数字化变电站中信息处理及网络信息安全分析

吴国威
(浙江大学电气工程学院，浙江 杭州 310027)

摘要：通信网络是数字化变电站的重要组成部分，尤其过程总线取代传统的硬接线，使得网络系统从二次延伸到了一次，大幅度增加了网络规模和网络流量；过程总线上传输的信息绝大多数要求有严格的实时性和高度的可靠性，因此，信息安全问题是威胁变电站安全、稳定、经济、优质运行的重大问题，需要引起足够重视。介绍了信息需求分类、信息合并等提高信息实时性的方法，提出将信息加密技术、防火墙技术、mobile agent、安全管理技术和虚拟专网（VPN）技术等网络安全技术应用于数字化变电站，并分析了具体应用方案及效果。

关键词：数字化变电站； 网络安全； 防火墙； mobile agent； VPN

Information disposal and network security analysis in digital substation

WU Guo-wei
(Zhejiang University, Hangzhou 310027, China)

Abstract: Communication network plays an important role in digital substation.With the process bus instead of the traditional hard connection,substation network extends from the secondary system to primal system and the network scale and its flux increases greatly,which requires most of the information transmission real-time and with reliability,so the information security becomes more important for the secure,stable,economic and superior operation of substation.This paper introduces the method of the classification of information in order to increase its punctunality in substation. In the light of the computer network structure in substation some security strategies and measures are proposed and various techniques are described such as the firewall,mobile agent,virtual private network and data encryption algorithm and analyzes its effect.

Key words: digital substation; network security; firewall; mobile agent; VPN

中图分类号： TM764 文献标识码： A 文章编号： 1003-4897(2007)12-0018-05

0 引言

根据国家电网公司规划，2007年在无锡110 kV苑石变电站示范应用数字化变电站，2009年在铜陵220 kV南郊变电站示范应用，2009年吉林公司安排500 kV电子式互感器示范应用；“十一五”后期开展500 kV数字化变电站示范应用。随着IEC 61850标准的正式颁布，以及国内外生产厂家、高校院所等的共同努力，数字化变电站逐渐进入实用化阶段。

数字化变电站中，除了常规的变电站监视、控制、保护、故障录波、量测等功能通过网络实现外，模拟量采集、电气设备状态监测、故障诊断、操作命令的下达和执行等都是通过过程总线实现的，使得信息的采集、传输、处理模式产生了根本性的变化，网络的作用和网络流量之多都是空前的（在过程总线、站级总线合二为一的情况下尤其突出），研究合理的信息需求分类、网络结构、信息合并等方法以保障信息的实时性迫在眉睫。

随着国家电力数据专用网SPDnet (State Power Data network)建设的深入，特别是远动系统网络化进程的加快，接入数据网络的电力控制系统越来越多，在电网调度中心、变电站之间进行的数据交换也越来越多。从内部来看，大量的远方控制，对电力控制系统和数据网络的安全性、可靠性、实时性提出了新的严峻挑战。从外部来看，随着Internet技术的广泛使用，以网络为主要传播途径的病毒和黑客也日益猖獗。变电站计算机网络安全问题的重要性日益突出。

本文基于数字化变电站的特点，提出了信息需求分类、信息合并等提高信息实时性的方法，以及几种针对性的网络信息安全技术。

1 过程层

常规变电站中，一次电气设备和二次装置之间的信息交互还是依靠强电控制、模拟信号传送和硬节点输入，开关场一次电气设备和控制室二次装置

之间需要敷设大量的二次电缆，施工、维护工作量很大；一次电气设备模拟信号和硬节点信号的数字化处理还是依靠二次装置来完成，无法做到一次电气设备和二次装置之间的电气隔离。

根据 IEC61850 标准体系的描述，数字化变电站可分为三层：站控层、间隔层、过程层。

过程层功能分为三类：电力运行的实时电气量测量、运行设备的状态参数检测、操作控制执行与驱动。过程层很多功能从间隔层独立出来，是一种趋势。长期以来，国内外一、二次系统厂家相对独立，是过程层进展缓慢的一个主要原因。

过程层与间隔层之间的硬接线连接将被基于交换式以太网的通信网络所代替，这种通信方式又称作过程总线通信。过程总线成功地解决了一次电气设备和二次装置之间的电气隔离，并节省了电缆，减轻了施工、维护工作量。

采样测量值和跳闸命令是过程总线上数据通信最为重要的两类信息。IEC61850 标准定义了两种抽象模型：采样值传输(SAV)模型和通用的以对象为中心的变电站事件(GOOSE)模型。其中 SAV 模型应用于采样值传输及相关服务，而 GOOSE 模型则提供了变电站事件(如命令、告警等)快速传输的机制，可用于跳闸和故障录波启动等。

此外，变电站电气设备状态监视系统技术发展迅速，作为保障电网安全运行的第一道防御系统的关键技术之一，已经成为智能化设备的不可分离的组成部分，它同时也加大了系统网络的流量。

过程总线、站级总线合二为一[1]，如图 1 所示，IED 只需一套以太网接口，简化了结构，降低了设备和维护费用。但是，带来的第一个问题是实时数据和非实时数据、控制性数据和非控制性数据共享同一网络，易导致网络资源争用以及安全性问题。

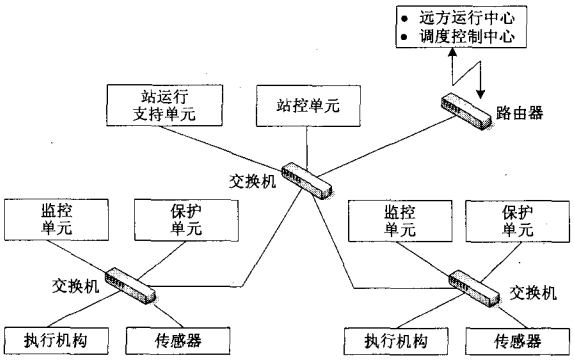

图1 合并总线

Fig.1　Merged station and procession bus

带来的第二个问题是，以前靠硬接线的跳、合闸控制，几乎是无延时的、直观可靠的。实时保护、测控功能高度依赖于模拟量的实时采集。现在模拟量采集、跳合闸依靠通信网络，如果由于网络的安全性、实时性原因引起误动、拒动，后果不堪设想。

2　信息处理

2.1 变电站的信息需求

基于IEC 61850的变电站自动化为三层结构模型，其信息传输时间需求如表1所示。表1中的信息传输时间需求详见参考文献[2]，该文献是由IEEE电力工程委员会变电站分会基于IEC 61850标准，组织编写的集成一体化变电站通信需求的技术报告。

表1 通过变电站通信接口的信息传输时间需求

Tab.1 Time requirements of information transmission across substation communication interfaces

信息流	时间需求	信息传输时间/ms
站控单元－保护单元	低	>100
保护单元间的动作信息传输	高	2-10
保护单元间的数据传输	中	10-100
测控单元－保护单元	中	10-100
同步相量测量信息	中	10-100
测控单元－开关设备	低	100-250
站控单元－控制单元	低	100-250
站控单元－技术服务中心	低	>100
测控单元之间	中	10-100
站控单元－控制中心	低	>100
保护单元－开关设备	很高	<2
CT/PT－各单元的采样信息	很高	<2

由表1可知，过程总线上的电流、电压互感器与保护、测控单元之间的实时电压电流采样值和保护单元发送到现场开关设备的保护信号的信息传输时间需求最紧急，信息传输时间小于2 ms；同步相量测量信息的传输时间可以大于10 ms。保护单元之间的保护动作信息具有较高的传输速率，通常信息传输时间为2～10 ms，而站控单元－技术服务中心间的数据文件传输时间可以大于100 ms。

通过对信息需求的分析，不仅可以为电力系统通信设计、规划提供一个参考标准，而且能够为电力信息系统的网络性能管理方案实施提供依据。

2.2 实时性保证方法

实时性，即严格时限要求规定，在特定的时间内完成特定的任务，如测量、保护、控制、事件记录的报文传输，确保极坏情况下，报文响应时间是可确定性的。

2.2.1 优先级设定

数据有轻重缓急之分，重要的数据须优先于其

它数据传输。要求支持优先级调度以提高时间紧迫性任务的信息传输可确定性。

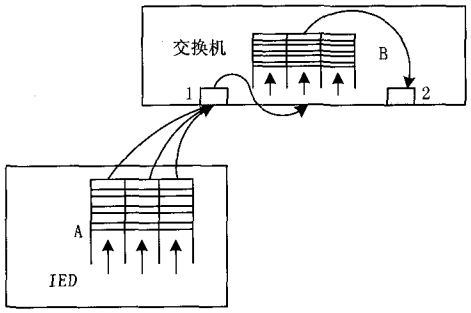

图2 报文传输优先级

Fig.2 Messages transfer priority

如图2示,报文传输优先级实质有两层含义，它包括设备自身内部的数据优先级队列A 和网络交换机内的数据优先级队列B。设备内部的数据优先级在协议的设计中考虑保证紧要报文优先发出去，报文到达交换机后当多个报文要同时传到一个节点时也存在报文的优先级处理，即在队列B中。目前，大部分交换机都支持报文的优先级传输。

2.2.2.信息合并原则

为减少网络信息及接点容量，监控系统内同一设备的意义相同的接点信号可合并发一个信号。因此，必须确定信息合并的原则，信息合并不能影响对基本结论性事件的判断，对于内涵一致，外延小于其它信号时不能合并；若信号性质相同，仅反映所发出的位置不同可以考虑合并。

如“保护装置异常”和“保护装置闭锁”信号，由于其涵盖内容多，性质不一样，不宜合并；

对于保护同一设备的两套保护装置，其传送到地调相同类型的接点信号可合并。

2.2.3 网络选型

由于以太网采用CSMA/CD 媒体控制协议，两个以上Ethernet 网节点同时访问共享的传输介质局域网时会造成数据冲突，这会导致无法确切估计出冲突节点需要的随机等待时间，因此可能造成“实时”信息传输无效。文献[3]对比研究了普通Ethernet 网和令牌总线网的性能。在网络负荷小于25%的情况下，Ethernet 网的响应速度比令牌总线网络快很多。同时，Ethernet 网的CSMA/CD 方法也优于令牌传递的传输管理方法，使用这种方法可随时发送某个节点要发送的数据，而不必获得令牌控制权。

目前控制网络流量小于25％的方法主要是提高网络带宽和减少数据传输量。由参考文献[4]网络仿真结果可见，100 Mb/s 带宽的Ethernet网络可以满足实际二次回路通信的需要，将数据通道变为10BaseT 后的数据包时延图，数据的时延逐渐上升并不断发散。这是由于通信流量超过通道带宽后数据通信出现阻塞而引起的。它说明10 Mbps 带宽的Ethernet网络已经不能满足实际二次回路通信的需要。

3 网络信息安全

IEC 61850 对变电站网络系统的安全性未做规定，但这显然是不容忽视的问题，尤其过程总线的应用使网络系统从二次延伸到了一次,模拟量采集、跳合闸命令均通过网络实时实现的。如果由于网络的安全性、实时性原因引起误动、拒动、整定参数的错误更改等，将给电力系统的安全稳定运行带来严重威胁，有时甚至引发灾难性事故。2000 年 10 月，我国某大型水电站发生了一起跳闸甩负荷冲击事故,据分析，很可能是网络安全漏洞所致。事故的发生向人们敲响了网络安全的警钟。

《全国电力二次系统安全防护总体框架》出台的目的就是防范对电网和电厂计算机监控系统及调度数据网络的攻击侵害及由此引起的电力系统事故，以保障我国电力系统的安全、稳定、经济运行，保护国家重要基础设施的安全。

3.1 网络安全威胁

对于常规变电站自动化系统而言，由于其核心部分（测控单元）是利用串行通信传递数据，与站控层局域网是通过中间层前置单元在逻辑上进行隔离的，可以认为无网络安全风险。然而，站级总线的出现，测控单元也有风险了。

3.1.1 站级网络安全威胁

站级网络安全威胁主要来自变电站所连接的外部网络。它包括非法截获、中断、篡改、伪造、恶意程序、权限管理不当、Internet 的安全漏洞等[5]。

3.1.2 设备故障问题

包括硬件故障和软件故障两方面。硬件故障应及时发现，报警和维修。要有一系列故障应急措施，因故障引起的重要数据被破坏是很难恢复的，解决的办法是应用备份技术和灾难恢复计划。

该计划必须对任何紧急情况作出快速恢复，系统备份是任何安全防护体系的重要组成部分，有利于网络的快速重建，所有成员都要熟悉灾难恢复计划并根据实践中的经验教训,对其做出合适的调整。

3.2 变电站网络安全策略[5]

原则上，其他应用网络所采用的安全策略都

适用于变电站计算机网络。但是由于变电站计算机网络要考虑信息传输的实时性，因而必须对其安全策略进行具体分析。

3.2.1 分层分区的总体防护体系

电力系统二次安全防护总体框架其核心思想是提出了分层分区的总体防护体系，不同的安全区确定了不同的安全防护要求，其中安全区Ⅰ的安全等级最高，安全区Ⅱ次之，其余依次类推。各区之间须采用硬件防火墙或相当设备进行逻辑隔离。安全区Ⅰ、Ⅱ与其余安全区之间采用专用安全隔离装置，该隔离装置应该达到或接近物理隔离的强度，传输信息的方向是单方向的。

专用安全设备横向隔离设备与纵向加密认证装置是实现电力二次系统“横向隔离、纵向认证”安全策略的关键设备。横向隔离设备在省及省级以上调度中心得到广泛应用，具备全面应用条件。纵向加密认证装置具备应用条件。

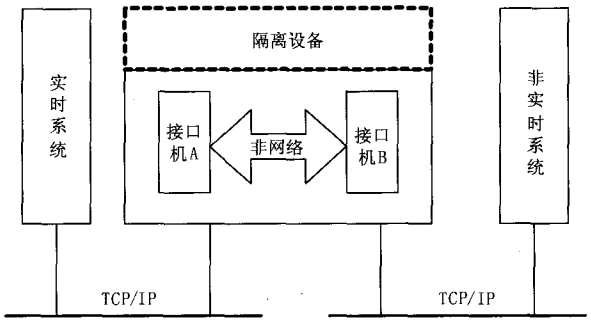

图3 隔离设备的硬件结构

Fig. 3 Hardware architecture of isolating device

网络安全隔离设备采用软、硬结合的安全措施，在硬件上使用双计算机结构实现物理上的隔离。在软件上，采用综合过滤、访问控制、应用代理技术、实现链路层网络层与应用层的隔离，在保证网络透明性的同时实现了对非法信息的隔离.

3.2.2 容错技术

容错技术包括软件容错和硬件容错两个方面。

软件容错是指软件系统对操作人员误操作具有一定的预防性；硬件容错是指系统具有组件冗余、无单点硬件失效、动态重组、错误校正等功能。其中，动态重组是指能够在线增减或更换系统组件而不干扰系统运行；错误校正指通过错误校正码和奇偶校验的结合达到保护数据的目的。在重要的变电站，也可以采取双机备份同步校验方式，或者采用双网冗余备份或信息分流的组网方式，建立一套可靠、高效的运行机制，当一个系统由于意外而崩溃时，计算机自动切换，以确保整个网络系统正常运转，保证各项数据信息的完整性和一致性。

3.2.3 加密技术

加密技术是最基本、最常用而又最有效的信息安全技术，可以有效地限制截获、中断、篡改、伪造的概率，从而达到保证信息安全的目的。针对变电站计算机网络，选用一些最常用的加密算法，例如国际数据加密算法就可以满足要求，密钥长度在56 位～ 128 位比较合适。

3.2.4 移动智能体(mobile agent) 技术

一旦外部的非法入侵者突破防火墙，进一步的网络安全防护工作就要由本地入侵监测系统负责。此时需要一个智能系统对非法入侵实时检测并迅速采取相应的对策，移动智能体技术则为其实现提供了一条便捷途径。

智能体(agent) 的概念来源于人工智能领域，一般是指任何具有智能和一定的自治性、按用户的意愿接受和处理的软件系统。当智能体能够从网络上的一个主机移动到另一个主机时，就可以称之为“移动智能体”。变电站自动化正在朝着分布式应用发展，因此，可将该技术应用于变电站局域网的安全管理中。国外学者在这方面已经做了很多工作，其中文献[6～8]就提供了各自的基于智能体技术的网络安全管理解决方案。

3.2.5 虚拟专网(VPN) 技术

VPN 是利用基于公共基础设施建设的公开网络的数据传输能力，借助相关安全技术和手段实现的，能够提供安全、可靠、可控的保密数据通信的一条安全通道。 确切来说，VPN 是利用不可靠的公用互联网络作为信息传输媒介，通过附加的安全隧道，用户认证和访问控制等技术实现与专用网络相类似的安全性能，从而实现对重要信息的安全传输。

3.2.6 建立基于深度防御理论的网络保护策略

深度防御必须在设计进程中予以考虑，要对与网络有关的任何技术的、决定性的方面进行综合性考虑，利用技术和管理上的控制尽可能地减小对网络各个层面的威胁；另外，每个层面的各个系统之间必须不受影响，例如，为防范内部威胁，要限制用户只访问与他工作有关的必需的那部分资源。

电力系统对于信息的安全性与一般的工业应用领域的需求是不一样的，电力系统由于其特殊的运行特征对于安全防护策略和一般工业系统的安全防护策略有较大的差异，如：

1)防止未经授权的调度员进入变电站控制系统，这种非法访问引起的后果要比一般的银行账户的非法访问严重得多；

2)在还使用窄带通道电力系统中，不能使用某

些钥密技术和加密算法；

3)许多系统采用多个通道的通信模式，常规的网络安全无法实施。

鉴于数据通信方式的多样性和来自信息非法访问的各种可能性，必须实施多层安全防护措施，如VPN仅保证传输层的安全性，不能保证应用层的安全性；必须采取附加的安全措施，如IEC62351-4所提供的应用层安全防护；此外，访问检测，访问名单控制，锁门技术，及其它的安全技术必须采用增加信息的安全防护措施后必须考虑对于系统性能的影响和对于网络带宽的影响。

4 结论

数字化变电站反映了数字化技术从变电站的二次设备向一次设备发展的必然趋势。本文综述了信息需求分类、信息合并等提高信息实时性的方法，以及几种针对性的提高网络信息安全性的技术。

参考文献

[1] 殷志良. 变电站自动化系统过程层与间隔层串行通信研究[J]. 中国电力, 2004, 37（7）.
YIN Zhi-liang.Investigation of Serial Communication Between Process Level and Bay Level of Substation Auto mation System[J]. Electric Power, 2004,37(7).

[2] IEEE TRPI 525-2003,Draft IEEE Technical Report on Substation Integrated Protection, Control and Data Acquisition Communication Requirements[Z]. 2003.

[3] 黄文君. 实时控制系统网络设计[J]. 机电工程，2000，17(3).
HUANG Wen-jun.Design of Real-time Control System Network[J].Mechanical & Electrical Engineering Maganize,2000,17(3).

[4] 韩小涛. 基于 OPNET 的变电站二次回路通信系统仿真研究[J]. 电网技术, 2005. 29(6).
HAN Xiao-tao.Research on Substation Secondary Circuit Communication System Using Opnet Simulator[J].Power System Technolog,2005,29(6).

[5] 高卓. 变电站的计算机网络安全分析[J]. 电力系统自动化，2002, 26(1):53-57.
GAO zhuo.Analysis of Computer Network Security in Substation[J].Automation of Electric Power Systems, 2002,26(1):53-57.

[6] Boudaoud K, Network Security Management with Intelligent Agents[A].In: Network Operations and Management Symposium[C].2000.

[7] JIANG Tao, LIU Ji-ren.The Research on Dynamic Self-adaptive Network Security Model Based on Mobile Agent[A]. In:36th International Conference on Technology of Object-oriented Languages and Systems[C]. 2000.

[8] LIN Zeng. Multiple Intelligent Agent Supported Internet Security System: Issues, Current Solutions and a Proposed Approach[A]. In: IEEE International Conference on Intelligent Processing Systems[C]. 1997.

收稿日期：2006-12-20； 修回日期：2007-01-09

作者简介：
吴国威(1971-)，男，硕士研究生。研究方向为继电保护及数字化变电站技术、信息技术在电力系统中的应用等。
E-mail:wu_guowei@zpepc.com.cn

（上接第 17 页 continued from page 17）

[4] 张海梁，袁荣湘，孙婉胜. 数据库访问中间件技术在SCADA数据库系统中的应用[J]. 电网技术，2006，29(17)：58-62.
ZHANG Hai-liang, YUAN Rong-xiang, SUN Wan-sheng. Application of Database Access Middleware Technology in SCADA Database[J]. Power System Technology, 2006, 29(17): 58-62.

[5] 朱韵箴，程代杰. 基于XML的分布式数据交换中间件模型设计[J]. 计算机工程与设计，2003，24(8)：35-38.
ZHU Yun-chi, CHENG Dai-jie. Design of XML-based Distributed Data Exchange Middleware[J].Computer Engineering and Design, 2003, 24(8): 35-38.

[6] 张小敏，李晓明，潘艳蓉. 基于数据库技术和Web应用的地方电网线损管理系统[J]. 继电器，2006，32(23)：62-65.
ZHANG Xiao-min, LI Xiao-ming, PAN Yan-rong.Energy Loss Management System of Local Electric Network Based on the Technology of Database and Application of Web[J]. Relay, 2006, 32(23): 62-65.

[7] 赖明江，耿英三，张国钢，等. 变电站自动化系统中实时数据库的研究[J]. 继电器，2006，34(2)：66-69.
LAI Ming-jiang, GENG Ying-san, ZHANG Guo-gang, et al. Study of Real-time Database Management System (RTDBMS) Applied in Substation Automation System[J]. Relay,2006,34(2):66-69.

收稿日期：2006-11-22； 修回日期：2006-12-24

作者简介：
蔡瑞强(1982-)，男，硕士研究生，主要研究方向为电力负荷预测和电力市场；E-mail:jacksin@sjtu.edu.cn
程浩忠(1962-)，男，教授，博士生导师，主要研究方向为电力系统电压稳定、电网规划和电能质量。