电力无线专网多业务隔离技术研究

江　华[1]，孙圆圆[2]
（1. 国网宁夏电力公司银川供电公司，宁夏　银川　750011；
2. 国网宁夏电力公司检修公司，宁夏　银川　750011）

摘　要： 通过研究当前电力无线专网现状，分析配用电业务对网络的通信需求及多业务隔离需求，提出基于 RAN-SHARING 和基于物理隔离的无线专网多业务承载隔离实施方案，实现不同安全大区业务的物理隔离和同一安全大区的逻辑隔离，为未来不同类型配用电业务混合组网和建设提供技术支撑。应用结果表明：该方案能够有效节约建网成本，提高电力服务水平。

关键词： 无线专网；TD-LTE；多业务隔离
中图分类号： TM78　　**文献标志码：** A　　**文章编号：** 1672-3643(2015)03-0051-06
有效访问地址： http://dx.doi.org/10.3969/j.issn.1672-3643.2015.03.011

Research on multi task isolation technology of special wireless power network

JIANG Hua[1], SUN Yuanyuan[2]
(1. Yinchuan Power Supply Filiale of State Grid Ningxia Power Co., Yinchuan Ningxia 750011, China;
2. Maintenance Filiale of State Grid Ningxia Power Co., Yinchuan Ningxia 750011, China)

Abstract: By studying the status quo of the current special wireless power network, analyzes the requirements of power distribution and consumption business on network communication and multi task isolation, puts forward implementation schemes of special wireless power network multi task operation and isolation based on RAN-SHARING and physical isolation, realizes business physical isolation in different security region and logic isolation in the same security region, provides the technical support for the hybrid networking and construction of different types of power distribution and consumption business in the future. The application result shows that the scheme can effectively save the cost of network construction and improve the power service level.

Key words: special wireless network; TD-LTE (time division long term evolution); multi task isolation
DOI: 10.3969/j.issn.1672-3643.2015.03.011

电力终端通信接入网作为智能电网的重要组成部分，处于电力系统通信网络的末端，覆盖范围广，通信节点较为分散。随着网络覆盖范围和建设规模逐年扩大，仅仅依赖光纤通信已经难以满足

收稿日期： 2015-03-29
作者简介： 江华(1982)，男，工程师，从事电力系统通信技术管理工作。

不同区域、不同业务的所有需求。因此，在光纤通信网络难以覆盖的地区，选择合理的无线通信网络是建设安全、可靠、实时、经济的电力终端接入网的重要环节。当前电力终端通信接入网，尤其是采用新型 TD-LTE 无线宽带接入技术的网络，在多业务承载和网络性能评估方面还存在许多问题。一方面，现有电力终端通信接入网一般根据业务部门需求单独建设，虽然有效地实现了不同安全大区业务的物理隔离，但每个物理网络仅承载同一安全分区的业务，网络资源独占，无法实现资源合理分配，造成网络资源的浪费和维护管理的不便。因此，如何根据不同业务的通信需求，通过研究多业务隔离技术，建设统一的物理网络来承载多种电力通信业务成为电力终端接入网一个重要的研究方向。

1　电力无线专网现状及需求分析

1.1　电力无线专网现状

1.1.1　建设现状

截止 2014 年底，国家电网公司范围内建设无线通信基站 854 座，覆盖无线终端 24.6 万个。其中华东区域共有基站 381 座，覆盖无线终端 19.5 万个；华中区域共有基站 249 座，覆盖无线终端约 2.8 万个；华北区域共有基站 128 座，覆盖无线终端约 1.1 万个；东北区域共有基站 73 座，覆盖无线终端约 0.8 万个；西北区域共有基站 23 座，覆盖无线终端 0.5 万个。

国家电网公司范围无线专网技术体制包括 230 MHz 数传电台、McWiLL、WiMAX、TD-LTE 等。其中，无线电台共计基站 672 座（占比 86%），覆盖无线终端 23.6 万个（占比 96%）；McWiLL 共计基站 110 座（占比 14%），覆盖无线终端 0.4 万个（占比 4%）。

1.1.2　技术现状

长期以来，电力无线专网由业务部门根据自身需求建设，网络规模较小，业务支撑能力较弱，使用的技术体制包括 230 MHz 数传电台、WiMAX、McWiLL、TD-LTE 等。

（1）230 MHz 数传电台由于调制方式相对落后，相比于 3G、4G 等新型技术体制，频谱利用率太低；同时不支持终端数据并发，只能通过轮询的方式进行数据采集，降低了数据传输的灵活性与效率，造成故障信息等紧急数据无法及时上传等技术限制，规模呈萎缩状况。

（2）WiMAX 由于工作在 2~11 GHz 频段，其绕射能力和抗遮挡性较差，因此在配用电自动化系统中主要适用于地势相对平坦的开阔地区。为了在大中城市范围内应用，需要采取中继等方式实现 WiMAX 覆盖，建设成本相对较高。

（3）McWiLL 单基站（5 MHz）吞吐量最大达 15 Mbps，已在银川、沈阳、蓬莱等地的配用电示范项目中进行试点。考虑地形地貌与业务带宽需求，试点中市区普遍选用了 1 785~1 805 MHz 频段，但是在 1 800 MHz 频段需要保护 GSM 通信[1]，一般仅能在 1 785~1 800 MHz 频段获得授权。

（4）TD-LTE 在公司范围内网络主要采用 230 MHz 频段（占 86%）进行建设，但由于电力系统在 230 MHz 频段仅具备 1 M 带宽合法频点，难以承载视频等高宽带业务，且设备成本较高。中国南方电网公司于 2012 年 5 月投运的珠海 1.8 GHz LTE 电力无线专网系统[2]是目前全球规模最大的电力无线专网，覆盖 20 km^2，满足了配网自动化、计量、视频监控、应急等智能电网关键核心业务。在无线专网技术中应用前景较好。

1.1.3　业务承载能力

电力无线专网主要用于承载负荷控制、配电自动化、用电信息采集、调度信息等业务。其中，承载负荷控制业务的基站 631 座，覆盖无线终端 23.5 万个；承载配电自动化业务的基站 41 座，覆盖无线终端 1 509 个；承载用电信息采集业务的基站 38 座，覆盖无线终端 6 225 个；承载其他业务的基站 143 座，覆盖无线终端 2 816 个。

1.2　终端通信接入网业务需求分析

目前电力无线专网主要部署于电力终端通信接入网，承载负荷控制、配电自动化、用电信息采集、调度信息等业务，对其他业务的承载较少。

1.2.1　配电通信网业务

智能配电通信网主要承载配电自动化及配电变压器监测、电能质量监测、配电运行监控、分布

式电源控制、配电线路视频监控等业务，业务类型以数据业务为主，也包含少量视频业务。其中，配电自动化、电能质量监测、分布式电源接入业务位于生产控制大区，承载于调度数据网；配电线路视频监控业务位于管理大区，承载于综合数据网。

1.2.1.1　可靠性需求

配电设备及通信设备大多运行在户外，系统选用软硬件产品应经过行业认证机构检测，具有可靠的质量保证，能保障在恶劣天气下正常工作；同时能抵抗噪声、高电压、大电流、雷电等强电磁干扰，保持稳定运行；同时，需要保证高可靠性的信息传输通道，在电网线路故障或网络结构发生变化时不允许中断对配电设备的检测，要求配电通信系统不受线路故障和网络结构发生变化的影响。在设备层面，关键设备应冗余配置，单点故障不应引起系统功能丧失和数据丢失。

1.2.1.2　安全性需求

配电环节的业务处于生产控制大区中控制区（除配电线路视频监控外），直接服务于生产调度，对安全防护等级要求较高。按照相关安全防护标准，为了保证控制的安全可靠性，必须满足以下安全防护需求。

（1）技术选型方面：具备遥控功能的业务应优先采用专网通信方式，保证一次设备的安全运行；对于不具备电力光纤通信条件的末梢配电终端和只采集遥信、遥测的配电终端，可采用无线公网（TD-SCDMA、GPRS、CDMA 等，优先选择 TD-SCDMA）方式进行通信，公网通信必须采取 APN 和 VPN 等安全隔离、访问控制、认证加密等安全措施，配电网自动化系统主站与公网之间必须采取严格安全隔离措施，严禁将公网联入调度数据网及配网专用通信网络。

（2）加密认证方面：无论采用何种远程通信方式，配电网自动化系统应该支持基于非对称密钥技术的单向认证功能，主站下发的遥控命令应带有基于调度证书的数字签名，子站侧或终端侧应能够鉴别主站的数字签名。

（3）安全防护[3]方面：具备遥控功能的业务应优先采用专网通信方式，保证一次设备的安全运行；无线专网信息接入应符合相关安全防护规定的要求，并有严格的安全防护策略。

无线专网信息接入应符合国网公司相关安全防护规定的要求并有严格的安全防护策略，防止通过串接、公共网络等对子站、终端进行攻击，造成用户供电中断。防止通过公共网络和配电终端入侵主站，造成更大范围的安全风险；保障重要数据的机密性、完整性；针对系统进行安全审计，指导信息安全的运维与管理工作。

1.2.2　用电通信网业务安全性需求

营销用电业务主要包括用电信息采集、电动汽车充换电站、分布式电源与微网接入（200 kW以下）等，位于信息安全 III 区、IV 区。存在业务节点多、业务类别多样、流向集中、信息采集要求在预定时间点集中采集全部用户的数据信息的特点。

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，位于信息内网。电力用户用电信息采集系统通过横向隔离装置（反向）与生产控制大区通信；生产控制大区通过横向隔离装置（正向）与电力用户用电信息采集系统通信；无线公网采集的用电信息通过防火墙与电力用户用电信息采集系统通信。

用电信息采集系统主站部分单独组网，不同主站系统之间以及系统与公网信道之间，需要建立远程安全加密通道，并采用身份认证、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重安全功能，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以及防止内部网络信息等攻击。

1.3　多业务承载需求

1.3.1　业务隔离需求

配电通信网承载业务跨越生产控制大区和管理信息大区，通过“安全分区、网络专用、横向隔离、纵向认证”等方式保证不同安全大区业务的有效隔离。不同安全大区业务隔离划分如图 1 所示。

配电自动化业务（除配电线路视频监控业务以外）均位于生产控制大区，用电通信网业务均位于管理控制大区，不同大区之间业务的统一承载需要安装横向隔离装置。生产控制大区业务流向

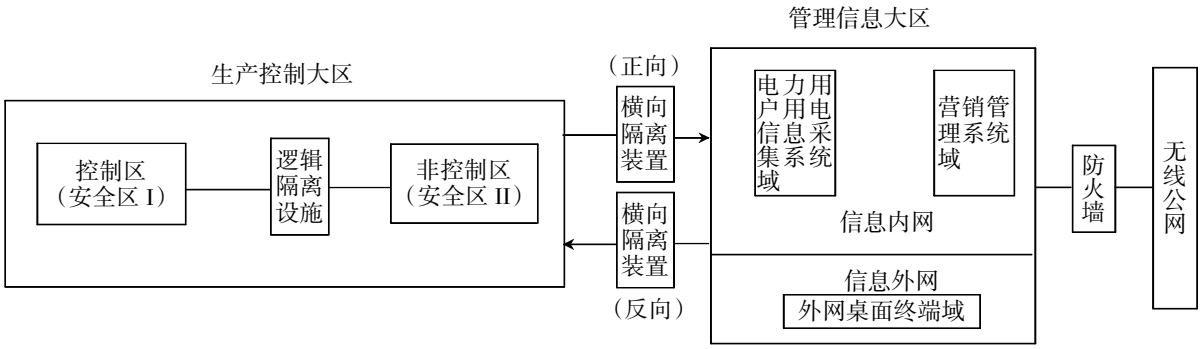

图 1　不同安全大区业务划分

管理信息大区时需要配置正向横向隔离装置，管理信息大区业务流向生产控制大区时需要配置反向横向隔离装置。在生产控制大区内部，根据业务实时性需求，分为控制区和非控制区，也即安全 I 区和安全 II 区，他们之间通过逻辑隔离装置进行隔离。在管理信息大区内容，电力用户用电信息采集系统位于信息内网，与公网之间通过防火墙连接。

因此，电力无线专网要实现多业务承载[4]必须解决不同大区业务之间的物理隔离，同一安全大区业务之间的逻辑隔离。

1.3.2　*无线专网承载需求*

配用电业务根据其功能属性，可分为控制类（遥控）、信息监测类（遥信、遥测）、视频类和市场营销类。不同属性业务的特性如表 1 所示。

表 1　配用电通信不同属性业务的特性

序号	业务属性	安全性要求	时延要求	路由要求	单点带宽要求/(Mbit·s^{-1})	通信失效对电网的影响
1	控制类	极高	秒级以下	严格	<0.01	严重
2	信息监测类	较高	数秒级	一般	<0.01	一般
3	视频类	较高	数秒级	一般	1~2	一般
4	市场营销类	高	数秒级	一般	<0.01	一般

无线专网可以用于承载各类配用电通信业务。当承载控制类业务时，对实时性、可靠性和安全性要求很高[5]，一般需要专用通道和高优先级的业务保证；当承载信息监测类业务时，对实时性、可靠性和安全性要求较高，一般仅次于控制类业务；当承载视频类业务时，对业务带宽有固定需求；当承载市场营销类业务时，对数据的安全性要求很高，实时性和可靠性要求相对较低。

2　电力无线专网多业务隔离方案设计

电力无线专网多业务隔离技术需要能够实现同一安全大区业务的逻辑隔离，不同安全大区业务的物理隔离。根据部署位置和功能的不同，电力无线专网包括无线终端、接入网和核心网 3 部分，因此可以从端口、基站、核心网 3 个层面进行业务隔离。

2.1　多业务隔离技术

2.1.1　*基于 RAN-SHARING 的多业务隔离技术*

基于 RAN-SHARING（无线接入网共享）技术的实现，包括基于二层 VPN 技术的虚拟网，基于频段或子载波划分的虚拟网两种。

（1）基于无线二层 VPN 技术的虚拟网业务隔离方案如图 2 所示。根据终端种类，将某一无线基站覆盖区域内相同业务类型的接入终端划分到一个 VLAN 内，不同 VLAN 的终端在无线接入时共享信道资源（包括 RRU 和 BBU），不为各种业务分配单独的专享信道。但是，根据业务实时性和传输带宽的要求，必须在 VLAN 之间设置接入优先级，同一个 VLAN 中的所有终端享有相同的接入优先级。

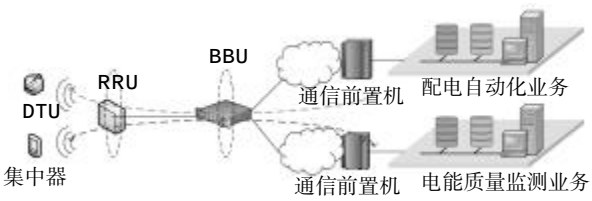

图 2　基于无线二层 VPN 技术的虚拟网业务隔离方案

基站接收到数据包后，解析终端的 IP 地址和所属的 VLAN，即可确定数据业务的类型。该方案在系统扩容增加新的接入终端时，不仅需要将新接入终端的地址重新添加进原有 VLAN 中，而且需要考虑是否逼近系统容量上限。该方案用于同一安全大区业务间的逻辑隔离。

(2)基于频段或子载波划分的虚拟网业务隔离方案如图 3 所示。在有限的频段内，将可以利用的子载波按照接入终端的种类、数量、数据传输的带宽要求等进行统计分析。在一个基站的覆盖范围内，固定分配若干个子载波给不同业务终端使用，各终端可以采用时分多址接入，也可以采用频分多址接入。由于子载波之间的正交性，使得尽管频谱叠加的子载波在传输信号时也不会产生干扰，因而能够保证所有传输不同业务子载波的逻辑隔离，并达到物理隔离效果。

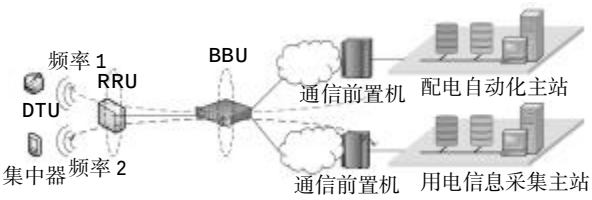

图 3　基于频段或子载波划分的虚拟网业务隔离方案

基站对收到的基带信号进行处理时，根据不同频率即可区分承载的业务数据类型，通过独立的业务板处理，并采用不同的物理端口将各类业务上传到相应大区的主站系统中。该方案可用于不同安全大区之间业务达到物理隔离效果。

2.1.2　基于物理隔离的无线多业务承载技术

对于分属于生产控制大区与管理信息大区的业务，考虑到安全性、实时性要求的差异，可以在同一区域内根据不同的终端接入类型，分别单独构建分属不同业务的无线专网，实现业务传输的物理隔离。每个基站仅承载一种类型的业务传输。采用不同基站组网时，要尽可能避免邻频率干扰，以提高系统容量和通信业务的传输质量。

2.2　基于多业务隔离技术的网络方案设计

现有的单一的业务隔离技术，均无法满足目前无线专网一网多用的隔离要求，基于配电自动化业务和用电信息采集业务的无线专网隔离方案设计目标是保证不同安全大区业务之间的隔离强度接近或达到物理隔离，并尽量保证通信资源的复用。方案设计中不仅需要解决终端侧物理隔离和核心侧物理隔离，同样需要综合解决无线空中传输物理隔离、基站侧物理隔离和 VPN 隔离技术等问题，各部分隔离思路如下。

2.2.1　无线终端接入侧

每类业务分别接入不同的 CPE 终端，由于每个终端只承载一种类型的业务，从而实现无线终端接入侧的物理隔离。

2.2.2　无线空中传输的物理隔离

为不同类型的业务划分不同的无线传输频段，安全 I、II 区终端接入使用频段 f_1，安全 III 区终端接入使用频段 f_2，f_1 与 f_2 不交叠。通过频谱和子载波间的保护间隔，确保不同安全区的业务在无线传输信道之间互不影响，实现无线空中接口传输的多业务物理隔离。

2.2.3　基站侧物理隔离

基站为所有接入的无线终端划分 VPN [6]或 APN，根据不同的 VPN/APN 标签，基站将射频端 RRU 收到的数据包处理后通过不同的上联 GE 端口发送到承载相应安全区业务的核心网设备。在基站内部，不同频段接收的业务数据在独立的业务板上进行处理，保证基站内流转的多业务数据流之间实现物理隔离。

2.2.4　VPN 隔离

从基站向上，通过交换机接入骨干传输网，通过采用 VPN 隔离（利用高安全可靠性的 IPSec 协议封装），为不同类型业务在骨干网上传输划分独立的逻辑通道，保证业务安全可靠地接入到核心网设备。

2.2.5　核心网设备物理隔离

根据不同安全区业务之间横向隔离的要求，在本系统中，I、II 区业务接入核心网设备 A，III 区业务接入核心网设备 B，每个核心网设备为各类业务指定不同的上联端口，送往不同安全区的应用服务器或者接入网关，实现同一设备（安全区 I 和 II）内不同业务的逻辑隔离。

以上设计思路，假设目前无线专网为最优的 TD-LTE，以目前接入的电能质量监测、配电自动化和用电信息采集 3 类业务接入为例，配电自动

化业务接入生产控制大区的控制区，即安全区 I；电能质量监测业务接入生产控制大区的非控制区，即安全区 II；安全区 I 与安全区 II 业务之间采用逻辑隔离。用电信息采集业务接入信息管理大区的安全区 III。业务隔离方案如图 4 所示。

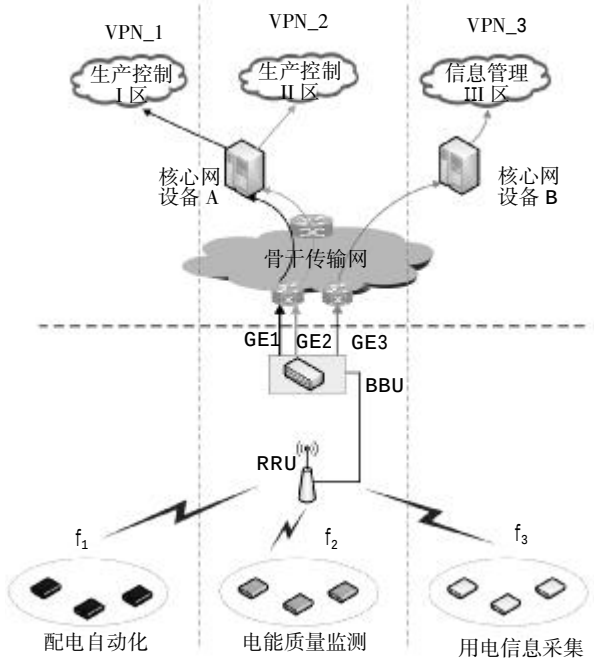

图 4　无线专网业务隔离方案

3　预期效果评价

TD-LTE 的 1.8 G 频段无线专网多业务承载网络已经于 2012 年分别在南网珠海和贵州遵义进行试点应用，网络建设初期未考虑多业务承载隔离问题。后续的无线专网建设过程中，如果能够在终端侧为每类业务接入不同 CPE 终端实现无线终端接入侧物理隔离，采用频谱和子载波间保护隔离实现无线空中接口传输的多业务物理隔离，通过划分 VPN 或 APN 保证基站内流转的多业务数据流之间实现物理隔离，利用高安全可靠性的 IPSec 协议封装的 VPN 隔离为不同业务划分逻辑通道，并根据不同安全区业务之间横向隔离的要求实现核心网设备物理隔离。将会实现从终端到主站整个无线通信网络的多业务安全隔离。整体网络真正实现一网多用。

4　结论

（1）本文针对配用电业务的无线专网业务隔离，结合无线终端接入侧隔离、VPN 隔离等 5 种隔离方式提出具体的网络模型，为无线专网的后期建设提出新的设计和应用标准。

（2）提出的业务隔离方案可以改善目前网络单一业务运用的项目投资格局，在综合部署一个网络的基础上可以解决多业务的承载和安全需要，大大节省网络建设成本，为建设一个低成本，广覆盖、高可靠性的数据通信提供了理论支撑。

（3）方案中的各种隔离技术均在已建网络中得到部分或组合应用，整体方案实用性较强。

参考文献：

[1] 王勇. MCWILL 无线宽带接入系统测试及其在中低压配电网通信中的应用[J].南方电网技术，2009,3-4.

[2] 仝杰.TD-LTE 构建电力无线宽带专网的探讨与实践[C]//电力通信管理暨智能电网通信技术论坛文集.北京：中国通信学会普及与教育工作委员会,2012,75-76.

[3] 尹晓华. 智能电网中无线宽带多业务支持策略研究[J].电力系统通信，2010,31(217):6-7.

[4] 詹翊春.分组化、高可靠的电力通信多业务承载网[J].电信技术，2012,(7):16-18.

[5] 王一蓉. 电力无线虚拟专网组网架构及 IP 地址分配研究[J].电力信息与通信技术，2014,12(6):16-21.

[6] 王妍.基于 IPSec 的 VPN 系统设计与实现[D].成都：电子科技大学，2013.

什么是应用研究

应用研究是把基础研究发现的新知识、新理论用于特定目标的研究，产生新方法、新方案和建立新标准等。它是基础研究与开发研究之间的桥梁。基础研究获取的知识必须经过应用研究才能发展为实际运用的形式。