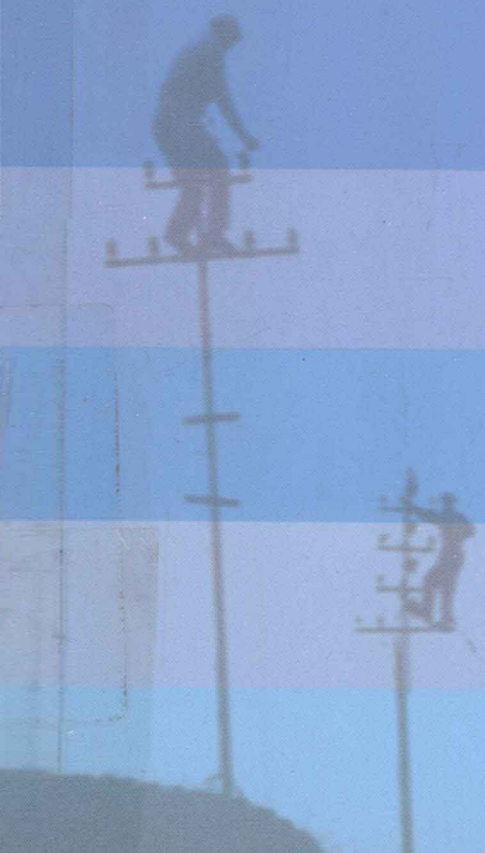
信息技术与电力系统安全操作

Information Technology And Safe Operations In Electric Power System

段斌 吴亚联 著



湘潭大学出版社

信息技术与电力系统安全操作

Information Technology And Safe Operations In Electric Power System

段斌　吴亚联　著

湘潭大学出版社

图书在版编目(CIP)数据

信息技术与电力系统安全操作 / 段斌，吴亚联著. —湘潭：湘潭大学出版社，2008.8
ISBN 978-7-81128-055-5

Ⅰ. 信… Ⅱ. ①段…②吴… Ⅲ. 信息技术—应用—电力系统—安全技术 Ⅳ. TM7-39

中国版本图书馆 CIP 数据核字 (2008) 第 118294 号

信息技术与电力系统安全操作

段 斌 吴亚联 著

责任编辑：龙顺潮
封面设计：罗志义
出版发行：湘潭大学出版社
社　　址：湖南省湘潭市 湘潭大学出版大楼
电话(传真)：0732-8298966　邮编：411105
网　　址：http://xtup.xtu.edu.cn
印　　刷：湘潭地调彩印厂
经　　销：湖南省新华书店
开　　本：787×1092　1/16
印　　张：10.5
字　　数：253 千字
版　　次：2008 年 8 月第 1 版　2008 年 8 月第 1 次印刷
书　　号：ISBN 978-7-81128-055-5
定　　价：24.00 元

前　言

电力系统中对电网设备的正确操作，是电网安全经济运行的重要前提。为了有效防范电气设备误操作引发的人身和重大设备事故，我国早在1990年就提出了电气设备“五防”的要求，并以法规形式行文规定了电气防误的管理、运行、设计和使用原则。在长期的工程实践中，形成了电力系统安全操作的一些基本规则：防止误入带电间隔；防止误分、合断路器；防止带负荷分、合隔离开关；防止带电合地刀闸（挂地线）；防止带地刀闸（地线）合断路器（隔离开关）等。

随着信息技术在电力系统中的广泛应用，变电站自动化程度的逐步提高，现在变电站设备与设备、一次与二次、远方与就地之间，不再是独立的或者是简单的电缆连接，而是通过先进的通讯技术形成统一的网络，从而实现变电站的信息共享和资源共享。随着变电站自动化通信技术的发展，变电站操作将是基于网络的访问过程，其安全措施将主要表现为对访问行为的规范，包括控制对象对访问权限的判定。

在国际上，以IEC TC57（第57技术委员会）推出的“变电站通信网络与系统”（IEC 61850）为代表，电力工业通信正在发生一场巨大变革，将由面向点、节约带宽、提供通信程序调用的专用通信技术，朝着面向对象、工程实现方便、提供信息服务的开放通信技术发展。

为适应变电站自动化技术的迅速发展，1995年国际电工委员会第57技术委员会（IEC TC 57）成立了3个工作组（WG 10/11/12），负责制定“变电站通信网络与系统”国际标准，经过近10年的努力，于2004年推出了由10个部分组成的IEC 61850标准。该标准是关于变电站自动化系统的第1个完整的通信标准体系。与传统的通信协议体系相比，在技术上IEC 61850有如下突出特点：（1）使用面向对象建模技术。将应用功能分解为最小实体（逻辑节点），通过虚拟化建立抽象模型；（2）分层目录服务。IEC 61850中的目录服务共有5层，分别是服务器目录、逻辑设备目录、逻辑节点目录、数据对象目录、读数据定义。在线情况下客户可以通过这些服务在客户数据库中建立对方全部的镜像，用于检索设备中整个分层的定义及全部可访问的信息定义、全部类的实例定义；（3）服务与映射分开。在IEC 61850中，提出了抽象通信服务接口（ACSI）和具体通信服务映射（SCSM），这样，就把通信服务要求跟具体的通信协议分离开，有利于适应通信技术的不断发展；（4）采用制造报文规范（MMS）技术。在IEC 61850-8-1中采用了MMS来完成通信过程。MMS是OSI 7层通信模型的一种应用层协议，主要用于过程自动化领域。

在制定IEC 61850的过程中，美国、德国、荷兰等国都有示范工程，用以验证标准，并通过实践反过来促进标准完善。Siemens、ABB等公司已推出了IEC 61850的变电站自动化系

统的产品。国内,在国家电力调度通信中心的组织下,正在进行 IEC 61850 互操作试验。从2004 年底启动至今,已成功进行了 5 次互操作试验,为推动 IEC 61850 在我国的应用起到了很好的作用。

电力工业通信领域技术发展的趋势是通信规约的网络化及国际标准化。随着开放性的增加,安全问题越来越突出。电力系统数据和通信安全的核心内容是认证和加密。认证,从简单的地址认证、口令认证方式过渡到利用安全证书,确保信息通信的合法性和完整性;加密,从通过物理隔离发展到利用 TLS 和 VLAN 来进行保密传输,保证通信过程中信息的私有性。

目前在电力系统得到广泛应用的通信协议是在信息安全没有成为工业的重要问题前发展起来的,不涉及通信的安全功能。因此,需要建立起网络环境下电力系统的数据通信安全体系。为了保证电力信息基础设施的安全,2007 年 6 月,IEC TC57 WG15 推出了第 1 套电力工业通信信息安全国际标准——IEC 62351(电力系统管理和相关的数据交换——数据和通信安全)。

结合对 IEC 61850、IEC 62351 等新一代电力系统自动化通信标准相关部分的分析、研究和实施,本书系统、全面地介绍了面向对象技术、软件工程、网络通信、信息安全等信息技术在电力系统安全操作中的应用成果。本书是湘潭大学信息安全理论与技术应用重点实验室全体成员多年来集体智慧的结晶。在本书写作过程中刘念博士、伍军博士、肖红光博士、马铭磷博士、段吉泉硕士、刘兵硕士、罗嘉文硕士、罗钦硕士、刘力政硕士、廖建容硕士、孙璐硕士、舒立硕士、张文奇硕士、肖衡硕士、周江龙硕士、陈晓辉硕士、邹吉昌硕士、李晶硕士、刘莉莉硕士、林素烟硕士、李光辉硕士等为本书提供了丰富的资料。在相关的科研工作中得到了湖南省电力公司调度通信局黄生龙高级工程师的大力支持。本书也是国家自然科学基金项目(批准号:50677058)、国家"863"项目(编号:2007AA012476),以及湖南省自然科学基金项目(编号:06JJ50081)的成果总结。

由于作者水平有限,书中难免出现各种失误和不当之处,欢迎大家批评指正。

作 者

2008 年 5 月

目 录

第 1 章　基于 IEC 61850 的变电站自动化通信系统

1.1　IEC 61850 标准的结构

国际电工委员会于 2004 年发布了 IEC 61850 标准[1~13]。IEC 61850 标准由 10 个部分组成，除了第 10 部分还未成为国际标准外，其他部分都已作为国际标准对外颁布。该标准包含了变电站自动化系统从性能要求、工程管理到数据建模和网络通信的一系列内容，具体内容如下：

IEC 61850-1：绪论（Introduction and overview），主要介绍了 IEC 61850 产生的必要性，以及标准各部分主要内容的简介。

IEC 61850-2：术语（Glossary），为该标准中变电站自动化系统的专门术语词汇表。

IEC 61850-3：总体要求（General requirements），介绍了变电站自动化系统内通信系统的质量要求，包括可靠性、可用性、可维护性和安全性等等。

IEC 61850-4：系统和工程管理（System and project management），包括变电站内必备硬件配置的定义、功能和信号质量的适应性以及所有具体定义的文档。

IEC 61850-5：功能和设备模型的通信要求（Communication requirements for substation automation system functions），包括变电站功能和接口的逻辑分配、互操作方法、逻辑节点的概念、PICOM（Piece of information for communication 通信信息片）概念、功能定义的规则、功能分类、逻辑节点列表、逻辑节点和相关的 PICOM、逻辑节点分配和交互原理、使用逻辑节点附加原理、PICOM 表、报文类型以及动态性能要求。

IEC 61850-6：变电站智能电子设备（IED）结构语言（Configuration language for electrical substation IEDs），主要介绍变电站配置语言 SCL 的对象模型和语言内容。

IEC 61850-7：变电站和馈线装置的基本通信结构（Basic communication structure for substation and feeder equipment），该部分是整个标准的核心内容，分为四个部分：

第一部分：原理和模型（Principles and models）；第二部分：抽象通信服务接口（Abstract Communication Service Interface，ACSI）；第三部分：公共数据模型（Common data classes）；第四部分：兼容逻辑节点和数据类（Compatible logical node classes and data classes）。

IEC 61850-8：变电站层与间隔层特定通信服务映射（Specific Communication Service Mapping，SCSM），将变电站层的服务映射到具体通信服务，比如说映射成 MMS、CORBA。

IEC 61850-9：间隔层与过程层特定通信服务映射（Specific Communication Service Mapping，SCSM）。该部分标准分为两个部分，第一部分：特定通信服务映射-通过连续单向多支路点对点连接传输采样值（Specific Communication Service Mapping（SCSM）-Sampled values o-

ver serial unidirectional multidrop point to point link)；第二部分：特定通信服务映射-通过ISO／IEC 8802-3 传输采样值(Specific Communication Service Mapping (SCSM)-Sampled values over ISO／IEC 8802-3)。

IEC 61850-10：一致性测试(Conformance testing)，对系统的一致性进行测试。

上述 10 个部分中，IEC 61850-7 是标准的核心部分，它是变电站自动化系统上层应用和下层实现的接口部分。

1.2 IEC 61850 标准的两个重要概念

(1) 互操作性(Interoperability)

同一个生产商或不同生产商制造的两个或多个智能电子设备(IED)之间能够交换信息，能够使用这些信息正确地执行特定功能，称之为互操作性。

(2) 互换性(Interchangeability)

在不改变系统内其他元件的前提下，一个生产商制造生产的 IED 装置能够代替另一个生产商的装置，称之为互换性。

1.3 变电站自动化系统体系结构

IEC 61850 标准将变电站自动化系统按功能和逻辑通信抽象为 3 层体系结构：变电站层(第 2 层)、间隔层(第 1 层)、过程层(第 0 层)[1]，其结构如图 1.1 所示。

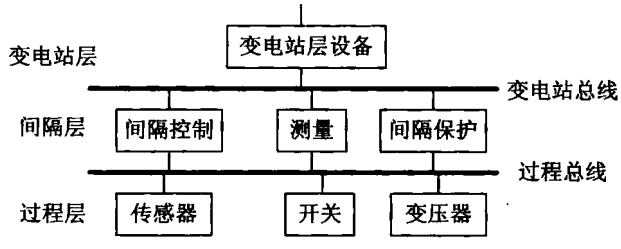


图 1.1 变电站自动化三层体系结构

变电站总线用于变电站层和间隔层间通信，过程总线用于间隔层和过程层间通信。过程层主要完成开关量 I／O、模拟量采集和控制命令发送等与一次设备相关的功能。IEC 61850 标准要求过程层的数字式传感器能够将一次侧的电压、电流等模拟量直接转换为数字信息，通过通信网络传送至间隔层；数字式执行器能够执行由通信网络传送的命令。间隔层的功能是利用本间隔的数据对本间隔的一次设备产生作用。变电站层完成对站内间隔层设备、一次设备的控制及与远方控制中心、工程师站及人机界面通信的功能。

由于 IEC 61850 并不规定通信拓扑，并且不限制任何物理的通信接口，而只是根据需求定义可以在物理的通信链路上应用的通信服务，因而上面的三层体系只是抽象的概念，并不限定实际的网络形式。IEC 61850 标准使用以太网作为基本通信技术，随着网络技术的发展，变电站总线和过程总线完全可以通过同一个网络来实现。这样的通信系统不但实现了变电站内的无缝连接，还有利于变电站与控制中心构成统一的无缝通信网络。

变电站自动化三层体系各自代表的功能为变电站层功能、间隔层功能、过程层功能，其相应的逻辑接口如图 1.2 所示。

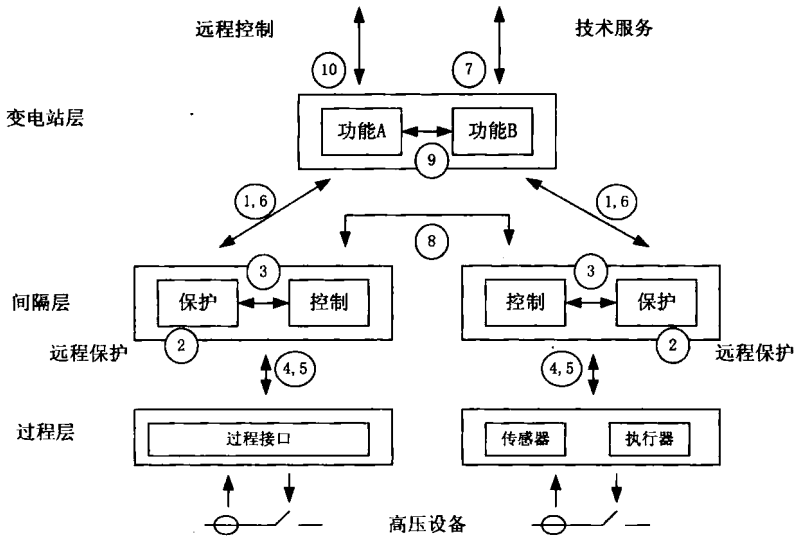


图 1.2　变电站自动化三层体系的功能与逻辑接口模型

逻辑接口功能：

接口①：间隔层与变电站层间的保护数据的交换；

接口②：间隔与远方保护设备间的保护数据的交换（超出 IEC 61850 标准范围）；

接口③：间隔层内的数据交换；

接口④：过程层与间隔层之间 CT、VT 的瞬时数据交换；

接口⑤：过程层与间隔层之间的控制数据的交换；

接口⑥：间隔层与变电站层间的控制数据的交换；

接口⑦：变电站与远方工程师工作站的外部通信；

接口⑧：间隔之间的直接数据交换（尤其对互锁类的快速功能的直接数据交换）；

接口⑨：变电站层内的数据交换；

接口⑩：变电站层和远方控制中心间的控制数据交换（超出 IEC 61850 标准范围）。

接口①、⑥、③、⑨、⑧通常组合成变电站／间隔层的总线，因为它既连接变电站层与间隔层，也连接不同的间隔本身。接口④、⑤组成过程总线，它连接间隔层与过程层以及不同的过程层的 IED。过程总线常常仅限定在单个间隔。如果把过程总线扩展到多个间隔，它可能也承担接口⑧的作用，至少用于其中的数据交换。接口⑦可以通过与变电站／间隔总线的直接接口来实现。接口②和接口⑩均超出本标准的范围。

三层体系的功能：

（1）变电站层功能有两类：第 1，相应于处理的变电站层功能是使用多个间隔或整站的数据，并且作用到多个间隔或整个站的一次设备。这些功能主要通过逻辑接口⑧通信。第 2，相应于接口的变电站层功能是表示 SAS 到本地站操作员 HMI（人机接口）、到远方控制中心 TCI（遥控接口）或远方监视维护工程 TMI（远方监视接口）接口的功能。这些功能通过逻辑接口①和⑥与间隔层通信，通过逻辑接口⑦和远方控制接口⑩与外部世界通信。

（2）间隔层功能是主要使用一个间隔内的数据并且对这个间隔的一次设备进行操作。这些功能是通过逻辑接口③在间隔层内通信，通过逻辑接口④和⑤与过程层通信，即与任何

类型的I/O或智能传感器和执行器通信。对于应用层和间隔层间通信,定义了一系列点到点接口,这些接口限定在逻辑接口④。过程层功能是连接到过程的全部功能。这些功能通过逻辑接口④和⑤与间隔层通信。从物理的角度,作为客户机的站级计算机可能仅具有HMI、TCI和TMI等基本功能。所有其他的变电站层功能可能完全分布在间隔层的设备上完成。在这种情况下,接口⑧就是系统的主干。另一方面,所有变电站层的功能,如相互闭锁等,可能驻留在变电站层的计算机中,既作为客户端又作为服务器。在这种情况下,接口①和⑥承担接口⑧的所有功能。相类似的解决方案还有很多。

(3) 间隔层的功能可能由专门的间隔层设备完成(保护单元,控制单元,有或没有冗余),或者由组合的保护控制单元完成。如果没有接口④和⑤,过程层功能在间隔层完成。实现接口④和⑤,过程层可能包含了远方I/O设备或智能传感器和执行部件,这些设备可以在过程层提供某些间隔层功能。

IEC 61850不限制对于实际通信网络,逻辑接口是如何分配的。逻辑接口可能在一个专门的物理接口上实现,也可能两个或多个逻辑接口组合在一个公用物理接口中。另外,这些接口可能组合形成一个或多个物理的局域网。这些物理接口的需求取决于层和设备的功能分布,而且,并不是所有接口都必须出现在变电站中,因而使得变电站的改进和扩建更加灵活。

1.4 变电站设备模型

IEC 61850除了将变电站自动化系统分成变电站层、间隔层、过程层之外,每个物理设备(IED)由服务器和应用组成,将服务器(Server)分层为逻辑设备(LD,Logical Device)-逻辑节点(LN,Logical Node)-数据对象(DO,Data object)-数据属性(DA,Data attributes)。从通信的角度来看,每个IED既可扮演服务器角色也可扮演客户的角色,如图1.3所示。这种分层,需要有相应的抽象服务来实现数据交换。ACSI服务有服务器模型、逻辑设备模型、逻辑节点模型、数据模型和数据集模型。如图1.4所示,通过Server Directory收集服务器中的逻辑设备名和文件名,通过LDDirectory收集每个逻辑设备中的逻辑节点名,通过LNDirectory收集每个逻辑节点中的数据对象名,通过DODirectory收集每个数据对象中的数据对象属性名,通过这样的服务建立起完整的分层数据库模型。通过GetDODefinition服务中的参数分别读取全部数据对象属性定义、一个数据对象属性定义或受请求功能约束的全部数据对象属性。这样就可以直接访问现场设备,对各个制造厂商的设备都用同一种方法进行访问。这种方法可以用于重构配置,很容易获得新加入的设备的名称和用于管理设备的属性。

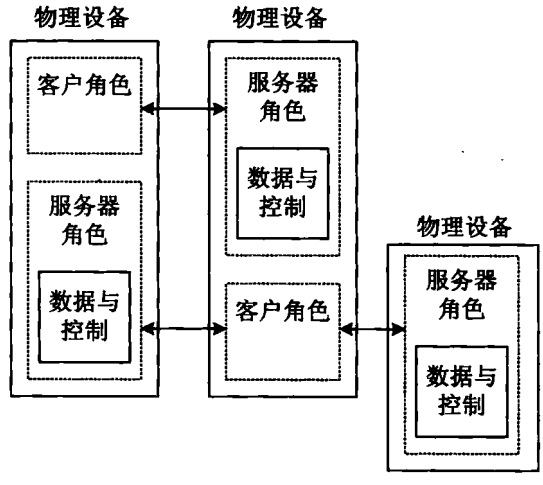


图1.3 物理设备的客户与服务器角色

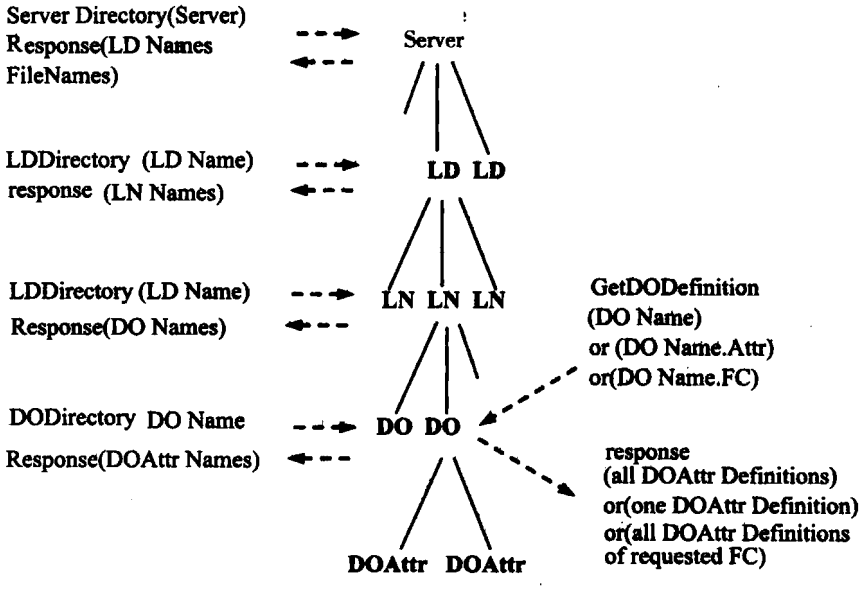


图 1.4　物理设备服务器的信息分层

1.5　设备的功能建模

IEC 61850 为了实现将变电站自动化功能分布和分配在不同 IED 上，将所有功能分解成逻辑节点。这些节点可能分布在一个或多个物理设备(PD，Physical Device)上。为了实现逻辑节点间的数据变换，逻辑节点间通过逻辑连接(LC，Logical Connection)相连，如图 1.5 所示。

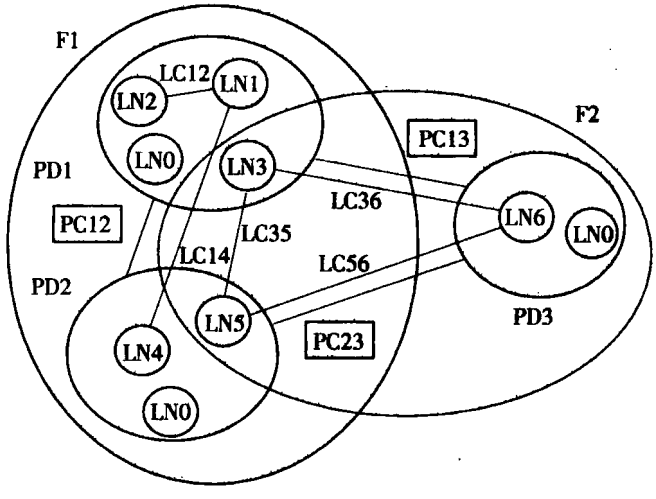


图 1.5　功能分解的示例

图 1.5 中主要实现两个功能 F1 和 F2。F1 功能分解成 5 个逻辑节点 LN1、LN2、LN3、LN4、LN5；F2 功能分解成三个逻辑节点 LN3、LN5、LN6。而在实际中这两个功能又由三个物理设备(IED)完成。第一个物理设备中含有三个逻辑节点，第二个设备中含有两个逻辑

节点,第三个设备只有一个逻辑节点。它们之间的连线表示通信联系。(注:LN0 是 IEC 61850 标准中一个特殊定义的逻辑节点,表示每一个物理设备的自我描述,而且是固定的。)

1.6 通信建模与服务映射

IEC 61850 标准把通信技术本身和要实现的通信功能分开。因为通信技术发展过快,最新制定出的通信协议出版时也不一定能代表当时的最新技术。标准规定了变电站功能和设备模型的通信要求,同时为支持功能的自由配置,对功能作了适当分解,分解成相互通信的逻辑节点,而且标准中列出了变电站各逻辑节点要交换的数据和性能要求。从信息抽象的角度来看,变电站的配置工作就成为定义变电站中的数据流向。IEC 61850 标准通过总结电力生产过程的特点和要求,归纳出变电站自动化所必须进行信息传输的网络服务,设计出抽象通信服务接口(ACSI),它和具体的网络应用层协议(例如目前采用的 MMS)独立,和采用的网络(例如现在采用的 TCP/IP 网络)无关。

在 IEC 61850 7-2、7-3、7-4 中,ACSI 共定义了 14 种通信服务接口模型,分别是服务器模型(Server Class Model)、应用关联模型(Application Association Model)、逻辑设备模型(Logical-Device Class Model)、逻辑节点模型(Logical- Node Class Model)、数据模型(Data Model)、数据集模型(Data-Set Class Model)、替代模型(Substitution Model)、设置控制模型(Settting-Group-Control-Block Class Model)、报告控制与记录控制模型(Report-Control-Block and Log- Control-Block Model)、通用变电站事件模型(Generic substation event class Model)、采样数据模型(Sampled Value Class Model)、控制模型(Control class Model)、时间与时间同步模型(Time and time synchronization Model)、文件传输模型(File transfer Model)。这些服务模型定义了通信对象以及如何对这些对象进行访问,包括请求、响应及服务过程。服务过程描述了某个具体服务请求如何被服务器所响应以及采取什么动作在什么时候以什么方式响应。任何设备、控制器,甚至 SCADA、维护系统或工程系统都可以使用 ACSI 服务实现设备间的互操作。

ACSI 中的抽象概念可以归纳为两个方面:第一,ACSI 仅仅建模了通信网络可视访问的实际设备(例如断路器)或功能,抽象出各种层次结构的类模型和它们的行为。第二,ACSI 从设备信息交换角度进行抽象,并且仅仅定义了概念上的互操作。具体的方法在 SCSM 中定义。

由于电力系统生产的复杂性,信息传输的响应时间要求不同,在变电站内需要采用不同的网络应用层协议和通信栈。通过改变相应特定通信服务映射(SCSM)便可完成。

特定通信服务映射定义了采用特定的通信栈如何实现服务和模型,映射和采用的应用层定义通过网路交换数据的语法(具体编码)。SCSM 作为中间层提供抽象应用层所不支持的功能并将抽象应用层的抽象服务映射为实际的服务。无论是变电站总线还是过程总线,IEC 61850 都提供了相应的特殊通信服务映射。SCSM 弥补了 ACSI 提供的功能与所采用的应用层提供的功能之间的差距。

IEC 61850 8-1、9-1、9-2 中的特殊通信服务映射(SCSM)定义了对象和服务向网络层的映射。按照应用的网络层协议不同,映射方法也各不相同,这由 IED 生产商自己定义,但是 IED 的抽象通信服务接口是相同的。

ACSI、SCSM 与应用通信层次模型如图 1.6 所示。特定通信服务映射(SCSM)将抽象通信服务、对象和参数映射到特定的应用层,这些应用层提供了具体的编码。

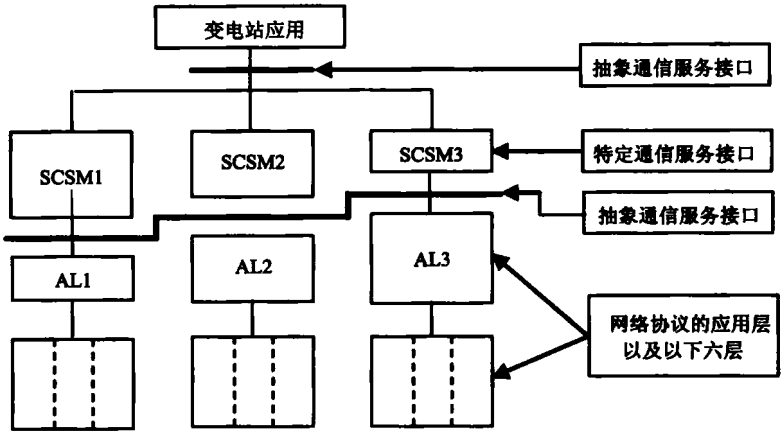


图 1.6　特定通信服务映射

ACSI 的核心部分通过 SCSM 映射到应用层协议为基于 TCP／IP 以太网的制造业报文规范（MMS，Manufacturing Message Specification）[14～16]。

参　考　文　献

[1] IEC TC57. IEC 61850-1, Communication Network and Systems in Substations-Part 1: Introduction and overview[S]. 2003

[2] IEC TC57. IEC 61850-2, Communication Network and Systems in Substations-Part 2: Glossary[S]. 2003

[3] IEC TC57. IEC 61850-3, Communication Network and Systems in Substations-Part 3: General repuirements[S]. 2003

[4] IEC TC57. IEC 61850-4, Communication Network and Systems in Substations-Part 4: System and project management[S]. 2003

[5] IEC TC57. IEC 61850-5, Communication networks and systems in substation-Part 5: Communication requirement for functions and device models[S]. 2003

[6] IEC TC57. IEC 61850-6, Communication networks and systems in substation-Part 6: Configuration description language for communication in electrical substations related to IEDs[S]. 2004

[7] IEC TC57. IEC 61850-7-1, Communication networks and systems in substation-Part 7-1: Basic communication structure for substation and feeder equipment-Principles and models[S]. 2003

[8] IEC TC57. IEC 61850-7-2, Communication networks and systems in substation Part 7-2: Basic communication structure for substation and feeder equipment-Abstract communication service interface (ACSI)[S]. 2003

[9] IEC TC57. IEC 61850-7-3, Communication networks and systems in substation Part 7-3: Basic communication structure for substation and feeder equipment-Common data classes[S]. 2003

[10] IEC TC57. IEC 61850-7-4, Communication networks and systems in substation Part 7-4: Basic communication structure for substation and feeder equipment-Compatible logical node classes and data classes[S]. 2003

[11] IEC TC57. IEC 61850-8-1, Communication networks and systems in substation- Part 8-1: Specific communication service mapping(SCSM)-Mapping to MMS(ISO／IEC 9506-1 and ISO／IEC 9506-2) and to ISO／IEC 8802-3[S]. 2003

[12] IEC TC57. IEC 61850-9-1, Communication networks and systems in substation- Part 9-1: Specific communication service mapping (SCSM)-Sampled values over serial unidirectional multidrop point to point link[S]. 2003

[13] IEC TC57. IEC 61850-9-2, Communication networks and systems in substation- Part 9-2: Specific Communication service mapping (SCSM)-Sampled values over ISO／IEC 8802-3[S]. 2004

[14] ISO TC184. ISO 9506-1: Industrial Automation Systems——Manufacturing Message Specification, Part1: Service Definition[S]. 2002

[15] ISO TC184. ISO 9506-2: Industrial Automation Systems——Manufacturing Message Specification, Part2: Protocol Definition[S]. 2002

[16] ISO TC184. ISO 9506-5: Industrial Automation Systems——Manufacturing Message Specification, Companion Standard: Protocol Specification of PLC[S]. 2000