电力物联网信息安全防护技术研究*

江泽鑫
（广州邦讯信息系统有限公司，广东 广州 510000）

摘　要：介绍了电力物联网在配电网的应用场景，总结了我国电力物联网信息安全防护的发展历程，分析了当前电力物联网信息安全应用中存在的主要问题和解决电力物联网信息安全的关键技术，最后提出了电力物联网终端本体的信息安全防护的四道防线模型和实践。

关键词：电力物联网；信息安全；安全接入区；电力监控系统安全防护
中图分类号：TP915.08　　**文献标识码**：A　　DOI：10.19358/j.issn.2096-5133.2020.01.006
引用格式：江泽鑫.电力物联网信息安全防护技术研究[J].信息技术与网络安全，2020，39(1)：31-37.

Research on information security protection technology for power IoT

Jiang Zexin
(Guangzhou Bonson Information System Co.,Ltd.,Guangzhou 510000,China)

Abstract: This paper introduces the application scenarios of power IoT, summarizes the history of power IoT security in China, analyzes the main problems existing in power IoT security and proposes the key technologies to solve it. Finally, a four-line defense model for power IoT terminal security is proposed.

Key words: power IoT; information security; security access domain; power monitoring system security protection

0　引言

电力系统发、输、变、配、用电等环节都广泛使用了工业物联网技术。根据国家电网"泛在电力物联"专题资料显示，目前存储的计量终端表达5.3亿个、各类型设备监控终端达300万套、视频监控摄像头终端50万个，累计日增数量60 TB以上。这些海量的物联网终端设备主要应用于电网配用电系统中，并广泛使用无线公网方式进行数据传输。

以配电物联网终端为例，配电物联网终端主要有一遥的故障指示器、二遥馈线自动化终端FTU、三遥配电自动化终端DTU和目前的智能配变终端TTU。配电物联网终端是配网自动化的重要组成部分，与配电线路的断路器和互感器等一次设备连接，实现对配电线路"遥信、遥测、遥控"等感知与控制，从而为配电网的运维提供快速的线路故障定位、故障隔离、转供电和快速复电等重要功能，最终提高电网的供电可靠性和电网服务质量。

图1是配网自动化示意图，由配网主站、通信网络和配电物联网终端三部分组成。配网通信网络主要有三种方式：(1)采用光纤专用网络，如xPON；(2)采用公网无线通信，如GPRS/4G；(3)采用电力专用的TD-LTE无线专网。目前对于部署在配电房或开关站内的配电物联网终端普遍采用光纤专网方式与配网主站通信，而对于部署在架空线路或环网柜等未实现光纤覆盖的区域则广泛使用运营的虚拟专用网络APN与配网主站通信。

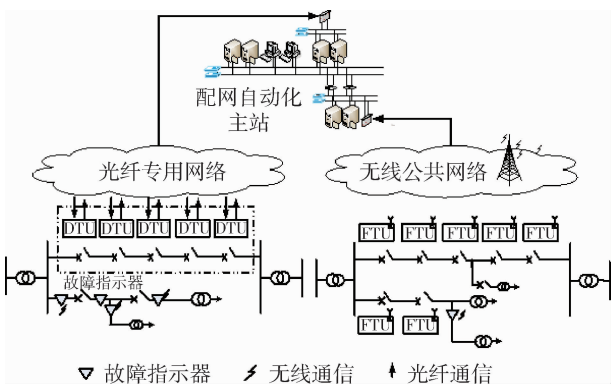

图1　配网自动化系统示意图

*基金项目：广州市"珠江科技新星"科技资助项目(201806010044)

电力物联网终端由于广泛部署在户外并且普遍使用公网无线通信,存在物理访问、物理攻击、无线通信数据泄露、报文被篡改、被重放等安全隐患。文献[1]介绍了几种针对配电网 IEC60870-5-104 规约的攻击方法及实验。为此,电力物联网的应用受到了很大的限制,譬如禁止了配网自动化最为重要的“遥控”功能,导致配网自动化被迫降至“半自动化”,电力物联网的信息安全防护极大程度制约着电力物联网的应用发展。因而,在国家和行业信息安全防护合规框架下,研究电力物联网的信息安全防护技术对于推动当前电力物联网应用和更多的功能落地具有十分重要的意义。

1 电力物联网信息安全防护发展历程

根据本文作者的研究,电力物联网终端的信息安全防护经历了以下三个阶段的发展。

1.1 应用初探阶段

早在 2014 年发改委 14 号令[2](后形成国标 GB / T36572-2018[3])发布之前,在配用电自动化系统的建设中,电力物联网终端和无线公网由于成本低和部署方便等特点在很多地区有广泛的应用。但由于原电监会 5 号令[4]未对此类应用的信息安全进行明确规范和众所周知的信息安全隐患的存在,导致电力物联网的信息安全防护普遍采取两个安全防护举措。

(1)禁止使用“遥控”功能,即“遥控”功能切换至就地模式;

(2)使用无线公网的物联网终端数据通过安全区 III 进入安全区 I 的配网自动化主站。

第一个举措导致对于使用无线公网的电力物联网终端明明具备“三遥”功能却不得不降至“二遥”使用,无法施展配网自动化的遥控威力,配网自动化的“自动化”程度受到制约。

第二个举措则存在两点不足,一是电力物联网终端的数据很大一部分是生产类数据,甚至属于控制类数据,如 IEC60870-5-101 规约报文;生产业务的数据通过无线公网和安全区 III,本身就不符合原 5 号令的“安全分区、网络专用”的设计原则和业务。二是安全区 III 与无线公网的边界普遍使用硬件防火墙进行逻辑隔离,如果电力物联要进行“遥控”也不符合 5 号令的针对控制类业务的“纵向加密”的加密认证要求,这也是不得不实施第一个举措的原因。电力监控系统安全防护整体架构示意图如图 2 所示。

1.2 合规指导阶段

2014 年发改委发布 14 号令,随后 2015 年国家能源局修订发布了 36 号文[5]。14 号令和 36 号文是针对原监会 2004 年 5 号令和 34 号文[6]的一次重大修订,其中针对电力物联网应用存在的信息安全防护策略进行了规范,主要内容包括:

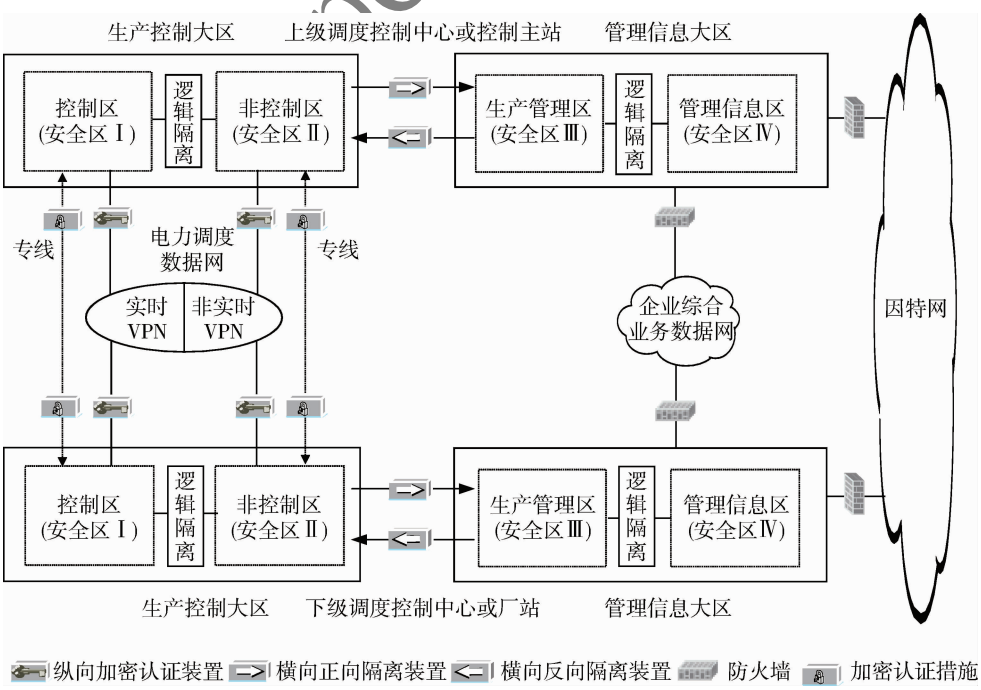

图 2 电力监控系统安全防护整体架构示意图

（1）提出“安全接入区”概念，安全接入区不属于安全区 III，更不属安全区 I，而是一个独立的安全区，其防护架构示意图如图 3 所示。在生产控制大区里的业务系统需要使用无线公网等网络时才设立安全接入区，安全接入区与生产控制大区的边界需要部署正反正隔离装置，同时与无线公网的边界需要部署加密认证措施。

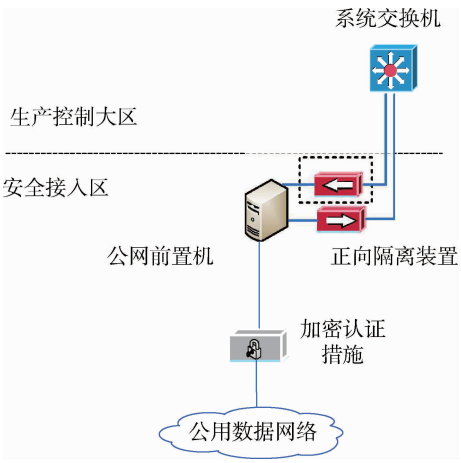

图 3　安全接入区防护架构示意图

安全接入区本质是一个安全缓冲区的概念，因为主网监控系统与配网监控系统同处安全区 I，而主网监控系统的安全防护较为成熟和完整，已经实现从物理光纤到 SDH 传输网再到基于 MPLS 的数据网全部专网专用。如果攻击面较大的配网监控系统，海量电力物联网终端通过安全防护级别相对较低的区域进入安全区 I，势必会殃及安全防护较为完整的主网监控系统。为阻隔来自类似配网等使用无线公网监控系统方向的黑客攻击，安全接入区作为安全缓冲区，与生产控制大区之间设计采用了安全强度最高的准物理隔离级别的电力专用正反向隔离装置进行防护。同时为了保证电力监控十六字方针的“纵向加密”整体防护架构，安全接入区与电力物联网终端之间设计了加密认证措施。

具体到落地层面上，如果将安全强度高的正反正隔离措施应用于安全接入区与无线公网的边界是最合适的。在实际情况中，这些采用无线公网的监控系统往往终端数量规模极为庞大，而且有实时监控的业务需求导致监控系统主站需要实时与海量的电力物联网进行通信，高实时高吞吐率的业务特点与高安全级别低性能低吞吐率的正反向隔离装置是矛盾的。为了保证业务系统的运行且能降低安全区 I 系统的安全风险，在安全接入区内，部署了针对无线公网的前置采集服务器，它通过相对容易实现高并发高吞吐率的加密认证措施与电力物联网终端连接。可见，安全接入区的设计可以看作是安全区 I 的一道来自无线公网攻击的防护缓冲屏障，将入侵电力物联网终端可能攻击整个配网和整个主网的安全风险降至只可能攻击部分配网而难攻击主网。

（2）在电力监控整体安全防护框架内明确了等级保护、商用密码、风险评估、可信计算、安全可控等规范和技术的要求。这些要求一方面为前沿的信息安全防护技术在电力行业的应用和发展提供了空间和铺垫，另一方面也意味着电力信息安全防护将逐步与国家标准相互融合，吸收先进的信息安全防护技术。

在此阶段中，电力物联网信息安全防护仍尚不完整，主要体现在安全接入区与无线公网的“加密认证措施”上。14 号令中提出了纵向的加密和认证要求，传统主网监控系统已经设计实施了电力专用的纵向加密认证装置和规范；但其造价极高，无法适用于海量电力物联网纵向的加密认证需求。同时针对不同的电力业务和不同专业意见，导致 36 号文并未形成明确统一一致的具体加密认证落地措施。也因此，在配网、计量等不同专业方向上，国家电网和南方电网采取了不同的加密认证措施。其中某公司的技术路线经历了基于数字签名的软件单向认证、到双向加密认证、到基于硬件的加密认证等实践和迭代。实践表明，只要面向市场开放海量物联网信息安全防护需求，将会有更加优质、低价、安全可控的安全产品出现。

1.3　安全防护水平提升和全面落地阶段

随着 2019 年的等级保护 2.0[7] 发布和泛在电力物联网需求提出，电力物联网的信息安全防护水平必将得到较高的水平提升。2019 年等级保护 2.0 相比于 2008 年等级保护的要求主要区别包括以下两点。

（1）对控制措施的框架描述进行修订，由原来偏技术思维的“物理、主机、网络、应用、数据、制度、组织、人员、建设、运维”十个层面调整为偏管理思维的“物理、网络及边界、计算环境、数据、策略、制度人员、建设、运维”八个层面。

（2）对象范围明确了云计算、移动互联网、物联

网、工业控制等针对性场景的等级保护扩展要求。

在等级保护 2.0 物联网扩展章节中,规范明确到了感知节点的物理防护、感知设备和网关节点的安全防护、网络入侵和接入控制、数据抗重放和数据融合处理。等级保护 2.0 的这些要求正好是 36 号文在电力物联网信息安全防护中比较缺失的部分。而目前国家电网公司提出建设泛在电力物联网的业务需求,这对于电力物联网的信息安全和建设具有非常强的推动作用。可以预见,密码芯片、商用密码技术、可信计算技术、软件定义安全技术等技术在电力物联网设备中将会有极大的落地潜力。

2 电力物联网安全防护关键技术

能源局 36 号文已经明确了电力监控系统的整体防护架构,在电力物联网安全防护落地上,需要进一步重点研究的是感知传感器/边缘计算网关与安全接入区之间纵向的信息安全防护,主要包括 VPN 技术应用、商密算法应用、密钥管理和证书系统、抗侧信道攻击技术应用、应用报文智能检测等方面。

2.1 VPN 技术应用

VPN 是一种在公共网络的基础上架设虚拟专网的技术,典型的 VPN 技术主要有:

(1)链路层 VPN 技术,包括 PPTP 或 L2TP。

(2)网络层 VPN 技术,包括 MPLS 和 IPSec。

(3)应用层 VPN 技术,包括 SSL/TLS。

VPN 并不意味着安全,PPTP、L2TP 主要通过账号密码进行安全防护级别较低的身份验证,并不带加密。MPLS 主要在网络路由协议之下,建构一个基于标签的快速高效数据交换传输技术,譬如电力调度数据网使用 MPLS 协议虚拟了两个子网,一个叫实时 VPN 用于传输安全区 I 业务数据,另一个叫非实时 VPN 用于传输安全区 II 业务数据。IPSec 和 SSL 都具有加密认证功能,但 SSL VPN 无法实现“网关-网关”(即 site to site)场景,其普遍应用于移动办公的远程接入的加密认证;IPSec 则不仅支持“网关-网关”、“终端-网关”等场景,而且支持传输模式和隧道模式,在系统安全改造方面可以实现“透明无感”的信息安全防护升级改造等特点。

依据《IPSec VPN 技术规范》[8],电力物联网终端与主站侧先基于 SM2 算法的公钥密码算法进行身份认证,然后进行通信密钥协商,最后基于协商的临时密钥进行加密通信。其临时会话密钥协商过程如图 4 所示。

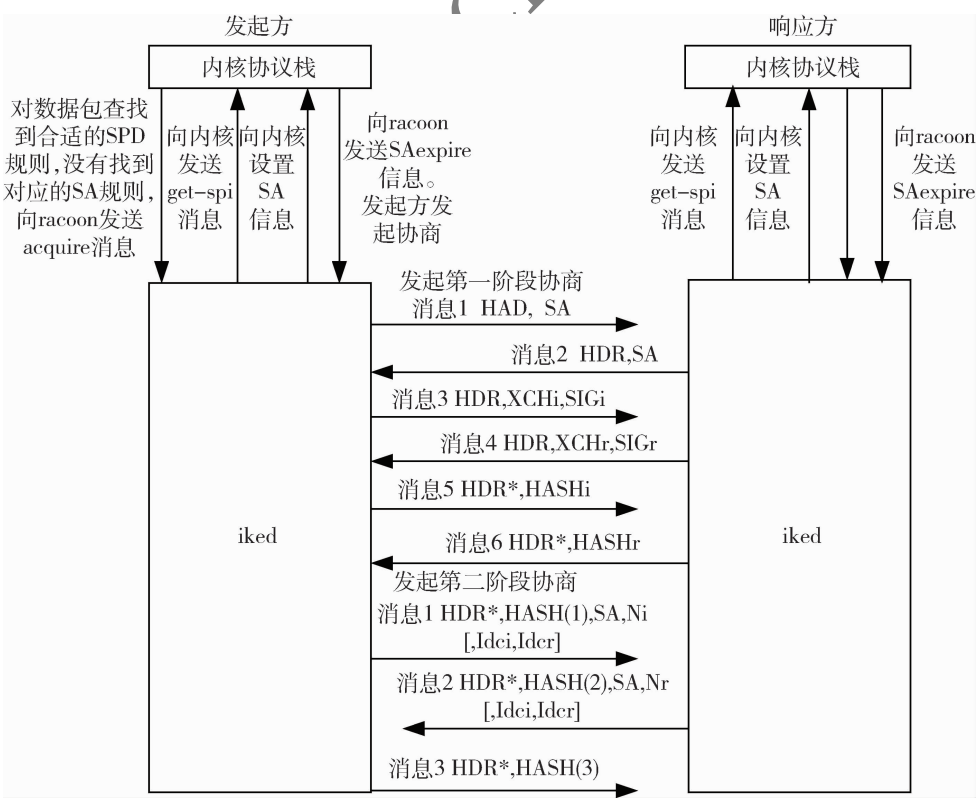

图 4 IPSec 密钥协商示意图

密钥协商主要包括两个阶段,其中第一阶段是IKE SA 协商,该阶段采用主模式,包括 6 个交互操作,主要是进行证书交换、身份认证以及工作密钥协商,该工作密钥用于保护第二阶段的会话密钥协商过程。第二阶段是 IPSec SA 协商,采用快速模式,包括 3 个交互操作,主要是协商出会话密钥,用于数据的加密传输。

2.2 SM2 密钥交换

在电力物联网信息安全防护中,加密认证的加密一般指数据传输过程的机密性保护,防范数据传输中遭受黑客的窃听攻击;而认证一般指数据传输前通信双方的身份真实性认证,防范伪造和假冒。

在物联网安全实践中主要有使用预设账号密码/设备 token 方式或使用非对称密码算法/数字证书方式进行身份真实性的鉴别认证。身份认证之后,为保证传输机密性,通过安全的方式生成会话密钥,目前常见的方式主要有 DH 方法、数字信封方法、SM2 密钥交换[9]方法。SM2 密钥交换协议是一种同时实现身份认证和会话密钥生成的协议,可以应用于基于 SM2 非对称密码算法的电力物联网设备之间的身份认证和会话密钥生成,其流程如图 5 所示。

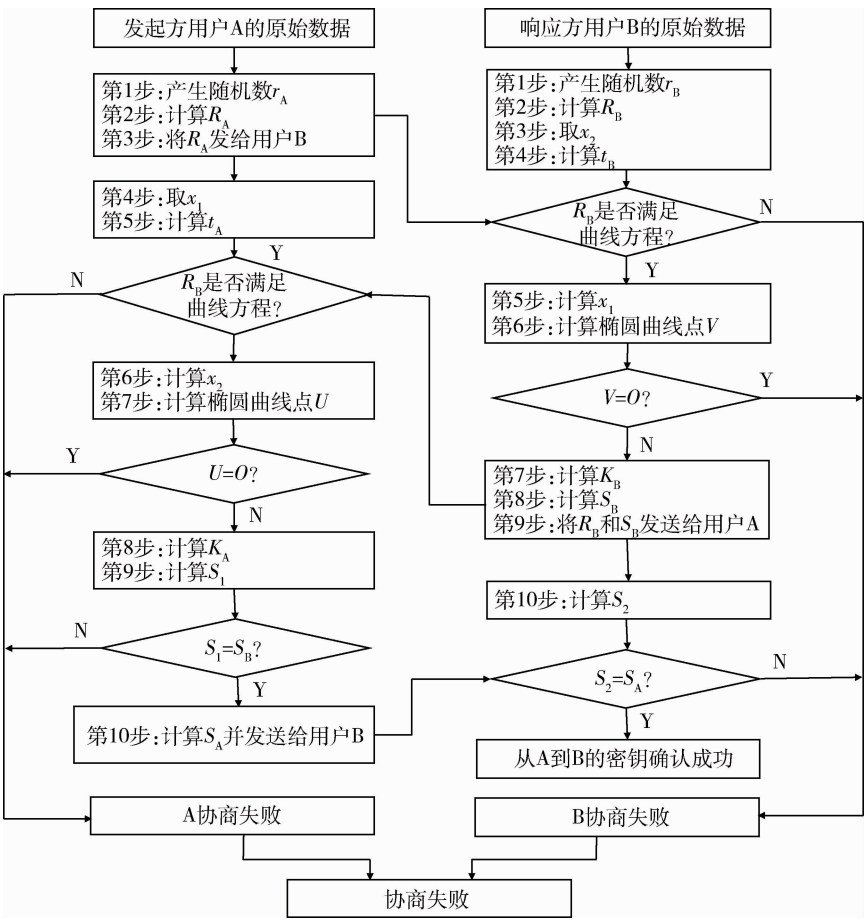

图 5 SM2 密钥交换流程图

2.3 密钥管理体系

对于广泛使用非对称密码算法的电力信息安全防护,每个电力物联网设备都将公开各自的公钥信息,而公钥信息的管理需要建设完善的公钥基础设施(Public Key Infrastructure,PKI)体系。在 PKI 体系中,最为重要的是 CA 系统建设和证书生命周期管理。在海量电力物联网终端场景下,传统主网基于离线部署方式的 CA 系统将难以满足业务的需求,新的部署模式又将可能带来新的安全风险。为此,研究基于标识的公钥算法(Identity-Based Cryptograph,IBC)在电力物联网应用也将可能是一个不错的解决方案。

SM9[10]是一种 IBC 算法,其密钥主要由密钥生成中心产生,涉及主密钥对(包括签名主密钥对和

加密主密钥对）和电力物联网设备的私钥。相比基于 SM2 或 RSA 的 PKI，IBC 可以极大地降低证书和公钥的管理难度，但设备私钥的生成过程导致其安全性会稍差一些。

2.4 应用报文安全检测技术

电力物联网终端往往部署在无人值守的户外，为降低黑客通过易物理访问电力物联网设备后，通过合法通信入侵电力物联网监控系统主站的风险，可以采用应用报文安全检测技术对电力物联网加密通道内的应用层协议报文进行安全性检测。

一方面，由于电力物联网监控系统主站的业务相对明确和单一，传输的报文规约也固定，可以使用白名单方式进行过滤和检测，从而防范和识别黑客攻击。

另一方面，可以使用机器学习等方法进一步对通信报文内容和报文到达的行为进行智能识别，从而达到对合法通道内的黑客攻击进行过滤和检测。

2.5 电力物联网终端设备本体安全防护

电力物联网终端设备容易失窃、容易遭受黑客物理访问和物理攻击，因而，除了电力物联网终端与主站之间的身份认证和传输加密之外，还应重点对电力物联网终端进行设备本体的信息安全防护，防护不仅包括芯片的故障注入、差分攻击、时间攻击、能量攻击等方面的防护，还应重点针对电力物联网终端的随机数和所有密钥的全生命周期管理方面，特别应在设备内设置检测和密钥应急销毁机制。

3 电力物联网终端安全防护设计

对于电力物联网终端设备本体的安全防护问题，36 号文和等级保护 2.0 标准中并未给出非常详细的设计方案。根据多年的物联网安全产品设计实践经验，总结设计了物联网终端产品安全防护由外往里的四道防线，如图 6 所示。

图 6 物联网终端产品安全四道防线设计示意图

第一道防线，物联网设备与外部交互过程安全防护，主要包括与物联网平台上行业务通道的安全防护和设备配置管理通道的安全防护。这一道防线可以采用传输加密、身份认证、报文检测、实体鉴别、双因素认证、登录失败策略控制、慢哈希等措施进行防护。主要用于防范设备与外部设备通信过程中的黑客窃听、扫描、重放、伪造等通信层面攻击。

第二道防线，物联网设备逻辑边界防护，这一防线在上行业务通道和设备配置管理通道上可以使用端口白名单、协议白名单、访问 IP 地址白名单等白名单机制进行设备防护。主要用于防范黑客对设备的扫描和非法访问。

第三道防线，物联网设备系统内部安全性检测，这一防线采用安全操作系统、设备内部程序/固件完整性检测、随机数检测、设备配置文件和证书文件的完整性检测等手段进行防护，同时特别注意升级固件包的完整性和真实性验证。这些防护手段分别在设备上电时、资源使用前和使用中进行周期检测。主要用于防范黑客若入侵系统后对系统的重要程序或配置参数进行篡改。

第四道防线，物联网终端设备内部的密钥防护，特别是私钥的保护。这一防线主要包括物联网终端产品的非法拆卸检测和密钥应急销毁联动机制以及物联网终端设备内部所有密钥从生成、导

出、存储、备份、更新、使用、销毁等的全生命周期安全管理和保护。主要用于防范黑客若入侵设备并获得系统超级管理员权限后获得密钥信息,或者黑客通过物理拆卸和侧信道攻击获得密钥信息。

4 结论

电力物联网信息安全防护是当前电力技术和应用发展的重要组成部分,是保障电力安全稳定运行的基础。本文总结了我国电力物联网信息安全防护的发展历程,分析了当下电力物联网信息安全应用中存在的主要问题和解决电力物联网信息安全的关键技术,最后设计提出了电力物联网终端本体的信息安全防护的四道防线模型和实践。

参考文献

[1] 江泽鑫. IEC60870-5-104 规约安全性分析及攻击实验[J]. 信息技术与网络安全,2018,37(10):1-4,14.

[2] 中华人民共和国国家发展和改革委员会, 中华人民共和国国家发展和改革委员会令 第 14 号[EB/OL]. (2014-08-01)[2019-10-10]. http://zfxxgk. nea. gov. cn/auto93/201408/t20140818_1832. htm.

[3] GB/T36572—2018, 电力监控系统网络安全防护导则[S]. 2018.

[4] 国家电力监管委员会.. 电力二次系统安全防护规定[EB/OL]. (2016-11-07)[2019-10-10]. http://jsb.nea. gov. cn/news/2006 - 11/2006117151906. htm.

[5] 国家能源局. 关于印发电力监控系统安全防护总体方案等安全防护方案和评估规范的通知[EB/OL]. (2015-03-12)[2019-10-10]. http://jsb. nea. gov. cn/news/2015 - 3/2015312105159. htm.

[6] 国家电力监管委员会. 电力二次系统安全防护方案[EB/OL]. (2016-11-10)[2019-10-10]. http://www.360doc. com/document/16/1211/16/38971085 _ 613815422. shtml.

[7] GB/T 22239 - 2019, 网络安全等级保护基本要求[S]. 2019.

[8] GM/T0022 - 2014, IPSecVPN 技术规范[S]. 2014.

[9] GMT 0003. 3 - 2012, SM2 椭圆曲线公钥密码算法[S]. 2012.

[10] GM / T 0044. 1 - 2016, SM9 标识密码算法[S]. 2016.

(收稿日期:2019-10-10)

作者简介:

江泽鑫(1985 -),男,硕士研究生,高级工程师,主要研究方向:工业物联网信息安全。

版权声明