ICS 29.240.01
F 21
备案号：68897-2019

DL

中华人民共和国电力行业标准

DL / T 1931 — 2018

电力 LTE 无线通信网络安全防护要求

Security protection requirements on LTE wireless communication network for power system

2018-12-25发布　　2019-05-01实施

国家能源局　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009《标准化工作导则　第 1 部分：标准的结构和编写》给出的规则起草。

本标准由中国电力企业联合会提出。

本标准由全国电力系统管理及其信息交换标准化技术委员会（SAC/TC 82）归口。

本标准起草单位：国网电力科学研究院有限公司、广东省电力设计研究院、国网江苏省电力有限公司、东南大学、华为技术有限公司、中兴通讯股份有限公司、南京南瑞继保电气有限公司、国网河北省电力有限公司、南京千步智能科技有限公司。

本标准主要起草人：卞宝银、黄鑫、汪晓岩、黄盛、韦磊、许威、刘庆江、许俊现、刘佳、刘金锁、李芹、张鑫、何晓阳、李秀彩、李文猛、张合明、王艺桦、高雪、杨贵、何应利、房树超、仇勇、宗俊丽、胡阳、王栋、马涛。

本标准为首次发布。

本标准在执行过程中的意见或建议反馈至中国电力企业联合会标准化管理中心（北京市白广路二条一号，100761）。

电力 LTE 无线通信网络安全防护要求

1 范围

本标准规定了电力 LTE 无线通信网络的基本构成与安全风险、总体要求、网络安全防护要求，网管安全防护要求和运行环境安全防护要求等。

本标准适用于电力系统中应用的 LTE 无线通信网络及设备。

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 2423.3 环境试验 第 2 部分：试验方法 试验 Cab：恒定湿热试验

GB/T 2423.4 电工电子产品环境试验 第 2 部分：试验方法 试验 Db：交变湿热（12h＋12h 循环）

GB/T 4208 外壳防护等级（IP 代码）

GB/T 14598.3 电气继电器 第 5 部分：量度继电器和保护装置的绝缘配合要求和试验

GB/T 15153.2 远动设备及系统 第 2 部分：工作条件 第 2 篇 环境条件（气候、机械和其他非电影响因素）

GB/T 17626.2 电磁兼容 试验和测量技术 静电放电抗扰度试验

GB/T 17626.3 电磁兼容 试验和测量技术 射频电磁场辐射抗扰度试验

GB/T 17626.4 电磁兼容 试验和测量技术 电快速瞬变脉冲群抗扰度试验

GB/T 17626.5 电磁兼容 试验和测量技术 浪涌（冲击）抗扰度试验

GB/T 17626.11 电磁兼容 试验和测量技术 电压暂降、短时中断和电压变化的抗扰度试验

GB/T 17626.12 电磁兼容 试验与测量技术 振铃波抗扰度试验

GB/T 17626.29 电磁兼容 试验和测量技术 直流电源输入端口电压暂降、短时中断和电压变化的抗扰度试验

GB 50011 建筑抗震设计规范

GB 50689 通信局（站）防雷与接地工程设计规范

YD/T 1744 传送网安全防护要求

国家发展和改革委员会令 2014 年第 14 号 电力监控系统安全防护规定

3 术语和定义

下列术语和定义适用于本文件。

3.1

长期演进 long term evolution；LTE

由 3GPP（The 3rd Generation Partnership Project，第三代合作伙伴计划）组织制定的通用移动通信系统技术标准的长期演进。

3.2

电力 LTE 无线通信网络 LTE wireless communication network of power system

电力企业自行建设、管理的采用 TD-LTE 和 LTE FDD 技术的专用无线通信网，包括电力 LTE 无线通信系统和电力 LTE 无线通信回传网，用于完成配用电、线路监测、视频监控等终端业务的接入承载。

3.3

物理隔离　physical isolation

不同通信网络之间不能直接通信，并且各自使用的不同通信网络的物理介质和通信设备的信息存储空间等资源独立专用。

利用不同时隙隔离或频率（波长）隔离可达到或接近物理隔离的强度。

3.4

逻辑隔离　logical isolation

不同通信网络之间不能直接通信，但各自使用的通信网络的物理介质、时隙、频率（波长）和通信设备的信息存储空间等资源可共享，通过技术手段（如：VPN、VLAN 等）保证在逻辑上是隔离的。

3.5

安全接入区　secure access area

专用通信网络、公共网络或其他通信网络接入生产控制大区和信息管理大区的安全防护和监管区域。

3.6

安全接入平台　union security access platform

对非信息管理大区区域终端提供以安全专网方式接入信息管理大区，并采用终端接入认证、数据隔离、实时监测审计等防护措施对接入边界进行防护。

4　缩略语

下列缩略语适用于本文件。

APN	access point name	接入点
BBU	base band unit	基带单元
FDD	frequency division duplex	频分复用技术
IPSec	Internet protocol security	IP 安全协议
MSTP	multi-service transport platform	业务传送节点
OTN	optica1 transport network	光传送网
PDN	public data network	公共数据网
PKI	public key infrastructure	公钥基础设施
QoS	quality of service	服务质量
RRU	remote RF unit	射频远端单元
SDH	synchronous digital hierarchy	同步数字体系
SSL	security socket layer	传输安全协议
TD-LTE	time division long term evolution	分时长期演进技术
VPN	virtual private network	虚拟专用网络
VLAN	virtual local area network	虚拟局域网
HTTPS	hyper text transfer protocol secure	超文本传输安全协议

5　电力 LTE 无线通信网络基本构成与安全风险

5.1　电力 LTE 无线通信网络基本构成

5.1.1　基本构成

电力 LTE 无线通信网可分为核心层、回传网、接入层和终端层，电力 LTE 无线通信网络架构如图 1 所示。

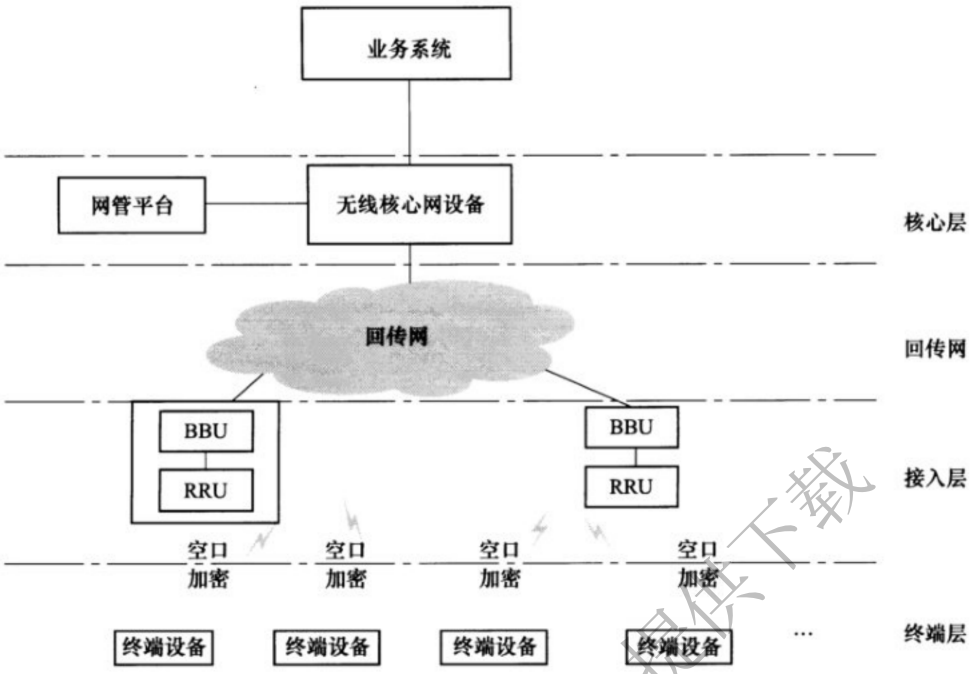

图 1　电力 LTE 无线通信网络架构

5.1.2　核心层

核心层主要包括移动性管理实体、服务网关、PDN 网关、归属用户服务器等网元，提供用户接入控制和安全管理、网络连接和会话管理、移动性管理、计费管理以及服务质量（QoS）管理等功能。整个核心层通过统一的网络管理系统进行集中的维护。

5.1.3　回传网

回传网主要包括光传送网络（SDH/MSTP 和 OTN 等）、微波接力传送网络和卫星传送网络等，用于实现核心层和接入层的数据互通。

5.1.4　接入层

接入层包括无线基站及其配套设备，主要为用户终端提供无线接入信号，负责无线资源的管理。

5.1.5　终端层

终端层由各类不同类型的终端组成，实现电力系统业务的数据交互，终端类型包括固定台、无线数据卡、手持终端等。

5.2　电力 LTE 无线通信网安全风险

电力 LTE 无线通信网的安全风险可分为网络及设备安全风险、环境安全风险和管理安全风险。环境安全风险包括自然界不可抗的风险和其他物理风险。管理风险主要包括安全管理机构、安全管理制度、人员安全管理、建设管理和运维管理。主要风险参见附录 A。

6　总体要求

6.1　电力 LTE 无线通信网安全防护应符合《电力监控系统安全防护规定》的规定。电力 LTE 无线通信网络安全防护方案如图 2 所示。

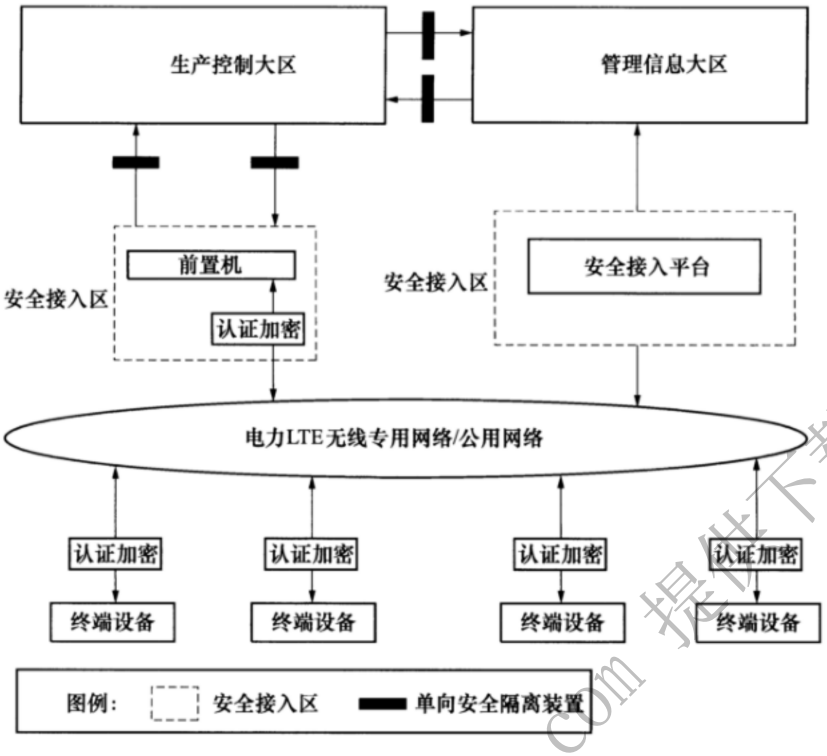

图 2　电力 LTE 无线通信网络安全防护方案

6.2　生产控制大区和信息管理大区的业务系统在与其终端的连接中使用电力 LTE 无线通信网络或公用网络等进行通信的，应设立安全接入区。接入生产控制大区的安全接入区应包含物理隔离部件、前置机和加密认证设备等。接入信息管理大区的安全接入区应包含安全接入平台和加密认证设备等。

6.3　终端设备应采用认证加密机制、访问控制措施，建立加密传输通道进行信息采集，保证业务数据的保密性和完整性。

6.4　电力 LTE 无线通信安全防护总体方案按照“分区、分级、分域”的防护原则，对核心层、回传网、接入层和终端层分别采取防护措施。

6.5　电力 LTE 无线通信网络安全防护主要类型及要求见表 1。

表 1　电力 LTE 无线通信网络安全防护主要类型及要求

防护类型	要　　求
网络隔离	电力 LTE 无线通信网络应与调度数据网物理隔离，确保调度数据网的网络专用性
业务隔离	业务终端应分别通过安全接入区接入生产控制大区和信息管理大区，各大区不同业务接入不同逻辑分区网络
网络管理安全	电力 LTE 无线通信网络应可管可控，网管操作与用户设备接入应鉴权认证审计，网络边界应实施安全防护控制措施，宜实现网络流量监测、分析、告警功能
频谱合法	电力 LTE 无线通信网络应采用国家无线电管理部门授权的无线频率组网
设备安全	无线通信设备支持高安全性的认证管理技术，应充分考虑电力特殊应用环境，如强电磁干扰等情况
管理安全	运行管理应配置完善的安全防护规章制度，杜绝内部人员的滥用权限与错误操作。应配置合适的安全管理技术手段，查漏补缺，识别与防范外部人员的安全攻击

7 电力 LTE 无线通信网络安全防护要求

7.1 网络结构安全防护要求

电力 LTE 无线通信网络应实现承载业务的逻辑隔离，不同电力业务终端接入无线网络时应根据不同安全分区级别和业务类型，接入不同专用接入点（APN）和对应虚拟 VPN，电力 LTE 无线专网安全方案框图如图 3 所示。

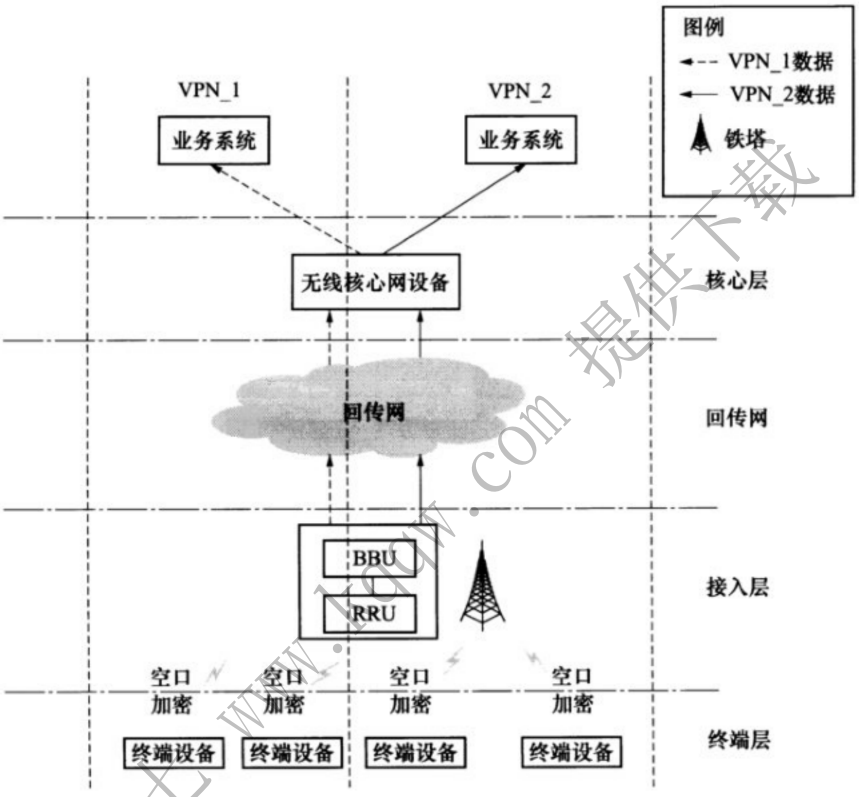

图 3 电力 LTE 无线专网安全方案框图

7.2 核心层安全防护要求

7.2.1 访问通道安全

访问通道安全应满足如下要求：

a） 应保证管理平面与用户平面隔离；

b） 所有能对系统进行管理的逻辑通信端口及协议都应具备接入认证机制（协议标准定义中无认证机制的除外），相关接入认证机制应缺省启用；

c） 所有在设备外部可见的能对系统进行管理的物理接口应具备接入认证机制，以防止非授权访问，相关接入认证机制应缺省启用；

d） 对于人机接口或可远程访问的机机接口之间，产品默认在所有口令设置时进行复杂度检查，若口令不符合复杂度规则，应禁止设置并进行警告；

e） 对于人机接口或可远程访问的机机接口之间，产品应提供防暴力破解机制，如登录失败尝试次数超阈值时的锁定和解锁机制；

f） 所有账户都应可被系统管理，禁止存在用户未知的账户，并在产品资料中提供所有账号及管理操作说明。

7.2.2 操作系统安全

操作系统安全应满足如下要求：

a） 产品应使用业界主流漏洞扫描工具对产品进行漏洞扫描测试；

b） 正式发布的版本应包含默认的操作系统安全加固策略文件；

c） 产品补丁计划中应包含操作系统安全补丁发布计划，并在公开网站上提供下载。

7.2.3 安全日志及审计

日志审计应满足如下要求：

a） 日志记录应涵盖管理平面上所有的用户活动和操作指令；

b） 用户活动、操作指令的日志应支持回溯审计；

c） 产品提供的日志模块/文件有相应的访问控制机制。

7.2.4 数据库安全

数据库安全应满足如下要求：

a） 产品出厂使用的数据库口令禁止使用数据库厂商的缺省口令；

b） 产品缺省应启用数据库口令复杂度检查功能；

c） 使用单独的操作系统的非管理员权限账号来运行数据库；

d） 数据库系统本身的文件及用户的数据文件应严格控制访问权限；

e） 对数据库账户授予的权限应进行严格清晰的划分。

7.2.5 冗余设备及系统要求

冗余设备及系统应满足如下要求：

a） 核心层主用节点出现故障，备用节点应接管主用节点服务，业务中断可快速恢复；

b） 核心层应提供记录、定位、排除主用节点故障的工具和手段；

c） 可根据业务需求配置冗余设备。

7.3 回传网安全防护要求

回传网安全防护要求参见 YD/T 1744，回传网应禁止使用调度数据网承载。

7.4 接入层安全防护要求

7.4.1 传输链路安全

传输链路安全应满足如下要求：

a） 应提供基站与周边网元、周边设备之间的操作维护传输链路、用户数据传输链路、信令传输链路等的安全保护，建立以 PKI 证书机制为中心的安全传输链路；

b） 应采用 IPSec 等安全隧道方式接入。

7.4.2 频率安全

应采用国家无线电管理部门授权的无线频率。

7.4.3 无线接口安全

宜提供基站与终端之间无线接口传输数据的机密性和完整性保护。

7.4.4 基站设备安全

应提供基站设备本身的保护，包括物理安全和防火墙功能。物理安全应保证基站硬件和站点安全；防火墙功能应保证基站输入的安全。

7.4.5 基站操作维护安全

基站操作维护安全应满足如下要求：

a） 应对接入基站设备的操作维护用户进行用户认证和访问控制，识别用户身份并对合法用户合理授权，约束用户的操作和可以访问的资源；
b） 系统应提供安全日志，具备安全事件的上报告警功能；
c） 应提供端到端传输安全协议（SSL）认证功能；
d） 应保证软件版本完整性。

7.5 终端层安全防护要求

7.5.1 终端硬件安全

终端硬件安全应满足如下要求：

a） 对外提供的近端业务、维护接口应具备安全认证功能；
b） 对外提供的近端无线接口应支持软件开启/关闭，应支持安全接入能力；
c） 应提供明确的物理（包括有线/无线）接口及其安全接入管控方式，不在未公开的外部硬件或软件接口。

7.5.2 终端接入安全

终端接入安全应满足如下要求：

a） 应能对接入的用户进行鉴权认证，验证用户的合法性，保证授权用户能够接入网络；
b） 应支持用户与无线通信网络之间的密钥协商机制，保证数据传输安全；
c） 应在系统边界部署访问控制设备，并启用访问控制功能；
d） 应对进出网络的信息内容进行过滤，实现对应用层协议命令级的控制；
e） 应采取技术手段防止地址欺骗；
f） 应按照访问规则，决定允许或拒绝管理用户对系统的资源访问；
g） 宜使用 HTTPS/SSL 等安全连接技术，防止敏感信息泄露。

8 网管安全防护要求

8.1 网管安全防护能力

8.1.1 用户管理、认证与鉴权

用户管理、认证与鉴权应满足如下要求：

a） 应采用强密码策略，对密码长度、特殊字符组合要求、密码错误次数和解锁时间等进行限制，保证系统用户密码的安全性；
b） 应支持系统用户安全管理功能，如操作时效性、超长时间自动锁定和自动注销等；
c） 应支持网管用户的集中管理功能，如账户管理、权限分配、用户鉴权等。

8.1.2 安全日志与审计

安全日志与审计要求见 7.2.3。

8.1.3 操作系统及数据库安全

操作系统及数据库安全应满足如下要求：

a） 操作系统应支持最小化安装，只安装和启用网管系统的组件及服务，并提供定期更新机制，同时关闭所有无用网络连接端口；

b） 网管数据库安全要求见 7.2.4。

8.1.4 系统连接及文件传送安全

网管系统服务器与网元设备、客户端及其他外部系统的连接、文件传输需支持安全传输协议。

8.2 网管数据备份与恢复

网管数据备份与恢复应满足如下要求：

a） 应建立对业务及应用关键数据和重要信息进行备份和恢复的管理和控制机制；

b） 相关业务及应用的关键数据（如业务数据、系统配置数据、管理员操作维护记录、用户信息等）应有必要的容灾备份；

c） 系统应提供数据自动保护功能，当发生故障后应保证系统应能够恢复到故障前的业务状态。

9 运行环境安全防护要求

9.1 通信设备环境适应性要求

9.1.1 环境适应性

设备环境适应性应满足 GB/T 15153.2 要求，具体环境参数见表 2。通信设备在规定的气候条件下应能正常工作。

表2 环境适应性要求

序号	项　　目	室外设备	室内设备	单　　位
1	低温	−40	−5	℃
2	高温	+70	+45	℃
3	低相对湿度	5	5	%
4	高相对湿度	95	95	%
5	低绝对湿度	0.1	0.5	g/m^3
6	高绝对湿度	35	29	g/m^3
7	温度变化率	1	0.5	℃/min
8	低气压	70	70	kPa
9	高气压	106	106	kPa
10	太阳辐射	1120	700	W/m^2
11	凝露条件	有	有	—

表 2（续）

序号	项　　目	室外设备	室内设备	单　　位
12	降水条件（雨、雪、雹等）	有	无	—
13	结冰和结霜条件	有	有	—
注 1：低和高相对湿度，受低和高绝对湿度的限制； 注 2：温度变化率取 5min 时段的平均值； 注 3：70kPa 表示户外使用的限值，通常海拔约为 3000m,对于海拔更高的场所，应考虑一个比较低的值。				

9.1.2 绝缘性能

设备绝缘性能应满足 GB/T 14598.3 中规定要求，绝缘性能试验结束后设备应能正常工作。

9.1.3 湿热性能要求

湿热性能应满足如下要求：

a） 室内设备应能承受 GB/T 2423.3 规定的恒定湿热试验要求，温度（40±2）℃，湿度（93±3）%，48h，试验过程中设备不通电，试验后各导电回路对外非带电导电部位及外壳之间、电气上无联系的各回路之间的绝缘电阻不应小于 1.5MΩ；

b） 室外设备应能承受 GB/T 2423.4 规定的交变湿热试验要求，高温温度 40℃，低温温度 25℃，48h，试验过程中设备通电，试验期间及试验结束后均应保持正常工作状态。

9.1.4 机械性能要求

通信设备机械性能要求应符合 GB/T 15153.2 要求，具体参数见表 3，试验结束后设备应无损伤，应能正常工作。

表 3 机械性能要求表

序号	项　　目	设 定 参 数	等 级 参 数		
1	正弦稳态振动	位移幅值 mm	7		
		加速度幅值 m/s^2		20	15
		频率范围 Hz	2～9	9～200	200～500
2	冲击	半正弦脉冲持续时间 ms	11		
		峰值加速度 m/s^2	300		
3	自由跌落	跌落高度 m	0.25		
注 1：正弦稳态振动项目，频率范围为 2Hz～9Hz 时，设定参数中选择位移幅值，加速幅值不适用。 注 2：正弦稳态振动项目，频率范围为 9Hz～200Hz 和 200Hz～500Hz 时，设定参数中选择加速幅值，位移幅值不适用。					

9.1.5 电磁兼容

通信设备的抗电磁干扰能力应满足表 4 要求，试验期间及试验结束后设备应无损伤，均应能正常工作。

表 4　抗电磁干扰性能要求

序号	项　　目	参 考 标 准	严 酷 等 级
1	静电放电抗扰度	GB/T 17626.2	3 级
2	射频电磁场辐射抗扰度	GB/T 17626.3	3 级
3	电快速瞬变脉冲群抗扰度	GB/T 17626.4	3 级
4	浪涌（冲击）抗扰度	GB/T 17626.5	3 级
5	交流电源暂时中断抗扰度	GB/T 17626.11	500ms/0%
6	振荡波抗扰度	GB/T 17626.12	3 级
7	直流电源暂时中断抗扰度	GB/T 17626.29	10ms/0%

9.1.6　外壳防护

外壳防护应满足如下要求：

a）　室外设备应满足 GB/T 4208 标准中定义的 IP65 等级；

b）　室内设备应满足 GB/T 4208 标准中定义的 IP20 等级。

9.2　室外设备场地物理环境

9.2.1　室外安装位置选择

室外设备场地应选择具有防震、防风和防雨等能力的建筑内；室外设备场地整体抗震能力应满足 GB 50011 要求；室外天线防雷应满足 GB 50689 要求。

9.2.2　防盗窃和防破坏

外壳防护应满足如下要求：

a）　应将主要设备放置在物理受限的范围内；

b）　应对设备或主要部件进行固定，并设置明显的不易除去的标记；

c）　应将通信线缆铺设在隐蔽处，如铺设在地下或管道中等。

9.2.3　防火

应设置灭火设备，并保持灭火设备的良好状态。

9.2.4　温湿度控制

宜设置温湿度自动调节设施，使室外无线接入设备所处环境的温、湿度的变化在设备运行所允许的范围之内。

9.2.5　电力供应

应设置稳压器和过电压防护设备；应提供短期的备用电力供应（如 UPS 设备）。

附 录 A
（资料性附录）
电力无线通信网络主要安全分析

电力无线通信网络主要安全分析见表 A.1。

表 A.1 电力无线通信网络主要安全分析

风险来源		风险分析
网络及设备安全风险		1. 网络拓扑设计不合理，网络节点设备、路由配置不合理，通信安全保护不充分，网络存在安全漏洞，外部和内部的访问控制不够。 2. 回传网拓扑设计不合理，使用公网或者使用调度通信网导致的安全风险。 3. 网络和设备的处理能力不够而导致在突发流量时业务提供不连续；业务数据的保密性不够，重要数据未及时进行本地和异地备份。 4. 账号和口令保护不够，鉴权和访问控制机制不完善，重要部件未配置主备用保护，系统配置不合理、设备补丁安全不及时更新、设备防病毒和攻击能力不够，备份和恢复机制不健全，设备超过使用年限或核心部件老化，设备发生故障后未及时报告。 5. 非法终端通过无线专网入侵电力内部数据网和信息系统。 6. 无线数据信号被非法泄露截获、复制攻击。 7. 终端共用无线传输资源存在相互影响
环境安全风险	物理环境	机房场地选择不合理，防火、供配电、防静电、接地与防雷、电磁防护、温湿度控制不符合规范，通信线路、机房设备的保护不符合规范
	自然环境	鼠蚁虫害、洪灾、火灾、泥石流、山体滑坡、地震、台风、雷击等
管理安全风险	安全管理机构	岗位设置不合理（如人员配置过少、职责不清），授权和审批程序过于简化，沟通和合作未执行，审核和检查未执行等
	安全管理制度	管理制度不完善、制度评审或修订不及时等
	人员安全管理	人员录用不符合程序，人员离岗未办理安全手续，人员未进行安全培训，对于第三方人员未进行限制访问等
	建设管理	安全方案不完善，软件开发不符合程序，工程实施未进行安全验收或验收不严格等
	运维管理	物理环境管理措施简单，存储介质使用不受限，设备没有定期维护，厂家支持力度不够，关键性能指标没有定期监控，无恶意代码防范措施，无数据备份和恢复策略，访问控制不严格，操作管理不规范等，应急保障措施不到位

中 华 人 民 共 和 国
电 力 行 业 标 准
电力 LTE 无线通信网络安全防护要求
DL / T 1931 — 2018
*
中国电力出版社出版、发行
（北京市东城区北京站西街 19 号　100005　http://www.cepp.sgcc.com.cn）
北京传奇佳彩印刷有限公司印刷
*
2019 年 7 月第一版　　2019 年 7 月北京第一次印刷
880 毫米×1230 毫米　16 开本　1 印张　25 千字
印数 001—500 册
*
统一书号 155198・1517　定价 **15.00** 元

155198.1517