电力 LTE 无线专网安全防护方案研究

韦 磊[1]，刘 锐[2]，高 雪[2]
(1.南京供电公司，江苏 南京 210019；2.国网电力科学研究院，江苏 南京 211106)

摘 要：从分析电力监控系统安全防护要求与所存在的安全威胁出发，论述了电力监控系统安全防护原则，针对长期演进(Long Term Evolution，LTE)系统结构及其在电力场景下的部署模式，进行了安全风险分析，并进一步给出了防护方法分析，最后从业务、LTE 网络、边界 3 个角度，提出了一套较为完整的电力 LTE 无线系统安全防护方案。方案为电力无线专网安全防护体系的建立提供了思路，在未来 LTE 网络安全策略制定中有一定的应用价值。

关键词：安全防护；LTE；电力通信系统
中图分类号：TM769 **文献标志码**：A **文章编号**：1009-0665(2016)03-0029-05

国网公司“十二·五”通信网规划中首次提出了“电力终端通信接入网”这一概念，标志着电力监控系统须遵循统筹规划、集中建设的发展思路，这有利于各电力业务间信息资源、通信网络的集约管理与环境共享。然而，电力监控系统统一化、信息化的发展趋势使得信息通信系统的安全问题凸显，防范外界对数据网络及计算机监控系统的攻击，保障电力系统安全稳定运行日益重要，建立和完善电力监控系统安全防护体系成为配用电通信系统规划设计中的重要环节。

目前所见的相关研究论著中，研究单一业务的信息安全防护较多，文献[1-3]均是针对电力调度、控制类业务制定业务系统专有安全方案；文献[4-6]侧重于对安全防护策略的论述或设计，与电力业务结合并不十分紧密。另外，于 2014 年实行的发改委第 14 号令与能源局电监安全 36 号文，在以往的防护要求基础上，有一些新的规定与调整，亟需体现到具体方案中去。

通信方式的选择也是终端通信接入网统一规划的一个关键环节。随着智能电网对通信的需求日趋完善与多元化，以长期演进(Long Term Evolution，LTE)为代表的新型专网无线通信技术在电力通信系统中的应用受到越来越多的关注。在网络安全防护方面，LTE 技术作为一种无线通信方式，除具有一般通信网络的固有安全问题外，在无线链路侧还有一些特有的安全威胁，如伪基站或伪终端的冒充、篡改、窃收、重放等[1]。文中结合 LTE 无线通信接入网络架构，在分析电力监控系统安全防护需求的基础上，提出一套完整的电力 LTE 无线专网安全防护方案。

1 电力监控系统安全防护原则

电力监控系统安全防护以“安全分区、网络专用、横向隔离、纵向认证”为设计原则。安全分区指对电力系统业务的重要程度及影响电力一次系统的强弱程度进行划分区域，对于生产电力及电力生产控制的系统进行重点防护；网络专用即按需采用隔离技术，实现不同业务通信系统的专网专用，为电力调度数据网与电力数据通信网提供多层次的防护；横向隔离即通过隔离装置在不同安全区之间实现逻辑或物理横向隔离；纵向认证即采用 IP 认证加密和硬件防火墙等方式实现各安全区的纵向安全防护。安全防护总体策略如图 1 所示。

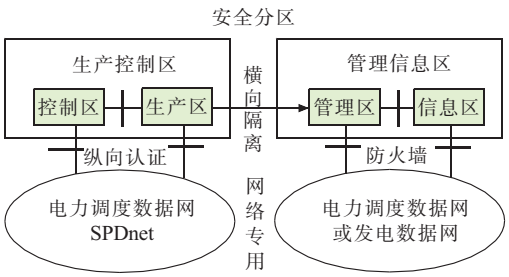

图 1 电力监控系统安全防护总体策略

电力监控系统根据业务的重要程度将安全工作区划分为生产控制大区和管理信息大区，其中生产控制大区又划分为实时控制区和非实时控制区。每个安全区都有不同的安全等级和防护要求。

特别地，于 2014 年实行的发改委第 14 号令与能源局电监安全 36 号文提出了安全接入区的概念，规范了接入网采用无线专网通信时安全接入区的边界隔离措施。

依据上述电力监控系统安全分区模型，根据国家政策、电信行业、电力二次系统安全防护和经验分析，电力通信网安全防护主要围绕“防网络攻击、保障数据安全”，“防物理损坏、保障可靠承载业务”两方面目标进行[2]。“防网络攻击、保障数据安全”即防止通信网络中传输、存储、处理的数据信息丢失、泄露或者被篡改；“防物理损坏，保障可靠承载业务”即防止通信网络阻塞、中断、瘫痪，或影响承载业务正常运行。

收稿日期：2015-12-24；修回日期：2016-02-23

2 安全风险及防护方法分析

2.1 安全风险分析

LTE 无线专网作为电力终端通信接入网时，将承载生产、营销、行政管理等多种电力业务数据传输。若不采取方案进行安全防护，电力 LTE 无线专网将面临多种安全风险，如图 2 所示。

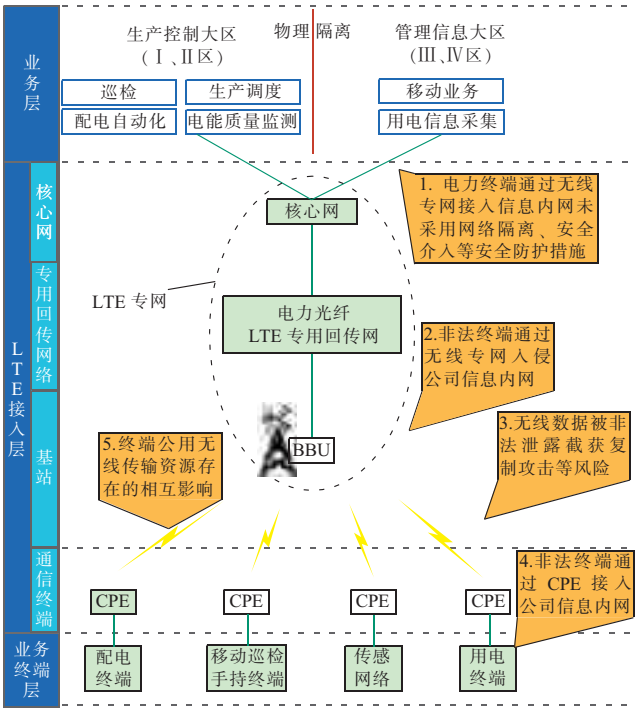

图 2 LTE 无线专网风险分析

LTE 无线通信终端(CPE)侧，在未作安全防护、隔离等措施的原始 LTE 系统中，终端通过无线专网接入，直接跨接在已物理隔离的 2 个信息内网上，存在如下安全风险：(1) 非法通信终端(伪终端)可能通过无线专网入侵公司信息内网；(2) 非法业务终端可能通过 CPE 接入公司信息内网；(3) 在终端和基站的双向通信过程中，无线数据或者控制命令可能被非法截获、篡改、伪造、重放攻击等；(4) 终端共用无线传输资源可能导致信道侧的相互干扰、占用等。

在 LTE 空口侧，无线网络被用于实现监测主站、子站和业务终端之间的通信，监测数据通过无线专网等通道明文传输可能被非法截获、篡改，重放攻击等，存在非法终端接入风险。同时，无线网络也是跨接在物理隔离的 2 张信息内网之间，同样会引起 2 张网络的物理隔离被打破，造成威胁的扩散。

2.2 防护方法分析

LTE 无线多业务承载网络的安全防护技术涉及电力业务安全防护、LTE 无线网络安全防护和终端安全防护 3 个方面。电力业务安全防护是指通信网络上承载的各类生产、营销、物资和管理等电力业务涉及的安全防护技术，电力业务安全需要根据业务种类不同，实施不同安全等级的安全防护措施[3]。如按照国网公司或行业标准中的要求，采取无线接入点名称(APN)和虚拟专用网络(VPN)等安全隔离、访问控制、认证加密、数字签名和基于非对称密钥技术的单向认证等安全措施。

LTE 无线网络安全防护主要针对 LTE 无线传输协议在数据传输时存在的三重安全隐患：(1) 数据接收方无法对数据来源的身份进行准确确认；(2) 数据接收方无法对接收到的数据的完整性进行确认；(3) 数据的收发双方都无法得知数据在传输过程中是否被第三方窥探过。针对上述网络协议的安全缺陷，LTE 无线网络安全防护主要采用 IP-VPN 技术，安全隧道技术和 Internet 协议安全性(IPSec)技术等加以解决。

终端安全防护是指满足无线终端安全性要求的安全防护技术或措施，包括：(1) 通过身份认证，防止非法终端接入网络向基站发送数据；(2) 防止伪基站向通信终端发送非法数据，从而威胁到业务终端的安全性；(3) 保障重要数据在无线链路传输过程中的机密性、完整性，防止非法监听和截获。

3 电力 LTE 无线专网安全防护方案

3.1 总体安全防护架构

安全防护总体方案依据“分区、分级、分域”的防护方针，在横向上，将系统分为生产控制大区(Ⅰ、Ⅱ区)与管理信息大区(Ⅲ、Ⅳ区)，纵向上，分为业务终端层、LTE 接入层、安全接入层和业务层等层面进行防护，以满足 LTE 无线专网系统的安全防护需求。系统总体防护框架如图 3 所示，业务终端层由配用电系统各类业务采集、检测等终端组成，是业务数据的来源；LTE 接入层即 LTE 无线专网系统，包括通信终端、基站、回传网络、核心网几个部分；安全接入层即 14 号令与 36 号文中规定的，采用无线或公用通信网络接入电力业务系统时所必须设置的“安全接入区”，一般由安全网关、防火墙等软硬件设备构成；业务层指各电力业务系统主站平台，是业务数据的应用层处理与控制中心。

按照电力监控系统安全防护要求和终端通信接入网络总体架构，并根据国网公司安全接入平台技术规范要求，应在信息内网边界部署安全接入平台，解决非公司信息内网区域的终端以安全专网方式接入信息内网的问题[4]。在该方案中，拟采用 VPN 技术和数据隔离技术实现数据的安全接入。

根据整个电力 LTE 无线专网系统的边界框架，将系统分为边界(网络区域边界)、监测系统(服务器)、LTE 通信网络、业务应用等层面进行防护，以满足电力 LTE 无线专网系统的安全防护需求。各业务终端处部署CPE，规范终端的自身安全防护问题，解决通过无线

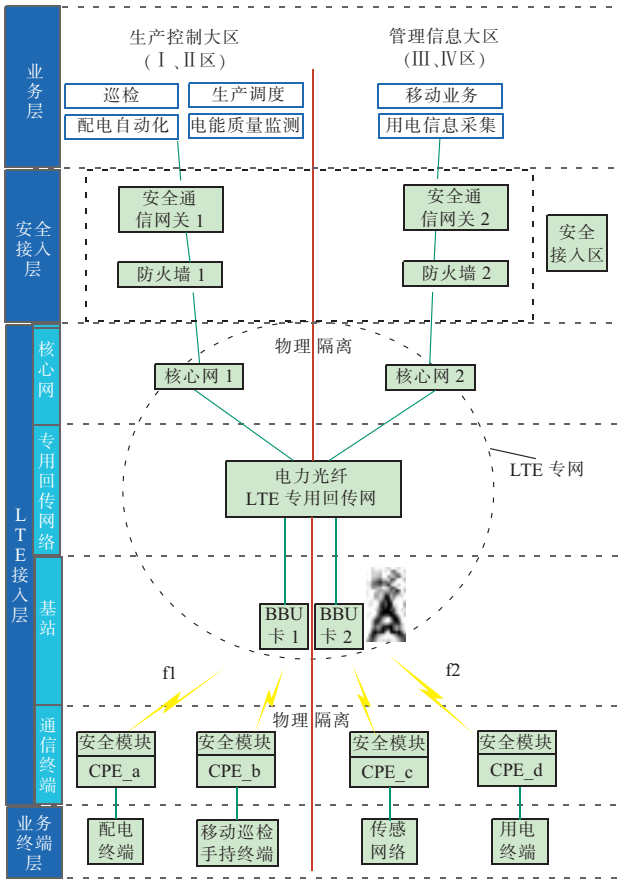

图 3 LTE 无线专网安全防护总体架构

网络传输数据的安全性问题。LTE 无线专网系统不改变业务终端原有身份认证与访问授权方式，不改变原有对接入对象的统一监管与审计，不影响原有业务的运行。

3.2 业务安全防护措施

电力业务安全防护措施针对不同大区的业务特点和安全防护要求,采用的业务安全措施也不尽相同。总体来说，统一承载不同业务的通信网络应遵循如下安全防护措施。

（1）业务主站侧安全防护。不同大区业务系统间应采用物理隔离防护措施，系统间需安装安全隔离装置。业务系统主站前置机应采用经国家指定部门认证的安全加固的操作系统,并采取严格的访问控制措施。接入网采用电力有线专网时，其前置机应配置安全模块;当采用无线通信技术、电力企业数据网或公用数据网时,接入网与主站业务系统间需设立“安全接入区”，安全接入区由单向认证模块、通信前置机及正反向隔离装置组成。

（2）业务子站及终端侧安全防护。终端设备上可配置安全模块，对来源于主站系统的控制命令和参数设置指令采取安全鉴别和数据完整性验证措施，防范冒充主站对终端进行攻击。为增加安全性,可配置具有双向认证加密能力的安全模块，实现主站和子站终端间的双向身份鉴别和数据加密。

终端的上行数据应通过安全模块生成摘要，使用对称算法计算相关的校验值，供主站识别数据传输的完整性,从而有效防止系统面临来自网络攻击的风险。

终端可以借助外置式、嵌入式等多种形式的安全模块实现安全防护过程。外置式安全模块适用于早期安装又不支持软件升级的终端；新安装的终端建议使用嵌入式安全模块，具体分为软算法库方式和安全芯片硬件方式(包括 DIP、SOP、TF 卡、SIM 卡等形态)。电力业务信息安全防护体系如图 4 所示。

由于生产控制大区的电力业务较信息管理大区的业务安全等级高[5],下文以Ⅰ区配电自动化业务为例具体介绍电力业务的安全防护措施。

配电自动化业务的信息安全防护系统涉及到的安全防护装置有防火墙、正 / 反向隔离装置、主站及终端安全模块等。

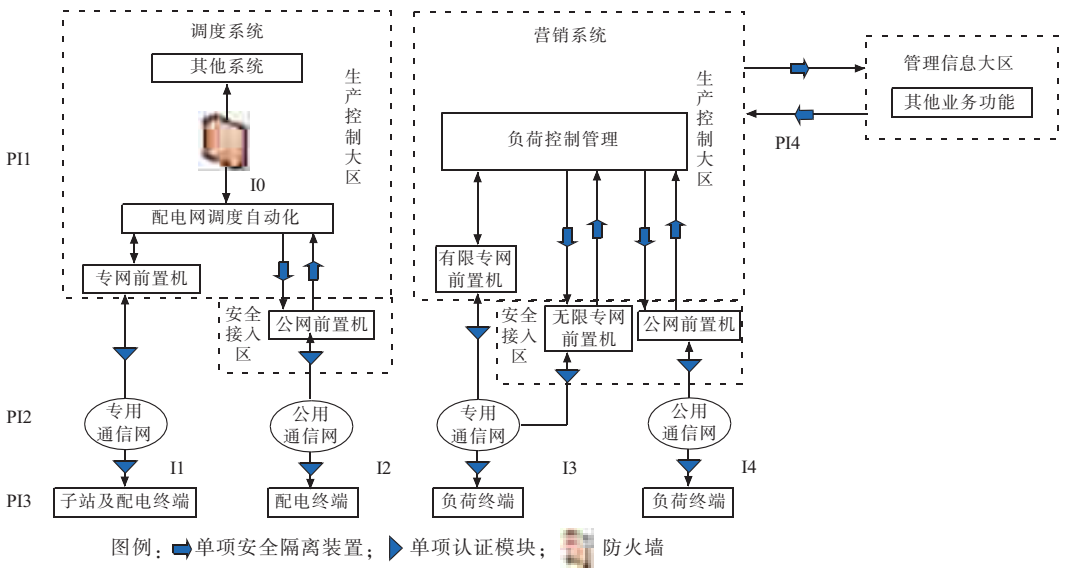

图 4 电力业务信息安全防护示意图

当配电网调度自动化系统与同一大区其他系统信息交互时,采用防火墙等逻辑隔离防护措施;当其与信息管理大区其他系统信息交互时,采用正/反向隔离装置进行物理隔离防护。

安全接入区位于主站侧与接入网侧之间,主要包括通信前置机、安全接入网关、安全审计等,当采用LTE无线专网接入时,还包括终端身份识别服务器(AAA)、安全监测系统(可选)等。当采用无线专网及公网传输通道时,前置机应配置安全模块(可选取串接配网安全网关、加装加密卡、旁接密码机等方式),对控制命令和参数设置指令进行签名操作,实现子站对主站的身份鉴别与报文完整性保护;对重要子站及终端的通信可采用双向认证加密,实现主站和子站间的双向身份鉴别,确保报文机密性和完整性。

信息安全综合审计是对配电通信网主站服务器、数据库等提供安全日志采集和分析技术支撑,为信息安全事件的追根溯源提供技术手段,实现对信息安全审计数据的自动分析,包括对运维安全审计、业务和数据库安全审计、主机日志安全审计、网络与边界安全审计,并进行信息汇总和关联分析,在配网系统中起到信息安全全面"故障录波"的作用。

3.3 LTE网络安全防护措施

LTE无线通信系统自身已具备完善的安全防护措施。但针对电力多业务统一承载这一特殊应用场景,还需引进IPSec VPN技术防护措施。

LTE系统分为用户设备、基站和核心网3个部分。用户设备和基站之间的通道叫做空中接口,基站和核心网之间的通道叫做回传网络。LTE无线网络的VPN安全防护分为空中接口安全防护和回传网络安全防护两部分,如图5所示。

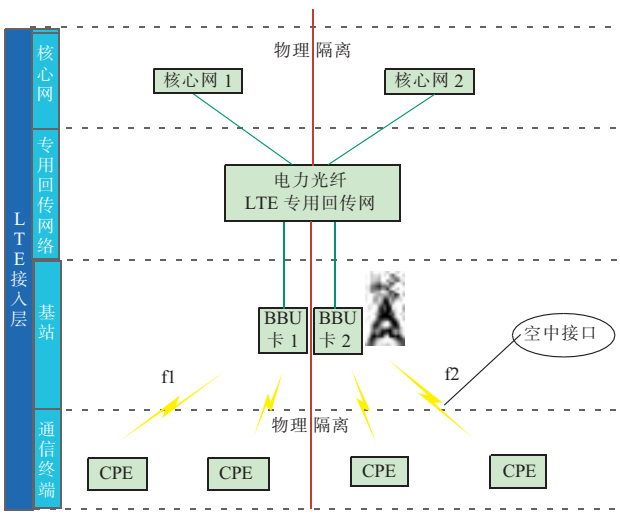

图5 无线网络安全防护措施

3.3.1 空中接口安全防护

空中接口安全防护措施用于保证CPE安全接入业务,防止空口攻击。具体包括:

(1)频率隔离,采用不同接入频率对生产终端和管理终端物理隔离;

(2)CPE身份保护:采用临时身份标识机制,保护用户隐私;

(3)网络认证,保证用户所访问的网络是合法(授权)网络;

(4)CPE认证,保证只有合法用户才能接入网络,防止伪终端接入;

(5)空口数据/信令加密保护,信令的完整性保护。

3.3.2 回传网络安全防护措施

回传网络安全传输方案如图6所示。3GPP标准建议eNodeB(LTE基站)的基站与核心网之间(S1)接口、基站与基站之间(X2)接口信令数据通过IPSec传输,于是将产生大量IPSec隧道。而在实际LTE网络部署中,X2接口流量可以通过网关节点转发,从而减少IPSec隧道数量,以降低设备处理负担。

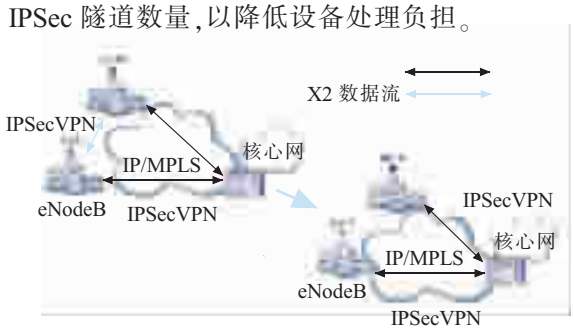

图6 针对回传网络的防护策略

LTE系统的回传网络采用不同光纤通道,对生产大区和管理大区的业务进行物理隔离。LTE网络安全传输技术可以应用IPSec VPN,在基站和基站之间建立IPSec隧道,采用CA双向认证。而基站间的信令交互通过网关节点转发,以更加安全可靠的物理隔离方式取代VPN隔离方式,提高了系统的安全性。

3.4 边界安全防护措施

网络边界是内部网络与外部接入网络之间的连接部分,在文中外部接入网络为LTE无线专网系统,边界处设备为LTE核心网。网络边界设备一般包括防火墙、安全网关等。边界安全防护关注如何对进出该边界的数据流进行有效监测和控制。电力LTE无线专网系统边界防护如图7所示。

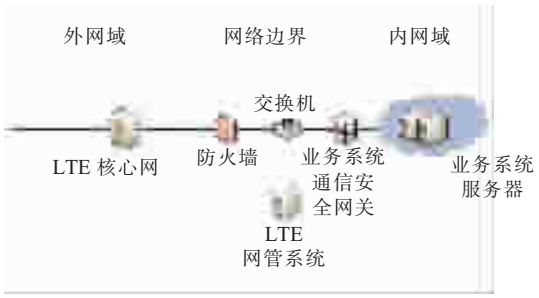

图7 针对边界的防护策略

(1) 防火墙,在 LTE 专网网络边界和外部网络的互联互通接口都要通过防火墙接入内部网络。防火墙应制定严格的访问策略实现专网域至网络边界域的访问控制。

(2) 安全网关,在 LTE 专网网络边界部署通信安全网关,对终端进行身份认证,对通信进行基于隧道的加解密,针对源地址制定访问控制(ACL),禁止不同 APN 业务互访。

(3) 安全防御,通信安全网关集成抗拒绝服务模块,识别攻击流和正常流,有效阻断攻击流,同时保证正常流通过,避免对正常流产生拒绝服务;防火墙集成防恶意代码攻击模块防御恶意代码攻击。

4 应用实例

上述安全防护方案在南京市溧水区 LTE 试点建设中进行了应用实践。具体措施如下。

(1) 业务信源加密:解决端到端应用层的业务数据加密问题。采用集成有安全加密认证模块的 LTE 可信终端设备 CPE,实现端到端的数据加密。信源解密在主站各类业务应用服务器完成。

(2) 接入层信道加密:解决接入层通信网络数据安全问题。CPE 完成信道加密,信道解密在 LTE 核心网完成。加密算法采用电力系统要求的国密算法。

(3) 身份认证:CPE 终端内置 USIM 卡,通过身份标识防止非法用户接入。

(4) 物理隔离:由于试点接入了配电自动化、用电信息采集、视频监控、智能家居、输电线路状态监测、负荷控制等不同安全大区的业务,采用基站处理单元(BBU)双板卡,以实现基站侧物理隔离。

(5) IPsec 隧道加密:确保 LTE 回传网络的安全可靠性。

(6) 安全接入区:针对 LTE 无线专网设立的安全接入区。由正反向隔离装置、前置机、安全接入网关构成。

溧水区 LTE 试点应用工程检验了该安全防护方案可行性。系统运行至今,安全防护效果良好,有效防止了伪基站、伪终端的接入及不同安全大区之间的信息渗透,安全防护体系具有较高的可靠性。

5 结束语

结合电力监控系统安全防护基本原则与配用电场景下的 LTE 无线专网架构,在分析了安全风险与防护方法的基础上,提出了一套较为完整的针对电力 LTE 无线接入专网的安全防护解决方案,重点解决涉及无线通信的安全接入、安全传输、终端自身安全以及身份认证、访问控制、数据过滤、统一监控与审计等六大类问题。在解决了面向多业务的 LTE 无线网络安全防护问题后,下一步研究方向为 LTE 无线专网所承载业务的 QoS 保障策略。

参考文献:

[1] 岳宏亮,陈鹏良,楼书氢. 地区电网控制中心二次系统安全防护策略分析[J]. 中国电力教育,2014(33):180-186.

[2] 周小燕,杨宏宇,崔恒志,等. 地区电力调度中心二次系统安全防护[J]. 江苏电机工程,2005,24(2):50-52.

[3] 焦 伟. 电力调度自动化网络安全防护系统的研究与实现[D]. 北京:华北电力大学,2014.

[4] 袁 慧. 面向用户准入控制的信息安全统一威胁防御管理[J]. 电力信息与通信技术,2015,9(11):102-105.

[5] 周 宁. 重庆电网二次系统安全防护体系结构及关键技术研究[D]. 重庆:重庆大学,2005.

[6] 李文武,游文霞,王先培. 电力系统信息安全研究综述[J]. 电力系统保护与控制,2011,10(39):140-147.

作者简介:

韦 磊(1982),男,江苏南京人,高级工程师,从事电力系统信息通信研究与管理工作;

刘 锐(1981),男,安徽合肥人,工程师,从事电力系统通信技术研究工作;

高 雪(1988),女,江苏连云港人,助理工程师,从事电力系统通信技术研究工作。

Research on Security Protection Solution to LTE Power Wireless Private Network

WEI Lei[1], LIU Rui[2], GAO Xue[2]

(1. Nanjing Power Supply Company, Nanjing 210019, China;

2.State Grid Electric Power Research Institute, Nanjing 211106, China)

Abstract: This paper discusses the security protection principle of electric power monitoring system through analyzing the requirements of security protection and the existing security threats in electric power monitoring system. According to the structure of LTE system and its deployment pattern in electric power area, the protection methods are analyzed by using safety risk analysis. At the end, from the point of views of business side, LTE messing and boundary, a fully protective solution to LTE wireless system in electrical area is proposed. This solution provides ideas for establishing security protection system of special wireless network in electric power area, and it is certainly valuable to developing security strategy for LTE network in the future.

Key words: security protection; LTE; electric power communication system