交换机端口安全策略在智能变电站中的应用研究

高吉普[1]，徐长宝[1]，戴 宇[1]，吴 杰[2]，张道农[3]

（1.贵州电力试验研究院，贵州 贵阳 550002；2.南京悠阔电气有限公司，江苏 南京 211100；
3.华北电力设计院，北京 100000）

摘要：为了保证智能变电站通讯网络运行的稳定性和安全性，提出了智能变电站通讯网络端口接入控制的安全策略。介绍了智能变电站的通讯方式和网络结构，分析了智能变电站存在的安全隐患和交换机的端口安全接入控制需求。解释了基于静态 MAC 地址的端口安全的工作原理和技术特点，阐述了基于 IEEE802.1X 协议的端口安全的组网方式、工作原理、认证过程和技术特点，总结了现阶段智能变电站端口安全策略的具体应用模式和实施方案。最后得出结论，现阶段采用静态 MAC 地址和 IEEE802.1X 相结合的方式进行交换机的端口安全接入控制可以兼顾有效性和可行性，具有实用价值。

关键词：智能变电站；交换机；端口安全；端口接入控制；静态 MAC；IEEE802.1X

Research on application of switch port access control in smart substation

GAO Ji-pu[1], XU Chang-bao[1], DAI Yu[1], WU Jie[2], ZHANG Dao-nong[3]

(1. Guizhou Electric Power Research Institute, Guiyang 550002, China;
2. Nanjing Youkuo Electric Co., Ltd, Nanjing 211100, China;
3. Huabei Electric Designation Institute, Beijing 100000, China)

Abstract: To ensure the stability and security of the communication network of the smart substation, the switch port access control strategy of the communication network in the smart substation is put forward. The smart substation communication mode and network structure are introduced, the potential safety hazard and the switch port access control requirements of smart substation are analyzed. The theory and technical characteristics of the port security based on static MAC address are explained, and the networking mode, theory, authentication process and technical characteristics of the port security based on IEEE802.1X protocol are elaborated. The application cases and implementation schemes of port security strategy during the present time in smart substation are concluded. In conclusion, to control the switch port security of the smart substation, the strategy combining with the static MAC address and IEEE802.1X protocol is valid, feasible and practical at present.

Key words: smart substation; switch; port security; port access control; static MAC; IEEE802.1X

中图分类号： TM764 文献标识码：A 文章编号： 1674-3415(2014)13-0117-06

0 引言

网络安全问题一直是伴随着网络技术发展而存在的一个问题，在互联网、银行、教育等诸多领域都已经有了广泛的重视和共识，在国外电力系统中也早有相关规范和应用研究。国内在智能变电站出现以前，由于二次设备对网络通信依赖度较小，变电站内通信网络安全问题一直未引起足够的关注。

随着网络通讯技术、微电子技术的发展，国内智能变电站建设发展迅速，逐渐成为综合自动化变电站的发展方向。在智能变电站中，以交换机为核心的通讯网络的重要性已经远远超过传统综合自动化变电站，网络的可靠性和安全性直接决定着站内设备的监控、模拟量和开关量的采集、保护跳闸命令的传输等各个方面[1]。

因此，关注和重视智能变电站内整个通讯网络的稳定性和安全性[2]，研究适应于智能变电站内部的安全应用模式十分必要。智能变电站内部的网络安全，主要涉及到站内交换机的端口安全（即端口接入控制，Port Access Control），本文将详细讨论智能变电站中交换机端口安全策略的基本原理和应用模式。

1 智能变电站网络安全分析

1.1 智能变电站的网络架构

目前智能变电站设备一般分为站控层、间隔层、过程层设备，通讯网络一般分为站控层和间隔层之间的 MMS 网(称为站控层网络)、间隔层和过程层之间 GOOSE 和 SV 网(统称为过程层网络)[3]，如图 1 所示。根据应用的电压等级不同，上述三种网络组网方式有所不同[4]，目前应用较多的是 MMS 网、GOOSE 网和 SV 网分别单独组网[5]，在一些较低电压等级的变电站中也有 GOOSE 网和 SV 网共网[6]，或 GOOSE 网和 MMS 共网，或 GOOSE、SV 和 MMS 三网合一的情况。

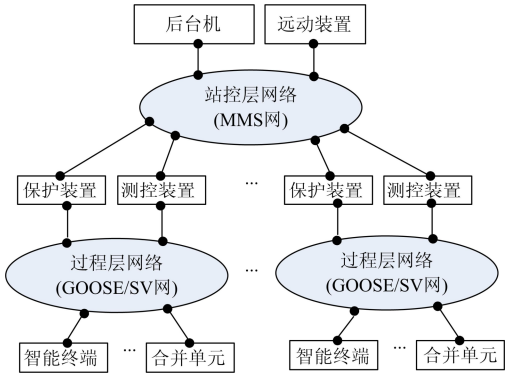

图 1 智能变电站网络架构

Fig. 1 Network structure of smart substation

MMS 网用于站控层设备和间隔层设备的信息交换，主要是对间隔层设备的监视和控制信息，可靠性的要求相对较低，但数据量相对较大[7]。

GOOSE 网主要用于传输保护跳闸命令、过程层设备之间的联闭锁信息和开关刀闸位置等开关量信息，GOOSE 网正常信息量较小，但当保护动作时有突发流量。因 GOOSE 直接传递跳闸命令，其可靠性不言而喻，GOOSE 本身的设计机制中已经通过多次发送等方式尽量保证其可靠性。同时，GOOSE 是一种实时应用[8]，根据 IEC61850 标准的规定，GOOSE 信号的通信延迟应小于 4 ms，在现实应用中，保证 GOOSE 正确可靠的前提下，应在发送端、交换机、接收端尽可能地提高实时性，以便缩短故障切除时间。

SV 网用于传输电子式互感器所采集的模拟量，SV 网信息数据量庞大，目前保护用的 SV 采样频率一般为每秒 4 000 点，电能质量装置用的 SV 采样频率更高。由于 SV 数据直接决定保护的动作行为，所以其传输的可靠性、实时性要求同样很高[8]，根据 IEC61850 标准的规定，SV 数据的通信延迟也应小于 4 ms。

鉴于 GOOSE 和 SV 报文的以上特点，必须保证交换机端口安全策略在实施过程中不影响其实时性和可靠性，尽量做到在端口安全接入控制的过程中，完全不影响交换机的吞吐量、延时等交换行为。

1.2 智能变电站对交换机端口安全策略的需求

智能变电站网络属于局域网范畴，局域网安全建设一般在等级防护、积极防御与综合防范的安全策略下进行，建设内容包括安全域的划分、应用区域边界安全、终端接入控制等。对于安全域划分和应用区域边界安全，《电力二次系统安全防护规定》（电监会 5 号令）中已经有了明确规定，但是在终端接入控制方面，并没有相关的规定和应用研究。

智能变电站中，由于有过程层网络的存在，跳闸命令、开关信号、采样值信息的传输将直接影响保护逻辑和故障跳闸，网络安全控制则更应加强。

在智能变电站网络条件下，潜在的危害主要有以下几种可能：

（1）专业攻击型。非法专业用户接入网络后，通过监听、截取、伪造信息等方式蓄意破坏智能变电站的运行，可以进行任何监视和控制操作。

（2）主动破坏型。非法用户接入网络后，向网络输入大量广播或多播无用报文，这种报文不仅占用网络带宽，而且如果输入报文量较大，会对所有装置都造成冲击，使装置网口异常，甚至出现死机、无法启动等，使整个网络瘫痪。

（3）无意识危害型。非专业用户接入网络，由于误操作或无意中通过广播报文等方式占用带宽，对设备的正常运行造成影响，致使装置异常，等发现问题时造成的危害已无法挽回。

综上所述，需要对智能变电站交换机进行端口接入控制，以便对接入网络的设备和使用接入设备的人员进行安全管理。

目前比较适合在智能变电站中使用的端口安全策略有两种，即基于静态 MAC 的端口安全和基于 IEEE802.1X（以下简称 802.1X）协议的端口安全。

2 基于静态 MAC 的端口安全

2.1 交换机基本原理

以太网交换机工作于 OSI 七层协议通讯模型的第二层（数据链路层），为上层协议提供服务，对上层协议透明，其交换功能的工作原理简介如下：

（1）交换机根据收到数据帧中的源 MAC 地址建立该地址同交换机端口的映射关系，并将其写入内部 MAC 地址表中，此过程称为 MAC 地址“学

习”，通过在数据帧的始发者和目标接收者之间建立临时的交换路径，使数据帧直接由源端口到达目的端口。

（2）交换机以收到的数据帧中的目的 MAC 地址查找已建立的 MAC 地址表，以决定该数据帧向哪个端口进行转发。

（3）如在已建立的 MAC 地址表中未找到数据帧中的目的 MAC 地址，则该数据帧向所有端口转发。这一过程称为泛洪（flood）。

（4）广播帧和多播帧在未经特殊控制的情况下向所有端口转发。

2.2 基于静态 MAC 的端口安全实现过程

交换机采用基于静态 MAC 的端口安全策略时，主要行为如下：

（1）该端口不再自动“学习”数据帧的源 MAC 地址；

（2）对源 MAC 地址未包含在 MAC 地址表中的数据包做丢弃处理。

这样，可以将要接入的合法装置的 MAC 地址和将要接入端口号的对应关系预先设置到交换机的 MAC 地址表中，就可以实现交换机的某端口只允许预先设定的一个或多个装置接入控制。

2.3 技术特点

基于静态 MAC 地址的端口安全有以下特点：

（1）原理简单、运行可靠。预先配置好后，后续工作过程无需 CPU 参与，芯片自动完成。

（2）配置工作只在交换机上进行，不需要终端装置中运行客户端程序支持，整个应用过程对终端装置无任何影响。

（3）如果有新装置欲接入网络时，或原有装置需要更改在交换机网络上的接入位置时，需要更改相应交换机的配置。

3　基于 802.1X 的端口安全

3.1 采用 802.1X 认证的网络结构

802.1X 是一种基于端口的认证协议，其认证的最终目的就是确定一个端口是否授权[9]。对于一个端口，如果认证成功那么就“开放”这个端口，允许所有的报文通过；如果认证不成功就使这个端口保持“关闭”，只允许 802.1X 认证协议报文通过。

802.1X 的体系结构中包括三个部分，如图 2 所示。

1）请求者系统。请求者是支持 802.1X 认证的用户终端设备。请求者和认证系统之间运行 802.1X 定义的 EAPOL(Extensible Authentication Protocol Over LAN，基于局域网的扩展认证协议)。

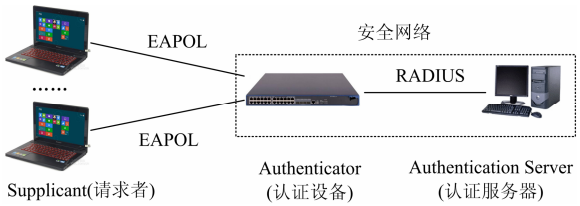

图 2　802.1X 认证网络结构

Fig. 2 Authentication network of 802.1X

2）认证系统。认证系统为支持 802.1X 协议的网络设备（如以太网交换机），它为请求者提供服务端口，实现 802.1X 认证，控制请求者的接入。

3）认证服务器系统。认证服务器是为认证系统提供认证服务的实体，来实现认证服务器的认证和授权功能，所有合法用户的用户名和口令等信息统一在认证服务器上管理。本文以常用的 RADIUS（Remote Authentication Dial In User Service，远程用户拨号认证系统）服务器为例进行说明。

3.2 小型网络时的简化网络结构

目前，多数管理型交换机支持 802.1X 功能的同时[10]，又支持充当 RADIUS 服务器功能[11]。在小型网络中，可以不配置单独的认证服务器。实施过程如下：

（1）选择网络中一台交换机（一般选中心交换机）同时开启 802.1X 功能和 RADIUS 服务器功能；

（2）该网络的所有合法用户信息统一在该交换机上配置；

（3）直接接入该交换机的终端装置认证时，RADIUS 协议认证过程在本交换机内完成；

（4）接入其他交换机的终端设备认证时，向该交换机完成 RADIUS 远程认证。

这样，可以简化网络结构，节约成本，不需要在交换机网络上引入单独的 RADIUS 服务器，非常适合小型网络中使用。智能变电站的 GOOSE 网和 SV 网认证时可以采用该种简化组网方式。

3.3 802.1X 的工作原理

如图 3 所示，认证系统（交换机）的每个物理端口内部逻辑上划分成受控端口和非受控端口。非受控端口始终处于双向连通状态，主要用来传递 EAPOL 协议帧，可随时保证接收认证请求者发出的 EAPOL 认证报文；受控端口缺省为“非授权”状态，不提供数据交换服务，只有在认证成功的状态下才“授权”，才可以交互数据。

在客户端 PAE(Port Access Entity，端口访问实

体)与交换机的 PAE 之间，协议报文使用 EAPOL 封装格式，直接承载于 LAN（Local Area Network，局域网）环境中。由于其报文格式是二层报文，无 IP 封装层，不可以穿越路由器等三层以上设备。

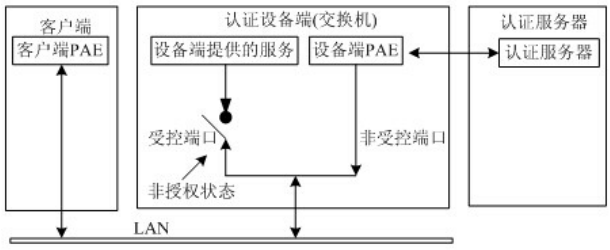

图 3 802.1X 认证体系结构

Fig. 3 Authentication system structure of 802.1X

在交换机 PAE 与认证服务器之间，认证协议采用 RADIUS 协议等基于 UDP 或 TCP 的高层认证协议，可以穿越路由器和广域网络。因此认证服务器可以部署在本地，也可以部署在远端广域网络中。

3.4 802.1X 的认证过程

802.1X 认证过程如图 4 所示。

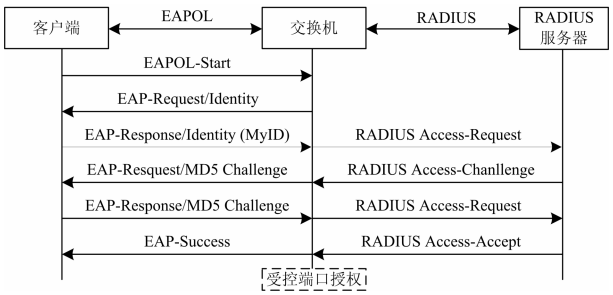

图 4 802.1X 认证过程

Fig. 4 Process of 802.1X authentication

（1）当终端有接入需求时启动 802.1X 客户端，输入合法的用户名和口令，发起连接请求（EAPOL-Start），开始一次认证过程。

（2）交换机收到请求认证的数据帧后，发出一个请求帧（EAP-Request/Identity）要求客户端程序发送用户名。

（3）客户端程序将用户名信息通过数据帧（EAP-Response/Identity）发送给交换机。交换机将客户端送上来的数据帧经过封包处理后（RADIUS Access-Request）发送给 RADIUS 服务器。

（4）RADIUS 服务器收到交换机转发的用户名信息后，将该信息与数据库中的用户名表相比对，找到该用户名对应的口令信息，用随机生成的一个加密字对它进行加密处理，同时也将此加密字通过报文(RADIUS Access-Challenge)传送给交换机，并由交换机继续传给（EAP-Request/MD5 Challenge）客户端程序。

（5）客户端程序收到由交换机传来的加密字后，用该加密字对口令部分进行加密（如 MD5 算法）处理，然后传给（EAP-Response/MD5 Challenge）交换机，交换机封装以后（RADIUS Access-Request）传给 RADIUS 服务器。

（6）RADIUS 服务器将收到的加密后的口令信息和自己经过加密运算后的口令信息进行对比，如果相同，则认为该用户为合法用户，反馈认证成功信息（RADIUS Access-Accept）给交换机，此时交换机将受控端口授权，开放端口数据交换功能，然后再发信息（EAP-Success）告知客户端认证成功，整个认证过程完成。

认证成功后交换机仍会定时向客户端要求重新认证，以便保证用户一直合法。客户端也可以主动发送报文给交换机，终止已认证状态，则交换机会将端口状态从授权状态改变成非授权状态。

3.5 802.1X 认证的技术特点

基于 802.1X 的端口安全有以下特点：

（1）简洁高效。按网络分层模型，802.1X 协议为二层协议，在链路层进行认证，去除了多层封装等不必要的开销和冗余，收发迅速，对用户的透明性好。

（2）安全可靠。所有认证过程中口令采用密文传输，保证安全性；认证报文和业务报文完全分离，认证后对业务报文传输再无影响，完全透明传输。这样，在智能变电站中，所有应用协议的实现均可不变，不需考虑 802.1X 认证过程。

（3）通用性好。Windows 操作系统内集成了 802.1X 客户端，Linux 系统上也有开源的客户端组件。

（4）保证吞吐量。802.1X 采取一种“认证后不管”的方式，在认证完成后，交换机对网络流量不做过多的干预，兼顾了安全性和网络的吞吐量两个方面。

（5）应用灵活。终端可以用户名和口令在网络的任何边缘口接入，终端也可以灵活更换。如有需要，可以与静态 MAC 绑定结合使用。

4 智能变电站端口安全应用模式

4.1 端口安全控制范围分析

智能变电站通讯网络普遍采用星形网络，网络建成以后，其内部的交换机端口按用途可分为边缘端口和级联端口。边缘端口用于接入保护、测控等终端装置，需要进行安全接入控制；级联端口用于连接其他交换机，组成该网络“主干”部分，该部

分属于安全网络，安全网络本身的安全性超出了本文讨论范围。如一旦星形网络内级联端口被断开，即安全网络内部遭到破坏，则该网络会解列成不同的物理网，监控系统中马上会报出大量装置的通讯中断等异常信号，站内监控系统和各级调度系统会立刻发现，这种对安全网络的直接破坏不属于端口接入控制的防范范围。因此，智能变电站通讯网络的安全接入控制，只需要在网络的边缘端口实施。

4.2 现阶段端口安全应用模式分析和选择

端口安全应用模式的选择主要考虑以下几个方面：

1）控制范围

基于 802.1X 的端口安全本身就是针对边缘端口控制设计的；基于静态 MAC 的端口安全可以控制边缘端口和级联端口，但如果只控制边缘端口，会减小很多配置工作量。总之，应用二者均可以满足控制网络边缘端口接入的需求。

2）对网络实时性、可靠性的影响

从其控制原理出发，基于静态 MAC 或 802.1X 的端口安全都不影响所传输报文的实时性和可靠性，完全不影响交换机的吞吐量、延时等交换行为，均可以在智能变电站中应用。

3）在各种组网方式的应用分析

端口安全控制在不同物理网之间互不干涉。

在同一物理网中，交换机之间的级联方式的调整都在安全网络的范围内，不属于边缘端口，所以端口安全可以不考虑组网方式调整的影响。况且，由于可靠性等因素，智能变电站内的网络一般均采用星形网络。

至于在应用层面的组网方式划分，如该网络是 SV 网、GOOSE 网、MMS 网或是几种应用网络的融合，与网络的端口安全接入控制更无关系。

4）现阶段应用条件限制

鉴于当前智能变电站建设和运行状况，单独使用基于静态 MAC 或者 802.1X 的端口安全都有不妥之处，具体如下：

（1）使用基于静态 MAC 的端口安全所有需接入装置必须预先确定。当后续维护过程中设备厂商需要接入调试笔记本时必须先修改交换机的配置，增加调试笔记本的静态 MAC，维护完成后还要删除对应的静态 MAC，将交换机配置恢复原样，流程繁琐，且经常修改交换机的配置存在安全隐患。

（2）使用基于 802.1X 的端口安全需要终端设备中含有 802.1X 客户端，及支持 EAPOL 协议。目前，一般 PC 机、工控机、服务器上都支持 802.1X 客户端或者有对应的商用软件，而嵌入式装置（如保护、测控、合并单元、智能终端）中基本都不支持 802.1X 客户端，需要重新开发，而各厂商从开发到广泛使用 EAPOL 协议需要一个较长的过程。

5）现阶段综合解决方案

在现阶段，为兼顾有效性和可行性，可以将基于静态 MAC 或者 802.1X 的端口安全结合使用，分别用于嵌入式装置和非嵌入式装置，这是现有条件下较好的选择，具体应用方案如下：

（1）交换机端口安全只在整个安全网络的边缘端口进行接入控制，如图 5 所示。

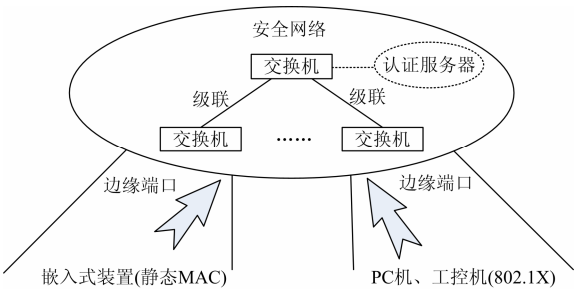

图 5 智能变电站端口接入控制方式

Fig. 5 Port access control mode in smart substation

（2）认证服务器接口和交换机级联口必须属于安全网络的一部分，设计时指定端口，不需要进行端口安全控制。认证服务器上预先管理好合法用户的用户名和口令。

（3）间隔层网络和过程层网络中的嵌入式终端（如保护、测控、合并单元、智能终端）采用静态 MAC 方式接入网络。采用静态 MAC 对终端装置无任何影响，也不需终端装置上客户端配合，而且这些装置在变电站网络设计时已指定端口，MAC 地址、数量、接入位置都是确定的，交换机配置好以后，后续维护过程中配置不需再改变。

（4）调试工程师的个人电脑或工控机等支持 802.1X 客户端的终端通过 802.1X 认证协议接入网络。这些装置的个数和 MAC 地址不能确定，连接位置也不能确定，当确定有合法用户需要接入时，只需输入预先在认证服务器上管理的户名和口令即可接入，无需更改交换机配置。

4.3 站控层和过程层网络 RAIDUS 服务器部署

站控层和过程层网络在端口安全接入控制时可以采用相同策略，但部署 RADIUS 服务器时可以根据网络规模和网络特点有所区别。

站控层网络规模相对较大，且必须有后台机接入，可以考虑用后台机充当 RADIUS 服务器，这样管理起来比较方便，也不会增加新的投资。

过程层网络通常分成多个独立的物理网络，每

个网络规模较小，而且不连到后台机，如果每个网络引入单独 RADIUS 服务器，则增加成本太多。因此，可以考虑采用本文 3.2 节中所讲的简化网络结构，用过程层网络内的中心交换机作为 RADIUS 服务器。这样，现有的组网方式就不需任何变化，而且可以省去若干台服务器的成本。

5 总结与展望

网络安全问题直接关系到智能变电站的运行安全，随着智能变电站技术的不断发展和进步，智能变电站内网络安全问题需要进一步重视。现阶段，采用静态 MAC 和 802.1X 相结合的方式进行交换机的端口安全接入控制可以兼顾有效性和可行性，同时不影响所传输报文的实时性和可靠性，在今后一段时间内必然有很大的应用空间。

参考文献

[1] 张清枝, 魏勇, 赵成功. 变电站网络化二次系统关键技术研究及应用[J]. 电力系统保护与控制, 2009, 37(8): 47-52.
ZHANG Qing-zhi, WEI Yong, ZHAO Cheng-gong. Research and application on key technologies of power secondary system in substation based on network[J]. Power System Protection and Control, 2009, 37(8): 47-52.

[2] 汪强. 基于IEC61850的光纤工业以太网交换机的设计及应用[J]. 电力系统保护与控制, 2010, 38(13): 113-115.
WANG Qiang. Design and application of fiber industrial ethernet switch based on IEC61850[J]. Power System Protection and Control, 2010, 38(13): 113-115.

[3] 李孟超, 王允平, 李献伟, 等. 智能变电站及技术特点分析[J]. 电力系统保护与控制, 2010, 38(18): 59-62.
LI Meng-chao, WANG Yun-ping, LI Xian-wei, et al. Smart substation and technical characteristics analysis[J]. Power System Protection and Control, 2010, 38(18): 59-62.

[4] 朱炳铨, 王松, 李慧. 基于IEC 61850 GOOSE技术的继电保护工程应用[J]. 电力系统自动化, 2009, 33(8): 104-107.
ZHU Bing-quan, WANG Song, LI Hui. Application of IEC 61850 GOOSE technology on protective relaying[J]. Automation of Electric Power Systems, 2009, 33(8): 104-107.

[5] 徐成斌, 孙一民. 数字化变电站过程层GOOSE通信方案[J]. 电力系统自动化, 2007, 31(19): 91-94.
XU Cheng-bin, SUN Yi-min. A communication solution of process layer GOOSE in digitized substation[J]. Automation of Electric Power Systems, 2007, 31(19): 91-94.

[6] 邱智勇, 陈建民. 500 kV 数字化变电站组网方式及VLAN 划分探讨[J]. 电工电能新技术, 2009, 28(4): 60-65.
QIU Zhi-yong, CHEN Jian-min. Discussion of 500 kV digital substation network mode and VLAN partition[J]. Advanced Technology of Electrical Engineering and Energy, 2009, 28(4): 60-65.

[7] 王松, 陆承宇. 数字化变电站继电保护的GOOSE网络方案[J]. 电力系统自动化, 2009, 33(3): 51-54.
WANG Song, LU Cheng-yu. A GOOSE network scheme for relay protection in digitized substations[J]. Automation of Electric Power Systems, 2009, 33(3): 51-54.

[8] 魏勇, 罗思需, 施迪, 等. 基于 IEC61850-9-2 及GOOSE 共网传输的数字化变电站技术应用与分析[J]. 电力系统保护与控制, 2010, 38(24): 146-152.
WEI Yong, LUO Si-xu, SHI Di, et al. Research and application on digital substation based on IEC61850-9-2 and GOOSE communication in one network[J]. Power System Protection and Control, 2010, 38(24): 146-152.

[9] 窦晓波, 胡敏强, 吴在军. 数字化变电站通信网络性能仿真分析[J]. 电网技术, 2008, 32(17): 98-104.
DOU Xiao-bo, HU Min-qiang, WU Zai-jun. Simulation analysis on performance of communication networks in digital substations[J]. Power System Technology, 2008, 32(17): 98-104.

[10] 王文龙, 杨贵, 刘明慧, 智能变电站过程层用交换机的研制[J]. 电力系统自动化, 2011, 35(18): 72-76.
WANG Wen-long, YANG Gui, LIU Ming-hui. Development of the switch used in process level of smart substation[J]. Automation of Electric Power Systems, 2011, 35(18): 72-76.

[11] 802.1X IEEE standard for local and metropolitan area networks port-based network access control[J]. IEEE Computer Society, 2010.

收稿日期：2013-09-30； 修回日期：2013-12-26

作者简介：

高吉普（1982-），男，硕士，工程师，研究方向为智能化变电站和智能电网相关研究；E-mail: jipugao@sina.com

徐长宝（1977-），男，工学硕士，高级工程师，从事数字化变电站技术研究；

戴 宇（1958-），男，本科，高级工程师，从事变电站二次和智能变电站相关研究。