，逻辑强隔离设备能够从通讯协议底层对内外网间的信息流进行隔离控制。具体安全防护措施和实现的功能如表 4-3 所示。

表 4-3 系统信息内外网边界安全防护

信息内网第三方边界安全防护内容	安全防护措施实现形式	配 置 方 式	实 现 效 果
内外网间的信息流隔离控制	逻辑强隔离设备	仅允许确定的业务数据流通过；	防止安全事件由外网至内网扩散，或阻断来自信息外网或互联网对信息内网服务器的攻击；

4.3.4 信息内网纵向上下级边界安全防护

信息内网纵向上下级单位边界包括国家电网公司总部与各网省公司、各网省公司与地市公司或直属单位、地市公司与县级单位间的网络边界，此外，如果平级单位间有信息传输，也按照此类边界进行安全防护。

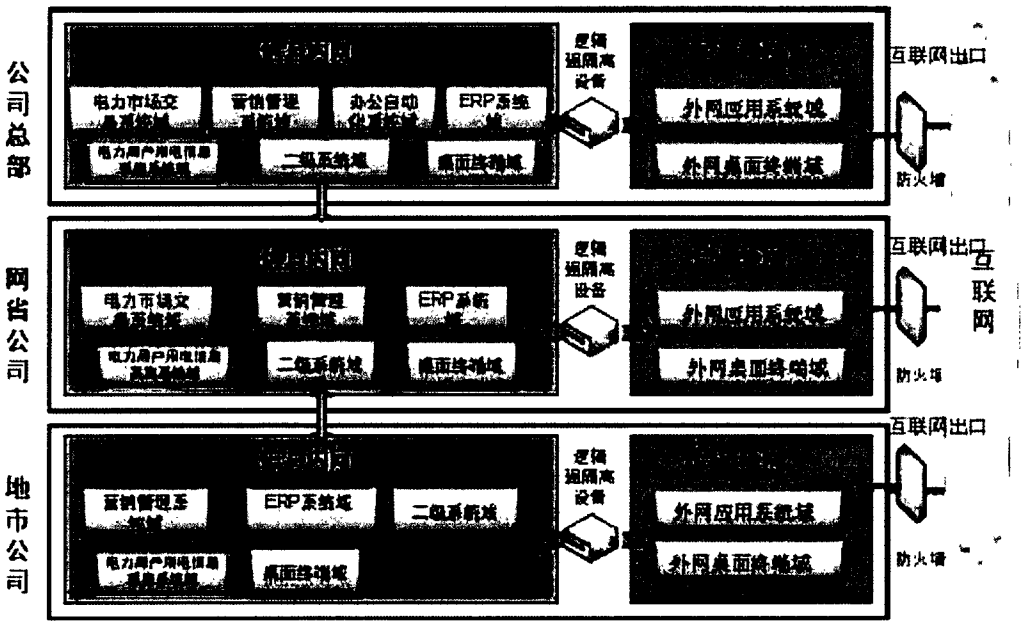

图 4-4 国家电网公司各级单位安全域分布示意图

具体安全防护措施和实现的功能如表 4-4 所示。

表 4-4 系统信息内网第三方边界安全防护

信息内网纵向上下级边界安全防护内容	安全防护措施实现形式	配 置 方 式	实 现 效 果
边界网络访问控制	防火墙	仅允许在防火墙上开放与确定的上下级单位主机间的、确定的网络通信	保护信息内网区的应用不被来自上下级单位的非法访问或病毒攻击；
信息入侵检测	入侵检测	将信息内网上下级单位边界的流量映	检测发现隐藏于流经边界正常信

	系统	射至入侵检测探头所在的交换机端口进行入侵监测；	息流中的入侵行为；

4.3.5 横向域间边界安全防护

横向域间边界安全防护是针对各安全域间的通信数据流传输所制定的安全防护措施，各系统跨安全域进行数据交换时应当采取适当的安全防护措施以保证所交换数据的安全。

横向域间边界的具体安全防护措施和实现的功能如表 4-5 所示。

表 4-5 系统横向域间边界安全防护

横向域间边界安全防护内容	安全防护措施实现形式	配 置 方 式	实 现 效 果
网络访问控制	防火墙 虚拟防火墙 VLAN 间访问控制	仅允许在网络访问控制设备上开放与确定其他安全域主机间的、确定的网络通信	保护信息内网本安全域的应用不被来自其他安全域的非法访问或病毒攻击；
信息入侵检测	入侵检测系统	将信息内网本安全域与其他安全域间的流量映射至入侵检测探头所在的交换机端口进行入侵监测；	检测发现隐藏于流经边界正常信息流中的入侵行为；

4.4 网络环境安全防护

网络环境安全防护面向国家电网公司整体支撑性网络，以及为各安全域提供网络支撑平台的网络环境设施，网络环境具体包括网络中提供连接的路由、交换设备及安全防护体系建设所引入的安全设备、网络基础服务设施。

网络环境安全防护具体防护措施和实现的功能如表 4-6 所示。

表 4-6 系统网络环境安全防护

网络环境安全防护内容	安全防护措施实现形式	配 置 方 式	实 现 效 果
安全接入控制	网络准入控制客户端	在各安全域网络交换设备上启用 802.1X 接入控制，在网络准入控制管理端制定统一的安全准入策略；在各安全域网络交换设备上启用 802.1X 接入控制，在网络准入控制管理端制定统一的安全准入策略；	保证安全区域不被未授权接入，保证不符合准入安全措施要求的桌面主机不能接入网络；
设备安全管理	用户名/口令身份认证 采用安全协议进行远程管理	只有用户名/口令通过认证的用户进行设备的配置管理	保证不具备权限的人员无法操作设备
设备安全加固	软件实现	对所有的网络设备和路由器进行加固；	保证网络设备配置和其传输数据的安全；
安全弱点扫描	弱点扫描系统	为所有的网络设备配置扫描策略；	有效实现对网络设备及操作系统、数据库、应用软件的漏洞扫描发现功能；
安全事件审计	日志管理分析系统	配置为以 Syslog 或 Snmp 方式收集核心网络、安全设备事件日志并进行事件分析	集中收集、存档核心网络、安全设备事件日志，并生成报表进行事件统计分析
网络入侵检测	网络入侵检测系统	由入侵检测控制台对 IDS Sensor 进行集中管理；	能有效发现病毒、蠕虫、黑客攻击、恶意代码攻击、拒绝服务攻击等威胁，并在事件发生后进行报警；

4.5 主机系统安全防护

主机系统安全防护包括对服务器及桌面终端的安全防护。服务器包括业务应用服务器、网络服务器、WEB 服务器、文件与通信等；桌面终端包括作为终端用户工作站的台式机与笔记本计算机。

主机系统安全防护具体防护措施和实现的功能如表 4-7 所示。

表 4-7 系统主机系统安全防护

主机系统安全防护内容	安全防护措施实现形式	配 置 方 式	实 现 效 果
安全加固	操作系统和基础服务安全加固	依据自动扫描或人工评估出的配置弱点进行加固； 依据操作系统厂商或专业安全组织提供的加固列表对操作系统进行安全加固；	加强主机的操作系统层面安全防护；
防病毒管理	防病毒系统客户端	配置为每天分发特征代码，开启病毒实时监控功能，病毒事件上报服务器；	提供对服务器或桌面终端的病毒防护；
访问控制	主机防火墙	依据业务访问需求配置访问控制策略；	保护主机不被未授权访问和攻击；
入侵检测	主机入侵检测系统	配置为对入侵行为进行检测和报警	保护主机不被入侵和攻击
主机资源监控	资源监控客户端	在网管系统控制台配置资源监控策略；	可以提供对主机资源使用状况的监控；
安全弱点扫描	弱点扫描系统	对主机操作系统及数据库的弱点进行扫描；	先于攻击者发现系统弱点并给出处理建议；
安全审计	日志管理分析系统	将应用主机上的日志收集客户端配置为将日志统一收集至日志服务器。	可以实现对于主机安全日志的集中管理、集中存档及统一分析。

4.6 应用安全防护

应用安全防护包括对于主站应用系统本身的防护，用户接口安全防护、系统间数据接口的安全防护、系统内数据接口的安全防护。

应用安全防护的目标是通过采取身份认证、访问控制等安全措施，保证应用系统自身的安全性，以及与其他系统进行数据交互时所传输数据的安全性；采取审计措施在安全事件发生前发现入侵企图或在安全事件发生后进行审计追踪。

应用安全防护具体防护措施和实现的功能如表 4-8 所示。

表 4-8 系 统 应 用 安 全 防 护

应用安全防护内容	安全防护措施实现形式	配 置 方 式	实 现 效 果
应用加固	实施在采集系统域的服务器上	依照各厂商发布的 checklist 安全列表剪裁后实现；	增强应用软件的安全性；
弱点扫描系统	安装于移动笔记本终端上	对应用系统进行弱点扫描；	发现应用系统中所采用的公用模块的纺点并给出处理建议；
总体方案对于应用系统的要求	在应用系统中实现	依照总体方案对于软件产品的要求进行系统开发或改造。	保证应用系统自身及其所处理业务的安全。

4.6.1 应用系统安全防护

应用系统安全防护应从应用系统安全、身份认证机制、用户权限及访问控制、应用安全审计、剩余信息保护、数据存储保密、数据存储完整、抗抵赖、软件容错、资源控制、应用数据的备份与恢复等方

面进行安全防护，具体防护措施及内容详见《国家电网公司信息化“SG186”工程安全防护总体方案》2.3.4.1。

4.6.2 用户接口安全防护

用户远程连接应用系统需进行身份认证，制定数据加密、访问控制等安全措施，并采用密码技术保证通信过程中数据的完整性。用户接口安全防护具体防护措施及内容详见《国家电网公司信息化“SG186”工程安全防护总体方案》2.3.4.2。

4.6.3 系统间数据接口安全防护

国家电网公司各应用系统间的数据交换采用两种模式：系统间直接数据接口交换或通过应用集成平台进行数据交换，处于这两种数据交换模式的系统均应制定系统间数据接口相关安全防护措施。

在《国家电网公司信息化“SG186”工程安全防护总体方案》中分别对系统间直接数据接口交换和通过数据集成平台进行系统间数据交换应采用的安全防护措施及具体内容进行了详细描述，具体内容及措施详见《国家电网公司信息化“SG186”工程安全防护总体方案》2.3.4.3。

4.6.4 系统内数据接口安全防护

系统内数据接口主要是针对电力用户用电信息采集系统中的主站与采集设备、计量设备之间的数据交互的接口。系统内数据接口主要采用信息加密技术实现安全防护。采用的信息加密技术包括对称密钥密码技术和公开密钥密码技术。对称密钥密码技术采用的对称密钥加密算法推荐选用国密 SM1 算法，公开密钥密码技术采用的非对称密钥加密算法推荐选用 RSA（1024bit 以上）。

在主站、采集设备、计量设备加装应用安全设备（密码机和安全模块）来实现信息加密，以确保数据传输中关键信息的完整性及敏感信息的安全性。

应用安全设备（密码机和安全模块）完全受控，由专门机构管理、制作和发放，并采用经过国家密码管理局批准的加密方式、密码算法和密钥管理技术来增强安全保障。

4.6.4.1 应用安全设备的部署位置

本系统内应用的安全设备主要是密码机和安全模块，其中密码机和加密模块均采用硬件加密算法。在电力用户用电信息采集系统的主站侧部署密码机，用于主站侧数据的加解密；在采集设备和计量设备中嵌入安全模块实现设备内部数据的加解密。

密码机和安全模块在系统中的部署位置如图 4-5 所示：

在图 4-5 中，要求前置通信服务器要配备双网卡，通过其中的一个网卡将前置通信服务器与密码机部署在同一个局域网内。密码机与前置通信服务器以 TCP/IP 的方式进行通信，其中密码机为服务器，前置通信服务器为客户端。在专变终端、集中器、远程多功能表、智能电能表等设备中加装安全模块，其中采集器只为数据传输通道，不需要加装安全模块。

4.6.4.2 系统内数据接口采用的安全防护措施

系统内数据接口主要采用信息加密技术实现安全防护，要求新建系统所有数据加解密都应采用硬件加密的方式实现，不允许使用软件加解密方式；已经建成的系统可以结合软件加密方式进行升级改造。

主站侧应采用国家密码管理局认可的密码机实现数据的加解密，密码机必须集成对称密钥加密算法和非对称密钥加密算法。

专变采集终端和集中器中应采用国家密码管理局认可的硬件安全模块实现数据的加解密。专变终端和集中器采用的硬件安全模块应采用同时集成有国家密码管理局认可的对称密钥加密算法和非对称密钥加密算法的安全模块。

智能电能表中应采用国家密码管理局认可的硬件安全模块以实现数据的加解密。智能电能表采用的硬件安全模块内部应至少集成有国家密码管理局认可的对称密钥加密算法。

对称密钥密码技术采用的对称密钥加密算法推荐选用国密 SM1 算法，公开密钥密码技术采用的非对称密钥加密算法推荐选用 RSA（1024bit 以上）。

对称密钥加密算法实现方式参见 GB/T 17903.2—1999：信息技术-安全技术-抗抵赖第 2 部分：使用

对称技术的机制（ISO/IEC 13888-2：1997）；

非对称密钥加密算法实现方式参见 GB/T 17903.3—1999：信息技术-安全技术-抗抵赖第 3 部分：使用非对称技术的机制（ISO/IEC 13888-3：1997）。

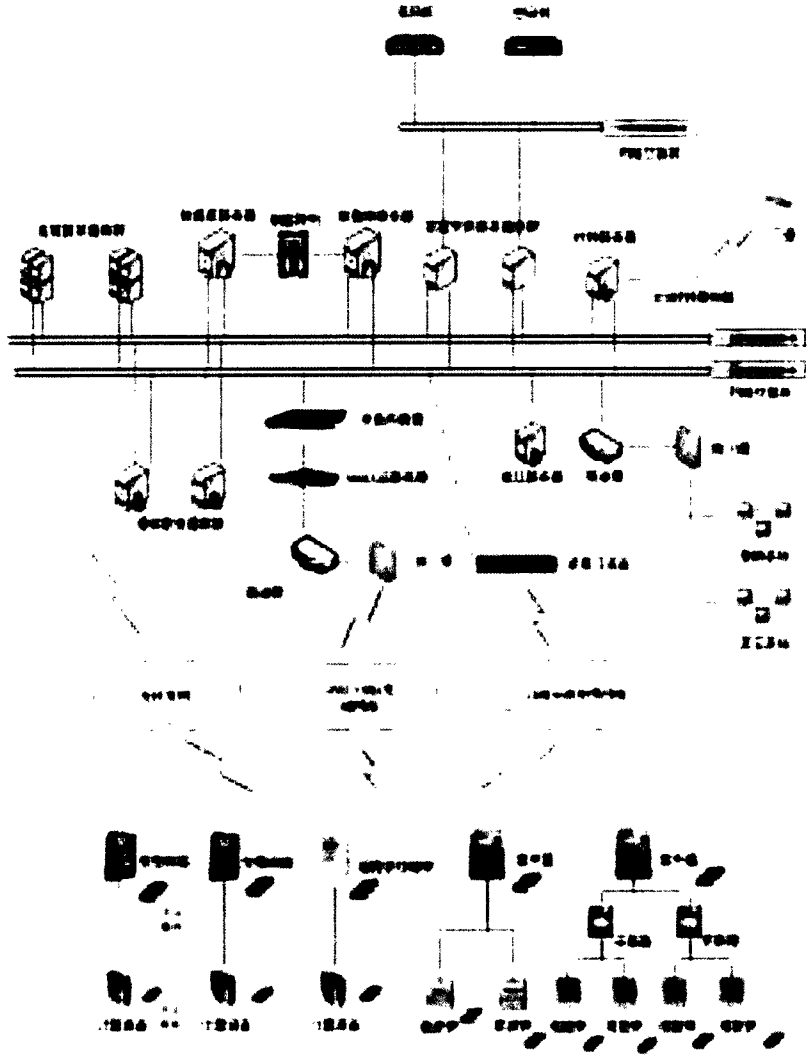

图 4-5　应用安全设备在系统中的部署图

4.6.4.2.1　**主站侧的防护措施**

主站侧采用国家密码管理局认可的密码机实现数据的加解密。密码机与前置通信服务器部署在同一个局域网内。

密码机与前置机之间采用服务器 / 客户端工作模式，其中密码机为服务器，前置机为客户端，其连接方式如图 4-6 所示。由前置机向密码机发起请求，密码机处理完后将结果发送给前置机，以完成数据的加解密处理等功能。

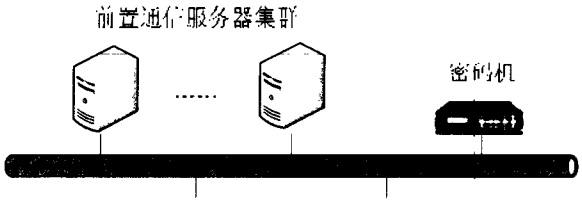

图 4-6　前置机与密码机的连接示意图

密码机在主站侧主要实现身份认证、密钥协商、密钥更新、关键数据的加解密、MAC（消息鉴别码 Message Authentication Code）计算和数据校验等功能。

在电力用户用电信息采集系统中，系统内数据接口所采用的非对称密钥加密算法主要用于终端的身份认证、密钥协商、对称密钥加密算法的密钥分发与更新。对称密钥加密算法主要用于设置参数、控制命令、数据转发等通信协议中规定的附加信息域（AUX）中需要携带消息认证码字段 PW（下行）报文的加解密数据处理，具体要求参见 Q/GDW 376.1-2009 的相关部分。

在系统运行过程中，前置通信服务器按照 Q/GDW 376.1-2009 的要求，根据应用层功能码（AFN）来判断哪些数据需要进行加密，把需要加密的明文数据送密码机，密码机对明文数据进行加密，并将加密后的密文数据及 MAC 送前置通信服务器，前置通信服务器将加密后的密文进行数据打包，再将打包的数据下发；不需要加密的数据不经过前置通信服务器处理，直接将数据打包、下发。

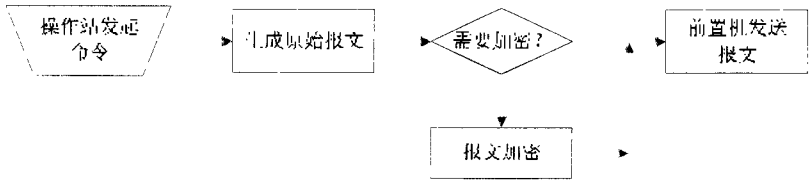

图 4-7　前置通信服务器报文加密处理过程

4.6.4.2.2　**采集设备的防护措施**

采集设备除了要具有防窃、防破坏、用电安全等防护措施外，还应采用安全模块确保系统内通信数据接口的安全。采集设备包括专变终端、集中器、采集器等设备，其中采集器不需要加装安全模块，其它采集设备均需加装安全模块。

在专变采集终端和集中器加装安模块，用于采集设备与主站之间、以及采集设备与智能电能表之间进行的身份识别、安全认证、关键信息和敏感信息安全传输。

采集设备与主站之间信道传输的加密数据根据功能可以划分为管理数据和传输数据这两类。

其中管理数据主要是与采集设备有关的一些关键数据，这些关键数据主要是用于采集设备的终端管理。管理数据的传输应按照 Q/GDW 376.1-2009 的要求，进行身份认证、密钥协商、对称密钥加密算法的密钥分发与更新、以及设置参数、控制命令等通信协议中规定的加密数据下行报文的 MAC 校验及数据解密。

其中传输数据主要利用主站与采集设备之间建立的加密信道进行数据的传输，主站与智能电能表之间就可以利用此加密信道进行数据传输。加密信道的建立方式是按照《电力用户用电信息采集系统主站与采集终端通信协议》的要求，以数据转发的方式进行数据传输，转发的数据内容即为传输数据。

采集设备与智能电能表之间传输的数据应按照 Q/GDW 365—2009 的要求进行数据传输。

4.6.4.2.2　**计量设备的防护措施**

计量设备除了要具有防窃、防破坏、用电安全等防护措施外，还应采用安全模块确保系统内通信数据接口的安全。计量设备主要包括智能电能表。在智能电能表内部也需要加装安全模块，考虑到智能电能表在电力用户用电信息采集系统中所处的位置及智能电能表的成本，要求智能电能表中加装的安全模块至少要满足对称密钥加密算法。

在智能电能表等计量设备中加装安模块，主要用于智能电能表与主站之间、智能电能表与采集设备之间、智能电能表与红外手持设备之间进行的身份识别、关键信息和敏感信息安全传输。

智能电能表与主站之间进行的身份识别、关键信息和敏感信息的通信主要借助主站与采集设备之间建立的传输数据加密通道，进行的数据传输。例如售电系统发出的售电信息的密文数据通过主站与采集设备之间建立的传输数据加密通道，进行数据的传输。主站与采集设备之间建立的传输数据加密通道是主站按照 Q/GDW 376.1-2009 的要求将需要传输给智能电能表的数据以数据转发的形式发送给智能电能表。

智能电能表与采集设备之间以及智能电能表与红外手持设备之间传输的数据按照 Q/GDW 365—2009 的具体要求进行数据的交互。

电力用户用电信息采集系统
安全技术规范

编 制 说 明

目　　次

1 项目来源

为深入贯彻落实国家电网公司“集团化运作、集约化发展、精益化管理、标准化建设”的管理要求，进一步规范用电信息采集终端的功能、型式、技术性能及验收试验等相关要求，满足电力用户用电信息采集系统和智能电网建设的需要，提高用电信息采集系统规范化、标准化管理水平，促进公司系统经营管理水平和优质服务水平的不断提高，国家电网公司在取得“电力用户用电信息采集系统建设研究”项目研究成果的基础上，把《电力用户用电信息采集系统》系列化标准列入了国家电网公司 2009 年企业标准制修订计划。

2 编制目的

通过制定《电力用户用电信息采集系统》系列标准提升用电信息采集系统管理的规范化、标准化水平，实现系统和采集终端的互联、互通，满足电能信息采集需要，体现智能电网 “信息化、自动化、互动化”的建设要求，提高采集终端的可靠性和使用寿命，促进采集终端质量提升，保障用电信息采集系统的可靠运行，进一步完善计量技术管理体系，推动用电信息采集工作健康有序发展。

3 编制原则及思路

1） 坚持先进性与实用性相结合、统一性与灵活性相结合、可靠性与经济性相结合的原则，以标准化为引领，服务公司科学发展。

2） 采用分散与集中讨论的形式，分析各网省公司用电信息采集系统的技术规范，充分了解各地用电信息采集系统建设现状，明确系统及终端功能需求，建立采集系统功能模型和数据模型，研究新的需求形势下不同管理要求、预付费管理方式以及不同地域与环境对终端的使用要求，体现研究的实用性和先进性。

3） 认真研究国内外现行相关的 IEC 标准、国家标准、行业标准、企业标准，体现通信特性和功能拓展的最新发展。

4） 坚持集中公司系统人才资源优势，整合、吸收公司系统各单位先进的管理要求和发展思路，体现公司集团化运作、集约化发展、精益化管理、标准化建设的理念。

5） 规范该类终端相关的术语和定义、技术要求、功能要求、型式要求、验收试验方法等相关内容，切实指导该类终端的采购和检测工作。

4 编制依据

本部分的制定过程主要依据和参考如下文献：

Q/GDW376.1-2009：电力用户用电信息采集系统通信协议：主站与采集终端通信协议；

GB 15853.3—1999：信息技术-安全技术-实体鉴别第 3 部分：使用非对称签名的机制（ISO/IEC 9798-3：1997）；

GB/T 17903.2—1999：信息技术-安全技术-抗抵赖第 2 部分：使用对称技术的机制（ISO/IEC 13888-2：1997）；

GB/T 17903.3—1999：信息技术-安全技术-抗抵赖第 3 部分：使用非对称技术的机制（ISO/IEC 13888-3：1997）；

Q/GDW ×××—2009 《电力用户用电信息采集系统》系列标准

《电力行业信息系统安全等级保护定级工作指导意见》（电监信息［2007］44 号）

《电力二次系统安全防护总体方案》

GB/T 22239—2008：信息安全技术信息系统安全等级保护基本要求

国家电网信息 316 号文《国家电网公司信息化“SG186”工程安全防护总体方案》

5 标准编制过程

1）项目启动

2008 年 9 月 22 日，国家电网公司营销部在天津召开会议 ，部署开展《计量、抄表、收费标准化建设》项目的研究工作；明确该项目中的《电能信息采集技术及推广应用研究》子课题由中国电力科学研究院、黑龙江、华北、北京、天津、山西、上海、江苏、浙江、安徽、福建、河北、河南、湖北、湖南、重庆、吉林、甘肃、新疆以及国网电力科学研究院、国网信通公司等 21 家单位共同承担。

2）交流座谈

2008 年 9 月 24 日，国家电网公司营销部在天津召开会议，详细了解公司系统主要单位用电信息采集系统的建设现状和应用效果、以及下一步的建设需求和技术方案，研讨相关技术可行性、系统可靠性和建设管理等问题。

3）确定研究大纲

2008 年 10 月 11 日，国家电网公司营销部在北京怀柔召开会议，听取各课题组工作进展情况的汇报，课题组编制课题研究大纲。会后国家电网公司按照会议研究结果，下发了《关于开展计量、抄表、收费标准化建设研究工作的通知》，以及《电能信息采集技术及推广应用研究大纲》，明确了课题的研究目的、思路、任务、分工以及进度要求，。

4）项目调研

根据研究大纲的要求，课题组编制了《电能信息采集技术及推广应用调研提纲》和《调研表格》，并由国家电网公司营销部组织在公司系统对用电信息采集系统进行现状调研。

5）集中研究

10 月 13 日，国家电网公司党组会议明确电力用户用电信息采集系统建设的方向，“电力用户用电信息采集系统建设研究”项目涉及采集系统建设、运行、检验等环节中的关键技术、标准化业务流程和管理规范，设备产业化、金融产业化发展策略等相关内容的 16 个课题，10 月 16 日至 10 月 23 日，课题组在哈尔滨开展用电信息采集系统建设现状及需求分析、功能规范、建设模式及技术方案、投资及收益分析四个课题的集中研究工作。完成了 4 个课题的研究报告，并编写了提交党组会审议的汇报材料，为党组决策提供依据。

6）分组研究

在完成第一阶段研究的同时，其他 12 个课题同步开展了研究工作，10 月 17 日—11 月 10 日，各课题组进行课题前期准备，编制研究大纲工作，11 月 10 日在研究工作领导小组的统一组织下对 12 个课题的研究大纲进行了审议，确定了各课题的研究内容和实施方案。各课题组按照研究大纲的要求采用分组编写、集中讨论、广泛征求意见的方式于 12 月 30 日完成了 16 个课题的研究报告，并对 16 个课题的研究内容进行汇总，形成了《电力用户用电信息采集系统建设研究报告》。

7）标准编制

课题组采用研究与编制相结合的原则，采用分组研究与全体讨论的形式，召开多次会议，先后完成了《电力用户用电信息采集系统》系列标准的初稿、征求意见稿。

8）征求意见

国家电网公司营销部组织对《电力用户用电信息采集系统》征求意见稿在公司系统进行征求意见，并对电力用户用电信息采集系统功能规范、技术规范、型式规范在社会主流采集设备制造企业征求意见。课题组对反馈的 166 条意见进行了认真讨论，确定了采纳修改的内容，形成了评审稿。

9）项目评审

2009 年 4 月 9 日，国家电网公司营销部在北京召开“计量、抄表和收费标准化建设”项目研究成果评审会，会议审议并通过了“电力用户用电信息采集系统”子课题的研究成果，与会专家给予了较高的评价，并一致建议尽快完成企业标准的报批和印发，以便更好指导电力用户用电信息采集系统的建设和

采集终端的生产、采购、检验和运行管理工作。

10）标准送审

2009 年 8 月 28 日至 9 月 3 日，邀请采集终端制造企业的代表以及公司系统的专家对采集终端的型式、结构进行了优化设计，对功能进一步修改完善。9 月 25 日至 26 日，国家电网公司营销部、科技部、智能电网部、信息化工作部共同组织，审议通过了《电力用户用电信息采集系统》系列标准“送审稿”。

6 标准主要内容

本部分依据《电力企业标准编制规则》DL/T 800—2001 的编写要求进行了编制。标准主要结构和内容如下：

1. 目次；
2. 前言；
3. 标准正文共 4 章：适用范围、规范性引用文件、术语和定义和安全技术要求。