The Research on the Configurating Technology and Application Security of IEC 61850

HUANG Wen-hua[1]，**LI Yong**[2]

1. School of telecommunications and information engineering，Xi'an university of posts & telecommunications, 710121,China;2.Shannxi electrical power corp. Xi'an beareu, 710032,China

Email：hwh_cara@yahoo.com.cn

Abstract: IEC 61850 is the next seamless communication standard of Substation Automation System. The technical characteristics of IEC 61850 are detailed summarized in this paper for the purpose to development of Intelligence equipment device in substation. IEC 61850 uses the layered technology in system. The object-oriented technology is used for setting up the model of system. And Abstract Communication Service Interface is used for realizing seamless communication. It is the first time that the paper points out that the intension of IEC 61850 is the integration of heterogeneous information. The Substation configuration technology and the application of XML in IEC 61850 is analyzed. It includes the structure of configuration file and the flow of configuration. The ideal communication model of IEC 61850 based on XML is found. The security questions to substation communication network are discussed. And some useful advices for security of power system are given. The research provides basis for designing of device and SAS based on IEC 61850.

Keywords: IEC 61850 the Integration of Heterogeneous Information XML Security

基于 IEC 61850 的变电站配置技术及应用安全研究

黄文华[1]，**李勇**[2]

1. 西安邮电学院通信与信息工程学院，陕西西安，中国，710121；

2. 陕西省电力公司西安供电局 陕西西安，中国，710032

Email：hwh_cara@yahoo.com.cn

【摘 要】IEC 61850 是下一代变电站的无缝通信标准，本文为了 IEC 61850 具体应用中设备开发的目的，对 IEC 61850 的技术特点进行了详细总结，在深刻理解标准的基础上首次提出 IEC 61850 标准是对异构信息进行集成的实质内涵；讨论了 XML 技术在 IEC 61850 中的应用，得到了理想的 IEC 61850 通信程序模型；针对应用 IEC 61850 标准电力网络通信的安全问题提出了建议和策略，为符合 IEC 61850 标准的变电站通信系统开发和设备设计提供了依据。

【关键词】IEC 61850，异构信息集成，XML，电力网络安全

1. 引 言

IEC 61850 是国际电工委员会负责电力系统控制及其通信的相关标准的第 57 技术委员会（IEC TC57）制定的关于变电站自动化系统结构和数据通信的一个国际标准，目的是使变电站内不同厂家的智能电子设备（IED）之间通过一种标准协议实现互操作和信息共享，取消多种协议转换环节和转换设备，使系统调试更加便捷，节省调试时间，实现“一个世界、一种技术、一个标准”[1]。

在制定 IEC 61850 标准的过程中，美、德、荷兰等国都建有示范工程，用以验证标准，同时又通过实践促进标准完善应用。应用 IEC 61850 的数字化变电站技术是我国十一五重点研究课题，目的在标准制定和产品研发方面追赶国际先进水平。IEC 61850 标准的正在我国电力系统普及发展，在地区电网的应用推广也在逐步实现中，而符合 IEC 61850 标准的设备的开发，需要对标准的深刻理解与掌握，本文对 IEC 61850 的相关技术进行研究与讨论。

2. IEC 61850 的技术特点概述

IEC 61850 规约体系完善，相对于基于报文结构

的传统规约，应用面向对象技术的 IEC 61850 有明显的技术特点和优势[2]。

2.1 系统分层技术

IEC 61850 明确了变电站自动化系统的三层结构：变电站层、间隔层和过程层以及各层之间的接口意义，如图 1 所示。变电站层主要功能有与过程相关的功能和与接口相关的功能。前者指利用各间隔或全站信息对多个间隔或全站一次设备进行控制；后者是指与远方控制中心、后台监控之间的通信。过程层通常包括远方 I/O、智能传感器和执行器等设备，实现开关量和模拟量的采集，进行现场信息上传、操作命令下传等与一次设备有关的功能。间隔层利用采集数据对该间隔的一次设备发送控制命令，实现线路保护等功能。将由一次设备组成的过程层纳入统一结构中，这是基于一次设备如传感器、执行器的智能化和网络化发展。

2.2 面向对象的建模技术

为了实现互操作性，IEC 61850 标准采用面向对象技术，建立统一的设备和系统模型，采用基于 XML 的 SCL[3]变电站设备通信配置语言来全面的描述设备和系统，提出设备必须具有自描述功能。对具体智能电子设备（IED）进行通信数据的建模，典型的操作数据以及配置数据都包含在逻辑节点中。由于数据均带有自我描述，因此不必对数据进行预先定义便可进行传输，从而简化了数据的管理和维护工作。这种自描述、自诊断和即插即用的特性，极大方便了系统的集成，降低了变电站自动化系统的工程费用。

2.3 抽象服务通信接口技术

IEC 61850 为实现无缝的通信网络，提出抽象通信服务接口（ACSI）[4]，积极采用其他行业的成熟技术如以太网、MMS 等构成通信网络。抽象服务通信接口技术独立于具体的网络应用层协议，与采用何种网络无关，可充分适应 TCP/IP 以及现场总线等各类通信体系，而且客户只需改动特定通信服务映射 (SCSM)，即可完成网络转换，从而适应了电力系统网络复杂多样的特点。

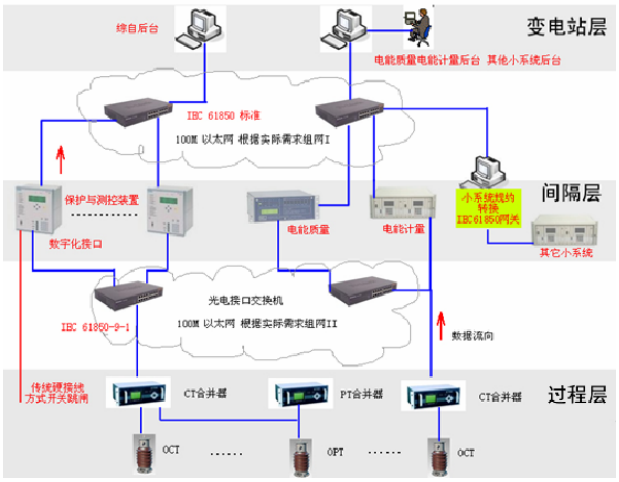

图 1. 基于 IEC61850 的数字化变电站主要设备及结构示意图

3. IEC 61850 标准的本质

作为下一代变电站的无缝通信标准，IEC 61850 充分借鉴了变电站通信、计算机、工业控制等领域的长期经验[5]。在 IEC 61850 鲜明技术特点的背后，是 IEC 61850 与以往变电站通信标准的实质性差别，而理解 IEC 61850 的本质是应用 IEC 61850 的基础。

IEC 61850 是变电站自动化通信标准，通信标准的本质目标是实现双方快速准确的理解相互传达与接收到的逻辑信息命令，并正确执行命令。由于各设备生产商生产的智能电子设备，可能采用不同的芯片、不同的硬件架构、不同的嵌入式系统，它们组成了一个复杂的异构环境系统，所以变电站中设备之间的通信是一个复杂的分布式信息交互问题。变电站设备要实现互操作实际就是解决如何在异构环境下实现数据交换的问题。IEC 61850 标准制定的思路与以往 IEC 60870 等标准在解决信息表达与传输问题方面相比上存在着根本的区别，主要是借鉴了近些年来计算机解决异构环境领域的常用的 ASN.1、XML 等技术来解决变电站中的信息交互问题，因此 IEC 61850 标准的本质可以理解为是解决

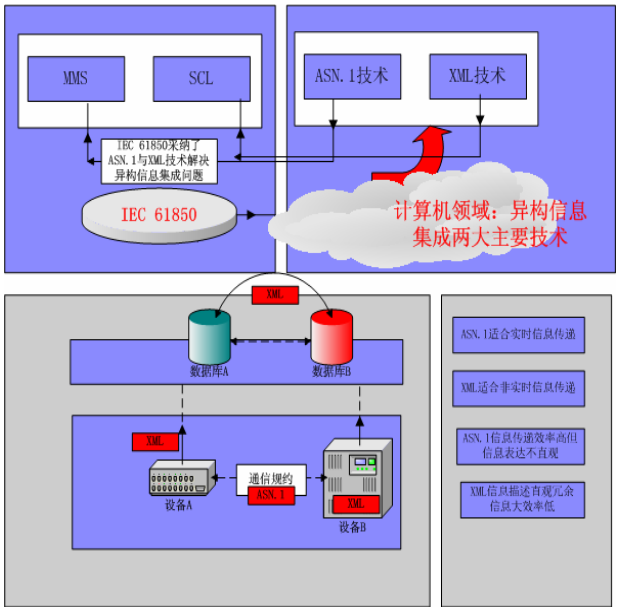

图2. IEC 61850标准中的异构信息集成技术

978-1-935068-23-5 © 2010 SciRes.

变电站中异构环境下数据交换问题的一个实现方案。

IEC 61850 标准适用于变电站内通信，因此对实时性要求特别高。标准充分糅合了 ASN.1 与 XML 两种技术的各自优势，利用 ASN.1 的二进制编码信息传输效率优势，用它作为主要的实时信息交互通信方式，利用 XML 直观与带自描述特性在 XML1.0 版本的基础上推出了变电站配置语言 SCL，用于描述变电站系统的结构与智能电子设备的能力及定义通信参数等。如图 2 所示。W2G 组织提出了要将 MMS 映射到 XML，采用 XML 技术来代替 MMS 协议中的 ASN.1 编码，所以 ASN.1 与 XML 两者正在不断的相互借鉴发展。

4. IEC 61850 中 XML 配置的运用

IEC 61850－6 部分规范了 SCL 语言规范了装置所含有的逻辑节点、数据集、报告控制块、站内连接方式、IP 地址等通信配置等等。通过采用 XML 的配置可以实现装置的功能自动组合，装置内的程序可以通过直接修改配置文件而动态的改变装置所具有的功能，比如修改逻辑节点或者数据集等等，这样就可以实现装置侧的程序通用，对于厂家而言，可以实现一个通用的通信程序，然后根据具体特定装置功能需求，设计配置不同的 XML 文件即可实现不同装置的通信。最理想的 IEC 61850 通信程序（图 3）的明显优势在于：程序一次编译完成，可以只需要简单的修改配置文件就可以应用到各个装置设备中，综合自动化后台通过读取装置配置文件就可以自动创建数据库实现装置接入与生成。但需要指出的是 IEC 61850-6 只是规范了对外通信的配置，不同的装置本身功能与其底层硬件本身是相关的，因此还对不同的厂家而言应该有自己的这一部分配置，这部分配置不在 IEC 61850 标准化的范围规范之内，属于装置的具体实现部分工作。

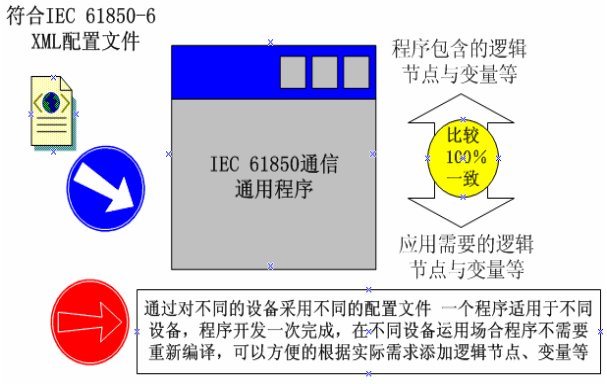

图3. 理想的IEC 61850通信程序

5. IEC 61850 应用安全问题

IEC 61850 标准的采用，可以有效的实现从上至下生产控制与调度运行信息的整合，减少了过去“信息孤岛”现象的产生，真正了实现设备间互操作与调度系统间信息的交互。但是 IEC 61850 的应用依赖于一个安全的网络环境。因此，当前电力系统在解决了信息异构集成问题后，突出面临的一个问题就是如何构造一个安全的网络通信系统，WG15 已经开始专注于电力数据和通信安全领域，来保证电网的安全运行[6]。

根据电力系统的特点、目前状况和安全要求，可以将整个信息网络系统分为四个等级：第一等级是实时控制类型，是安全保护的重点与核心。凡是实时监控系统均应属于这一类型。第二等级是控制生产类型。主要为不具备控制功能的生产业务和批发交易业务系统。第三等级生产管理类型，主要是为支持企业经营、管理、运营的管理信息系统。第四等级是管理信息类型。

电力系统安全防护重点在实时控制系统，IEC 61850标准在变电站分层中提出了过程层，并在这一层也采用以太网通信完全替代原来传统的硬接线方式。由于在过程层中诸如跳闸的GOOSE报文要求在4ms内到达通信接收的另一端，与以太网在变电站层和间隔层相比需要保障更高的安全可靠性，因此，如何保障变电站内过程层网络的安全性问题比以往显的更为突出和重要。

从应用安全的角度出发，基于IEC 61850的变电站通信系统应具备以下防御措施：

1) 采用VPN技术解决端到端的数据安全问题。主要采用隧道技术、加解密技术、密钥管理技术、使用者与设备身份认证技术等四项技术来保证安全。通过安全策略和安全规则的制定，把网络划分成不同的安全区域，控制VPN通道内不同的安全区域之间的访问，可以进一步减少了内部窃听的风险和不安全因素，使网络的

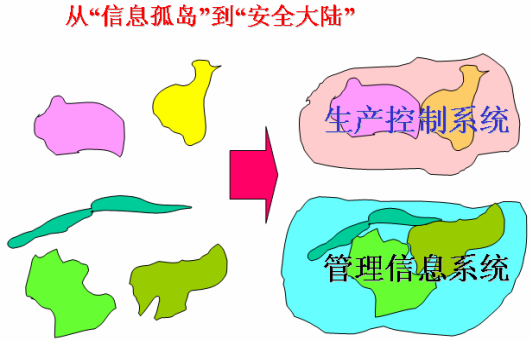

图4. 电力通信面临的安全问题

安全性得到进一步的提升。

2) 采用SSL/TLS加密技术，对变电站通信系统中面向连接通信机制的服务器连接进行授权验证，在对象建模中对不同用户加入访问权限限制，并报告试图进行未授权下的访问操作。

3) 采用SNMP（简单网络管理协议）来管理变电站通信网络，定期建立数据备份与实施冗余机制。

4) 建立入侵监测防御措施，建立控制中心安全策略应对措施，基于IEC 61850的变电站通信系统控制中心应采取多层安全机制保证，当受到攻击时可以降低使用情况而不至于系统瘫痪。

除了以上从技术的角度应对电网安全问题外，还应注意人员的管理与安全意识、工程施工等与电网安全运行密切相关的因素。

6. 结束语

IEC 61850标准作为未来国际变电站的统一标准，已经在逐步走向成熟。本文为了IEC 61850具体应用中IED设备开发的目的，对IEC 61850的技术特点进行了总结，首次提出IEC 61850标准是对异构信息进行集成的实质内涵，讨论了XML技术在IEC 61850中的应用，得到了理想的IEC 61850通信程序模型；针对应用IEC 61850标准电力网络通信的安全问题提出了建议和策略。在中高压综合自动化系统中，IEC 61850的性能与优势能得到更多的体现。IEC 61850标准可以有效的解决变电站内设备的互操作问题，作为一致公推的变电站标准必将给变电站自动化系统带来深远的影响。

References(参考文献)

[1] Wang Hao, Bo Chunquan, Research on IEC 61850[J]. Equipment Manufacturing Technology,2008(12):161-163
王昊，薄纯全，IEC 61850 标准研究[J]. 装备制造技术, 2008(12):161-163

[2] Li Guanghui, Study on substation device modeling based on IEC 61850[J]. Telecommunications for Electric Power System, 2009(4):27-29
李光辉,基于IEC 61850 的变电站装置建模[J]. 电力系统通信, 2009(4):27-29

[3] IEC 61850-6, Com munication network and systems in substations. Part6: Configuration description language in electrical substations related to IEDs [S]. [s.n.],U.S.A. 2008

[4] IEC 61850-7，Communication network and systems in substations. Part7-2:Basic communication structure for substations and feeder equipment –Abstract communication service interfaces[S].[s.n.],U.S.A. 2008

[5] Wu Xiaobo, Wang Yongfu, Yang Wei, Du Shengyun,Yuan Wenguang, Developments in Digital Substation Automation Systems[J].Automation of Electric Power Systems,2009(16):101-106
吴晓博, 王永福, 杨威, 杜升云, 袁文广, 数字化变电站自动化系统开发建议[J]. 电力系统自动化, 2009(16):101-106

[6] Mo Jun, Tan Jiancheng, Research on network security in substations based on IEC 61850[J]. Telecommunications for Electric Power System,2009(4):17-21
莫峻，谭建成, 基于IEC 61850 的变电站网络安全分析[J]. 电力系统通信, 2009(4):17-21

978-1-935068-23-5 © 2010 SciRes.