Communication and Control in Electric Power Systems: Application of Parallel and Distributed Processing
Mohammad Shahidehpour, Yaoyu Wang

ISBN: 0-471-45325-0

Chapter 3

Information System for Control Centers

3.1 INTRODUCTION

As we saw in the preceding chapters, the ISO acts as a security coordinator for the entire control area, which is made up many subareas. Individual subarea control centers perform AGC (automatic generation control) and switching operations under the direction of the ISO. The transmission system is usually owned by a group of transmission owners, and the transmission capacity is limited by the physical characteristics of the grid. With its primary mission of ensuring the reliability of the transmission system, the ISO performs a wide range of functions. The ISO ensures that all transmission customers receive non-discriminatory and equal access to the transmission system under its jurisdiction and functional control. The ISO is responsible for the coordination of energy transfers to maximize the grid utilization in a manner that maintains the integrity of the grid. Besides administering transmission tariffs, the ISO facilitates planning studies for transmission expansion and generation siting.

To fulfill all these missions, the ISO should have a custodial trust relationship with transmission owners when performing the following functions:

- Maximizing transmission service revenues
- Distributing transmission service revenues to transmission owners
- Preventing damages to the transmission grid

3.2 ICCS IN POWER SYSTEMS

Because the ISO has to perform many complicated and interrelated operations, the ISO's control center infrastructure has formed an integrated control center system (ICCS), which is essentially an integrated information system [Web01, Web07, Web10-11] and has the following fundamental requirements:

- Flexible user interfaces to the ISO to view the system information, re-dispatch resources, and monitor and coordinate the security of transmission system.
- A reliable backup system to cover the possible loss of ICCS functionalities, all the real-time functions of ICCS should remain operational in any case of significant interruption;
- A distributed computing environment with LAN and WAN such that there would be no restrictions on the geographical dispersal of applications among ICCS computers.
- An application environment with adequate flexibility and what is economical and easy to maintain and upgrade.

All ICCS applications must conform to mainstream computing standards, and data communications of ICCS must conform to OSI standards, in particular IEC 870-6 and TCP/IP (Transmission Control Protocol/Internet Protocol) protocols.

ICCS consists of many interconnected elements and processes that must function continuously and reliably. To meet the requirement for reliability, ICCS is configured as a fully redundant distributed system so that there can be no single point of failure among critical ICCS processing units (PUs). Normally the ISO carries out its functions from a primary control center that is equipped with an exactly identical backup control center; these two control centers are equipped with the same ICCS hardware/software functionality and configuration [Nie89].

The ICCS communications system is comprised of communication interfaces and communication networks. Included are ICCS LANs, the ISO's private network, the NERC's ISN (Interregional Security Network), and the public Internet. Specially designed firewalls are installed to interface between these communications networks and to provide protection from possible security threats occurring from external communication networks. Any data that are to be made public will be obtained from the information storage and retrieval (IS&R) system of ICCS via such a firewall. The IS&R system may consist of a commercial database management system for accommodating the long-term archival and retrieval of information produced by ICCS [Web01, Web10-14].

In this chapter we will discuss the configuration and services of ICCS including electronic tagging services, and the utilization of UCA (utility communications architecture) and ICCP (inter-control-center communication protocol) by ICCS [Rob95].

3.3 ICCS CONFIGURATION

3.3.1 ICCS LAN

Recall that the ICCS is a distributed system based on LAN. Various sophisticated ICCS applications are logically integrated on this LAN, which consists of a number of PUs dedicated to particular functions. Industry standards are used for the design and implementation of ICCS hardware, software, and user interfaces to ensure interoperability and software portability. This open architecture allows the addition of future functionality and the replacement of hardware without disruption to the initial ICCS. The LAN for this application comprises two parts: LAN for ICCS applications, which is called the ICCS LAN, and LAN for ICCS administration, which is called the ICCS administration LAN. The general architecture of ICCS LANs is depicted in Figure 3.1 [Dyl94, Bla90, Bri91].

As shown in Figure 3.1, an ICCS LAN adopts a redundant structure that consists of a primary LAN and a backup secondary LAN. Each PU is connected to these two LANs at the same time. Obviously this configuration provides a capability for meeting the specified availability and reliability in a cost-effective manner. The ICCS LAN is connected to the ISO's administrative LAN via a firewall to isolate ICCS from the administration systems LAN. The firewall provides the protection from possible security threats occurring at the administration system LAN. Various suitable user interfaces are provided for ISO operators to use ICCS for viewing the power system information, to re-dispatch resources, and to monitor and coordinate the security of power systems.

The ICCS function will be transferred automatically from a failed PU to an alternative PU as a failure occurs. Certain failure logic is applied to all PUs in ICCS. Each PU is at least monitored by another PU, configuration management software, or dedicated hardware so that appropriate actions are activated as necessary. Dedicated detection mechanisms are employed to detect software and hardware failures throughout the entire ICCS and are used to supervise the whole process of switching functions from a failed PU to a backup PU [Sko02].

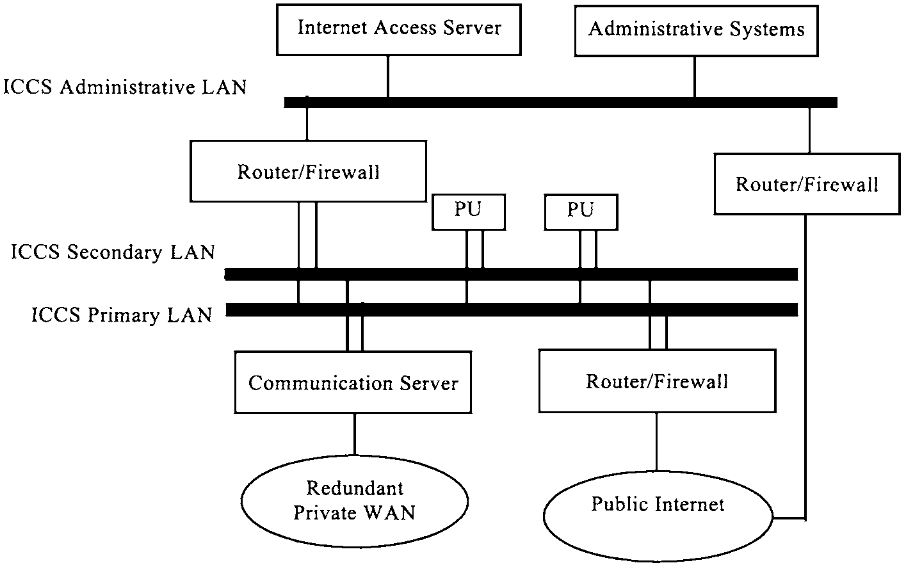


Figure 3.1 Architecture of ICCS LANs

In the case of a LAN failure, the LAN functions will be automatically transferred to an alternative LAN. The probability of two simultaneous LAN failures is very small but when it happens, ICCS functions at the ISO's primary control site can be entirely transferred to the ICCS at the ISO's backup site. Functions of any failed communication server would automatically be transferred to another available communication server. Likewise functions of any failed peripheral will be automatically transferred to another available peripheral. Any transfer will set off an alarm that announces a function transfer.

3.3.2 Availability and Redundancy of ICCS

The ability of each ICCS component to perform its specific tasks under normal conditions and during hardware and software failures is of paramount importance to the ISO. Hence, sufficient redundancy is introduced in ICCS to guarantee that any single failure would only cause a brief interruption in the availability of that function. A functional processing interrupted by a failure would automatically be taken over by an alternative processor. Functional transfers are completed automatically and without any loss of data. Functions that were previously scheduled to be executed during a functional transfer would automatically be executed right after the completion of transfer.

A suitable redundancy should be provided at ICCS to prevent the loss of any critical ISO functionality. One design option indicates that the ISO could carry out its mission using a primary control center and a backup control center that are located remotely from each other. These two control centers have the same ICCS hardware and software functionality and configuration. The backup ICCS is provided to cover those situations where the loss of ICCS functionality could occur and last for an extended period of time. ICCS is configured as a single fully redundant distributed system so that there is no single point of failure among the critical ICCS PUs. Normally the ISO operates from the primary control center, which is continuously connected with an exactly identical backup control center. The primary ISO periodically checks the condition of the backup ICCS and keeps it initialized.

The backup ICCS is required to be in a ready condition without the need for on-site personnel while in the standby mode. In contingencies the backup ICCS is required to take over the entire functionality of the primary ICCS within a fraction of a minute. Once the primary ISO is ready to return to its normal service, it is initialized from the backup ICCS in order to reflect the current state of the power system. For a short period of time, both the primary and the backup ICCS need to operate in parallel as functionality is transferred back to the primary ICCS.

Redundancy for reliability is achieved both locally at each site and between the sites, as shown in Figure 3.2. ICCS LANs at each site are connected by a wide-band WAN communication link for coordinating the primary and backup sites. Although this link could be thousands of miles long and routers or bridges are installed at both terminals of the link, the LANs appear to ICCS as a single local redundant LAN for all ICCS processors.

For the sake of software reliability, ICCS applications data have a backup version that can be automatically brought up as part of a restart or transfer procedure. If a hot start-up is required, the start-up procedure will detect whether any data entry was lost and then notify users of the need for re-entry of the data. The hot start-up procedure will also detect whether any program-generated transaction was lost and when necessary will automatically initiate the recovery procedure to maintain application integrity [Web04-14].

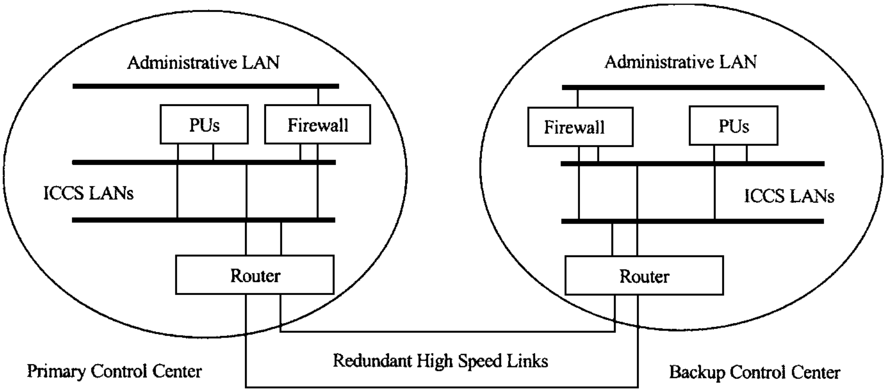


Figure 3.2 Redundant Structure of ICCS

3.4 INFORMATION SYSTEM FOR ICCS

The functional configuration of ICCS makes the ICCS to be a centralized information system that has the following features:

- Communication interfaces with a suitable firewall protection: these connect to external computer systems and services.
- Processor/server interfaces via a LAN: this interconnects various application functions.
- User interfaces: these consist of workstations, PCs and a rear projection video display matrix.
- Peripheral support facilities: these include telephones, printers, copiers, and fax machines.

As demonstrated in Figure 3.3, the ISO's functions are part of ICCS functions. The ICCS has the following major functions:

- Interfaces to communication networks connected to the ISO
- Communication services to collect and send information

- Data exchange and processing of information between the ISO and its participants
- Communications between the primary and the backup control centers
- Data models and databases for ICCS application functions.
- Information storage and retrieval applications used by other applications to create records of important information and to find and retrieve that information for use by ICCS applications, displays, and reports [Web10-11].

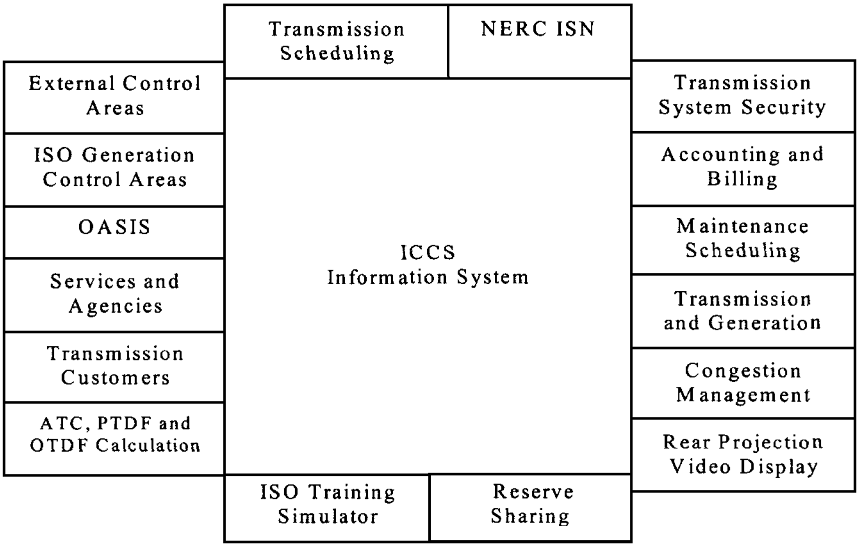


Figure 3.3 ICCS Functional Configuration

3.5 CCAPI FOR ICCS

ICCS users interact with ICCS through applications of executables, local datasets, and public datasets. Local data are private to a particular application and not a concern in plug-in interfaces. For the integration of ICCS applications, what matters is the way an executable in one application accesses another application's public data, or the way an executable exchanges messages with an executable in another application. In general, as defined in CCAPI (Control Center Application Program Interface [EPR96]), a runtime application space has a reference model as depicted in Figure 3.4.

There are two kinds of interfaces for applications to exchange information: message bus interface and data access interface. The message bus interface is a general message-passing interface that is used for program-to-program exchanges. The data access interface provides shared access to public data entities and is mainly used for program to dataset exchanges. Based on the model for a run-time application space, a CCAPI reference model for ICCS is depicted in Figure 3.5 [EPR96, Web04, Web07, Web10].

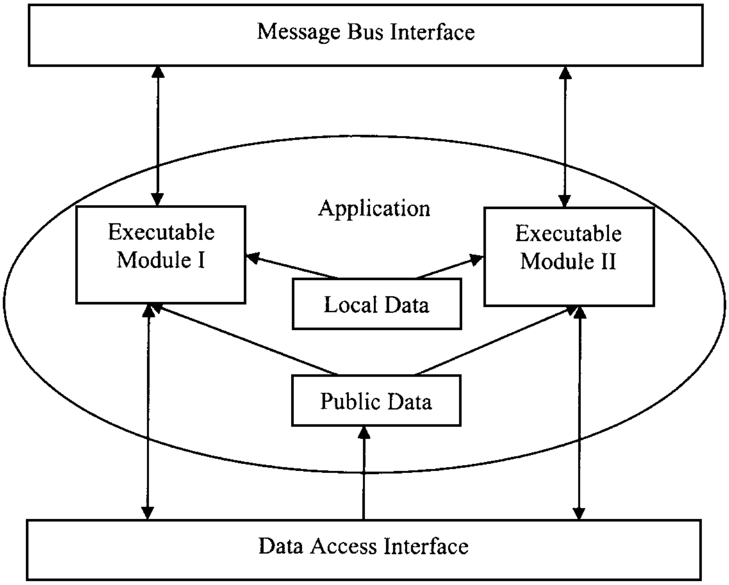


Figure 3.4 Model for Run-time Application Space

3.6 INTERFACES FOR ICCS USERS

Because ICCS is an integrated and centralized information system, ICCS users almost comprise all entities of a restructured power system, which include the ISO operators at the ISO's primary and backup control centers, transmission owners, transmission customers, and other users as shown in Figure 3.6. There are four departments of ISO, as shown in Figure 3.7, that are the major ICCS users. The respective functions of these departments are discussed next [Web10-14].

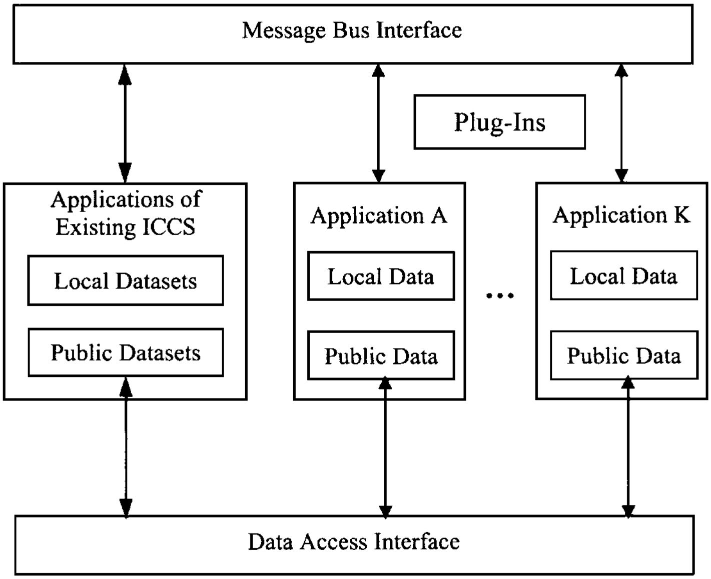


Figure 3.5 CCAPI Reference Model for ICCS

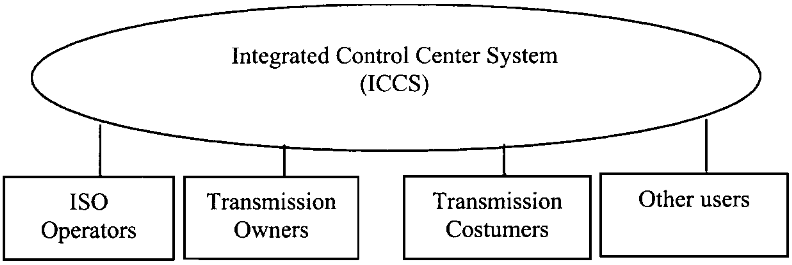


Figure 3.6 ICCS Users

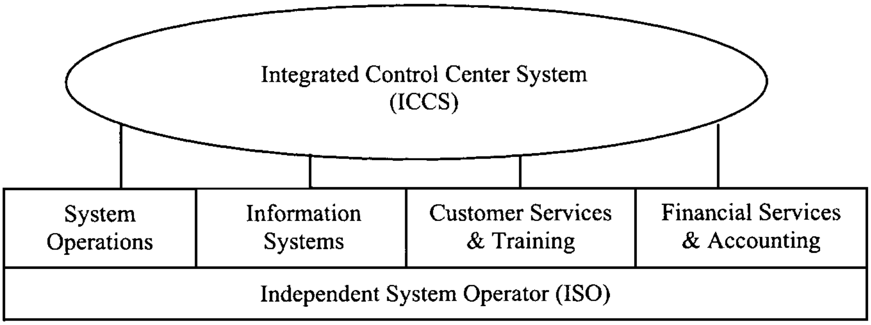

Integrated Control Center System
(ICCS)
System Operations
Information Systems
Customer Services & Training
Financial Services & Accounting
Independent System Operator (ISO)

Figure 3.7 ISO Departments Related to ICCS Activities

- **Interfaces to System Operations.** The system operations department is responsible for the real-time administration of the ISO tariff, security coordination, scheduling and coordination of control area generation, operations support, transmission operational planning, and other operations engineering activities. Tasks to be fulfilled by this department mainly include real-time database maintenance and applications, technical operations, accounting and billing, communications, and hardware and software platform support.

- **Interfaces to Information System.** The information system department is responsible for all computer infrastructure activities, including application programming, data models, user interface, communications programming, and computer and communications hardware, as shown in Figure 3.8. Basic functions that information systems would provide include interfaces to communication networks connected to the ISO control center, communication services to collect information from and send information to various sources, data exchange and processing of information between the ISO and its participants, communications between the primary control center and the backup control center, and data models and databases to be used by the ICCS application functions.

- **Interfaces to Customer Services and Training.** The customer services and training department deals with customers for scheduling coordination, billing, and settlement questions, and providing information to loads and suppliers. It also provides training function for the ISO staff and for customers. The main functions are as follows: administer and register transmission customer applications for the ISO services, prepare procedure manuals for transmission customers, conduct transmission customer training, conduct the ISO staff training, coordinate meetings, coordinate transmission customer dispute resolution, and monitor the power market.

- **Interfaces to Financial Services and Accounting.** The financial services and accounting department handles the bookkeeping, billing, settlements, and accounting functions of the ISO. It mainly has the following functions: define the processes and procedures for transmission service settlement, define algorithms and formulas for accounting and billing, prepare transmission customers' invoices, administer electronic transfers of funds, and administer the ISO's business accounting and billing.

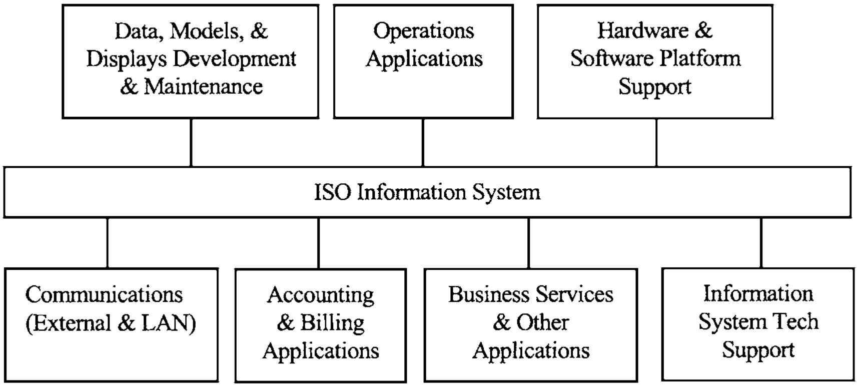

Data, Models, & Displays Development & Maintenance
Operations Applications
Hardware & Software Platform Support
ISO Information System
Communications (External & LAN)
Accounting & Billing Applications
Business Services & Other Applications
Information System Tech Support

Figure 3.8 ISO Information System Functions

The latest graphics display standards are adopted for user interfaces in all ICCS functions. User interfaces and activities are normally accomplished through window, tool bar, menu, and icon operations using a mouse and keyboard. For convenience, consistent graphics standards are applied to all displays. To let the data with similar appearances have a consistent interpretation throughout ICCS, each function should be consistent in its use of graphics, commands, menus, colors, point and click procedures, and data entry.

In addition to the user interfaces discussed above, appropriate hardware and software are provided for ICCS to interface with other facilities including OASIS, time synchronization, and satellite communications backup, among other telecommunications services. The OASIS node of ICCS would meet FERC Standards and Communications Protocols (S&CP), and utilize both the public Internet and the ISO private intranet to interface with transmission customers. In other words, transmission customers can choose to use the public Internet or the ISO's private intranet to conduct business on OASIS, which requires the ICCS to support identical applications running over both the public Internet and the private intranet. Besides, interfaces to other communications service applications such as public telephone, NERC hotline, fax, weather services, voice recorder for system operations, and accounting and billing with the capability to e-mail conversations are also provided.

3.7 ICCS COMMUNICATION NETWORKS

The ISO provides the necessary components for ICCS communications infrastructure. In addition to ICCS LANs discussed in Section 3.1, the ISO would mainly use the following three types of computer networks to support various communication functions and services of ICCS:

- ISO's private WAN
- The public Internet
- NERC's interregional security network

These three networks are WAN computer networks. This section provides a general overview of the relationship between these three supporting communication networks and the corresponding ICCS functions [Web10-12, Web14].

3.7.1 Private WAN of the ISO

The ISO's infrastructure includes a private WAN that is dedicated to the ISO's participants. This network is primarily used for exchanging the data between ICCS and transmission owner control centers and serving the ISO's transmission customers. This private network is particularly built to interconnect the ISO's control center and all its member control centers which are irregularly distributed in the ISO's control territory. As part of this private network, a wideband link is utilized to connect the ISO's primary control center and the backup site. From the viewpoint of the ISO, this private network is a kind of intranet. All the ISO members' control centers would have access to this private intranet. Though it is also available to transmission customers, power exchanges, and regional reliability councils, this private intranet is principally used for data exchange between ICCS and the ISO members' control centers.

The structure of the private intranet can be of any form determined by the ISO according to its specific relation with its member control centers. Because the ISO members' control centers are usually irregularly distributed in power systems, and interconnected by different communication links, the structure of the ISO's private intranet can be quite irregular. Figure 3.9 shows a possible star type of structure for the ISO's private intranet. The reliability of the computer system in Figure 3.9 is often enhanced by a mirrored architecture across the two centers. This is analogous to the reliability of the ISO's private intranet, which consists of two separate networks: the primary WAN and the secondary WAN. This redundant configuration is illustrated in Figure 3.10.

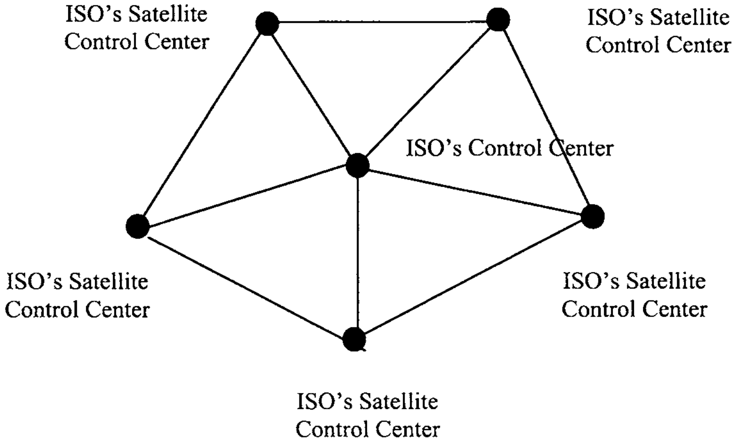

ISO's Satellite Control Center
ISO's Satellite Control Center
ISO's Control Center
ISO's Satellite Control Center
ISO's Satellite Control Center
ISO's Satellite Control Center

Figure 3.9 Architecture of the ISO's Private WAN

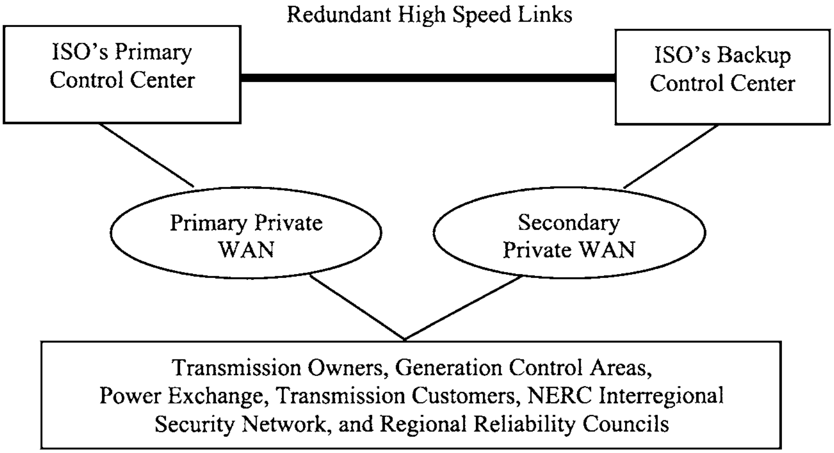

Redundant High Speed Links
ISO's Primary Control Center
ISO's Backup Control Center
Primary Private WAN
Secondary Private WAN
Transmission Owners, Generation Control Areas, Power Exchange, Transmission Customers, NERC Interregional Security Network, and Regional Reliability Councils

Figure 3.10 Redundant ISO Intranet Configurations

Normally the primary WAN is connected to the primary ISO's site and the secondary WAN is connected to the backup ISO's site. ICCS supports an access to redundant WANs from either the primary or the backup ISO's sites, regardless of the location of system operators or active PUs. A PU located at the primary ISO's site would have access to the communication server connected to the secondary WAN if the primary communication server fails or the primary WAN becomes unavailable, and vice versa. The two ISO's control centers coordinate their operations to ensure that at any time one site could operate in the primary mode, and the other in the backup mode. The same criterion applies to any operating PU and its complementary PU at each control center [Raj94].

Extensive data exchange would take place between the ICCS and the ISO members' control centers. An ICCP is used for ICCS to support the system monitoring and transaction processing [Eri97, Rob95, Vaa01]. Traditional real-time data are exchanged between the ISO and its members' control centers; these data are also accumulated for the historical storage, planning, and analysis. General messaging applications such as messaging communications, curtailment instructions, and dispatch requests are supported by this private intranet. Functions for file transfers are also supported, since common Internet applications such as Web servers, FTP servers, and e-mail servers are implemented over this private intranet. Likewise the dissemination of accounting information and time-related schedules such as planned generation schedules, transaction schedules, and ancillary service commitment schedules are supported.

3.7.2 NERC's Interregional Security Network

The NERC's interregional security network (ISN) is used for the ISO's communications with other NERC security coordinators, external control areas, and ISOs. As required by NERC orders, an ISO must be able to quickly and reliably communicate with neighboring security coordinators. The ISO has access to the NERC ISN for the purpose of meeting the NERC security coordinator requirements. The protocol used for ISN access is ICCP, which will not be used for peer-to-peer communication among transmission owners or between transmission owners and the ISO. The data exchange between the ISO and other security coordinators would support system security applications. When necessary, the ISO can also communicate with external control areas via the NERC ISN [Web11].

The ISO accesses the NERC ISN to collect real-time data from external control areas and to provide real-time data to other NERC security coordinators and external control areas. In many cases System Data Exchange (SDX) is also used to provide data exchange between the ISO and other security coordinators.

Figure 3.11 provides general diagram that shows how the three communications networks discussed above are interrelated and how they interface with the network users. The dotted communication lines between the ISO's private WAN and the power exchange, regional reliability councils (RRCs) and transmission customers point out that these communication links are optional, because they can normally access the ISO through the public Internet.

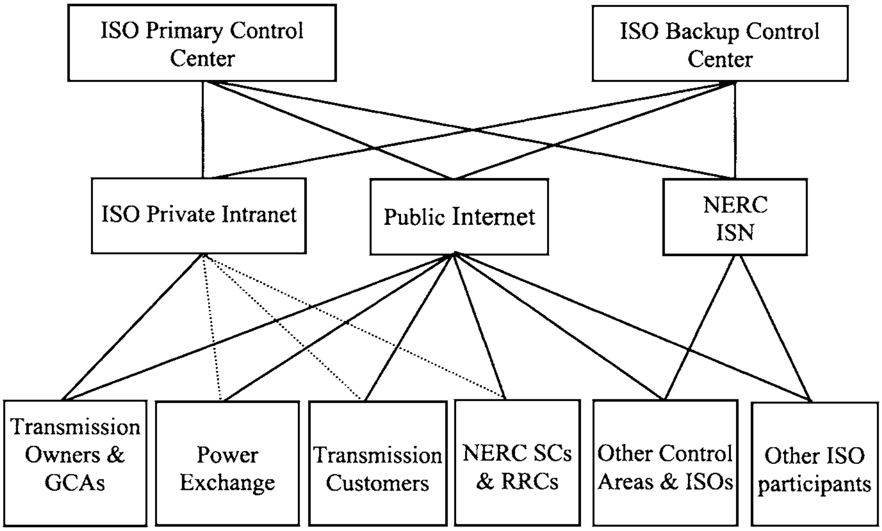


Figure 3.11 ICCS Communications Networks

3.7.3 Public Internet

The public Internet is the most common tool for the ISO to communicate with power market participants and OASIS. As a kind of public utility, the public Internet can be accessed by anyone who has been given an appropriate access authorization. For security reasons, suitable firewalls are built to prevent any unauthorized access to the ISO's control center via the Internet.

The ISO provides access for its member using both a private intranet as well as the public Internet. All services that are implemented on the ISO private intranet, including ICCP communications, are also made available over the Internet using the same communication and data processing applications. In addition to supporting access for its members to ICCS core services via the Internet connections, the ISO uses the Internet for more traditional administrative applications such as accessing Web sites, exchanging e-mails with non-member organizations, and downloading data files using FTP. However, consoles on the ICCS LAN and workstations on the administrative LAN will require the Internet applications for the completion of their daily functions and services.

Generally, transmission customers can access the ISO either via the ISO's private network or via the public Internet. Transmission owners and generation control areas normally access the ISO via the ISO's private intranet, but in the event that private intranet is not available, the communication will be via the public Internet. This switching process is quite automatic as identical software tools and services are provided by the ICCS for users to operate on these two networks.

3.8 ICCS TIME SYNCHRONIZATION

Since the concept of time is most critical to the ISO, satellite control centers, and power market participants, the system time at either the ISO control center or its satellite control centers is maintained locally using global position system (GPS) timeservers. ICCS is equipped with a time facility to determine the universal coordinated time (UCT), which is obtained from the global positioning system (GPS) satellite constellation. The ICCS is able to correctly interpret and distribute time stamps on time-sensitive data regardless of the local time zones to which the data applies.

Specifically, the ICCS time synchronization includes computer time synchronization, network time synchronization and OASIS time synchronization as discussed next [Web07, Web10-14].

- **Computer time synchronization.** Each of ICCS computers maintains a common internal calendar and 24-hour clock time. All applications on any of these computers are required to take into account any time-related issues such as local date and time that are shown on all displays and reports. When necessary, a single point adjustment is performed to keep the time synchronized.

- **Network time synchronization.** The ICCS network time is maintained for all component elements of ICCS. Distributed time services are used for synchronization among computers in the ICCS network. Every computer on the network periodically synchronizes to the time server, and all network computer clocks are automatically synchronized to within one microsecond of the time standard. When the time synchronization service is unavailable, the users can manually update the computer clock through the user interface. If a computer's internal clock and the time standard differ by more than an adjustable amount, an alarm message will be set off to inform the operator.

- **OASIS time synchronization.** The OASIS time synchronization is implemented by using the network time protocol (NTP) or by using other standard time signals such as GPS. Through time synchronization, the time stamps of all transactions on the same OASIS node can be accurate to within ± 0.5 seconds of the standard time.

3.9 UTILITY COMMUNICATIONS ARCHITECTURE

The integration of various power system applications was extremely complicated and costly because individual power system commercial software vendors had designed proprietary communications systems for their own products. To solve the problem of by providing a standard communications architecture for both electric utilities and vendors, in the late 1980s, EPRI initiated a project called Integrated Utility Communications (IUC) as a first step toward creating the necessary industry standards. The Utility Communications Architecture (UCA) is one of the IUC activities.

The objective behind the UCA effort was to build an information architecture that could meet the communication needs of electric utilities. At the beginning, UCA was used to clarify the types of information that electric utilities would need to communicate and the ways they would communicate; as these issues were resolved, UCA could be used to identify the types of protocol that utilities would use to perform these functions.

The long-term goal of UCA is to build an architecture that has vendor-independent communication tools, easily expandable services, and enterprise-wide access to the real-time information. To avoid the development of a utility-specific communication protocol, UCA has incorporated several existing international standards and technologies. Since no single transport protocol is perfect for all applications, UCA provides several protocols within communication layers from which vendors and integrators can choose to suit their different applications. A manufacturing message specifications (MMS) protocol serves as the application protocol for all applications [IEEE01].

UCA represents several advantages for utility operations. First, UCA facilitates integrations and allows utilities to choose the best-in-class equipment for their specific tasks. Second, UCA facilitates the use of distributed measurement, control, and communication schemes, and thus provides an alternative to all-in-one-box solution that usually provides more functionality than necessary. For instance, when a traditional EMS is replaced by an OFDEMS (open functional distributed EMS) [Wang97], which has several computers on a LAN, feasible EMS applications would increase. Moreover, if the LAN is fast enough, the distributed processing of OFDEMS applications would be practical. Third, depending on the communication specifications on a WAN, UCA can allow users' access to real-time data for certain functions. Thus system operators, planners, power brokers, and finance personnel can all benefit from the availability of the real-time information [EPR96].

3.9.1 Communication Scheme

The data communication in UCA is based on the seven-layer model of the OSI, which is a general model for network communication developed by the International Standards Organization. This model shown in Figure 3.12 is composed of seven separate layers with distinct functionalities.

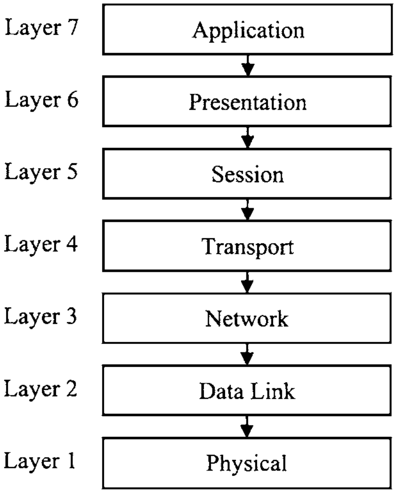


Figure 3.12 OSI Seven-Layer Model

More specifically, the OSI stack of seven layers is grouped into the following three sets of profiles:

- **A-Profiles.** Including application, presentation and session layers, which decide on the information packaging and format. In the presentation and session layers some necessary tags are added to the data that will be recognized by the communication protocol at the receiving end.

- **T-Profiles.** Including transport and network layers. The transport layer ensures a reliable message transfers across the network, and the network layer provides addressing and routing functions to allow the connection of multiple network segments to larger networks.

- **L-Profiles.** Including the last two layers of the stack, namely data-link and physical layers. The data-link layer controls the access to the network media, and the physical layer specifies wires, voltages, connectors, and other physical attributes of the system.

In the communication process, this seven-layer model will function as follows: At the sending end, the data generated from certain processes enter the application layer first, proceed through all layers to layer one, and then traverse across communication links to the receiving end. At the receiving end, the data make its way up through all the seven layers.

This seven-layer OSI model has been used for various networking schemes, such as TCP/IP, Microsoft, Novell, DNP, and UCA. Because of the prevalence of the Internet, most routers and gateways on networks are usually set up to deal with TCP/IP rather than OSI. TCP/IP was originally designed to transport data streams from one point or one application to another. Because TCP/IP streams use timers to detect the end of the data stream, TCP/IP may sit idle for a short while in awaiting the arrival of additional data. These time lags may be unacceptable for many time-critical functions of electric utilities. The OSI stacks are oriented toward packets rather than streams. These packets have a clear beginning and end signals. If a client receives an incomplete packet, it will be simply discarded and a new one may be requested at the same time. Hence, a client will not sit idle while awaiting the rest of the information. For this reason, OSI suits time-critical communications better than the TCP/IP.

The UCA component communication is illustrated in Figure 3.13, where the WAN could be the ISO's private WAN, the NERC ISN, or the public Internet. Every component could have a LAN as shown in Figure 3.14 [EPR96, Vaa01].

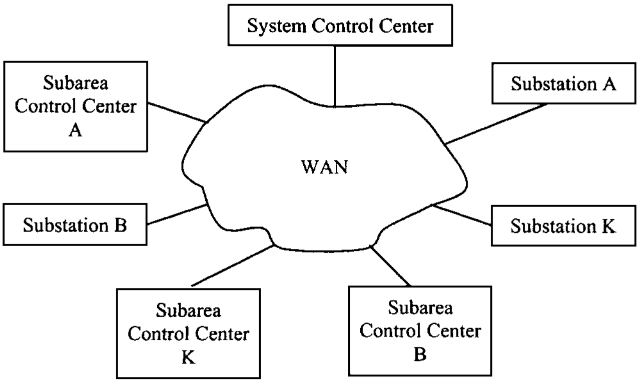
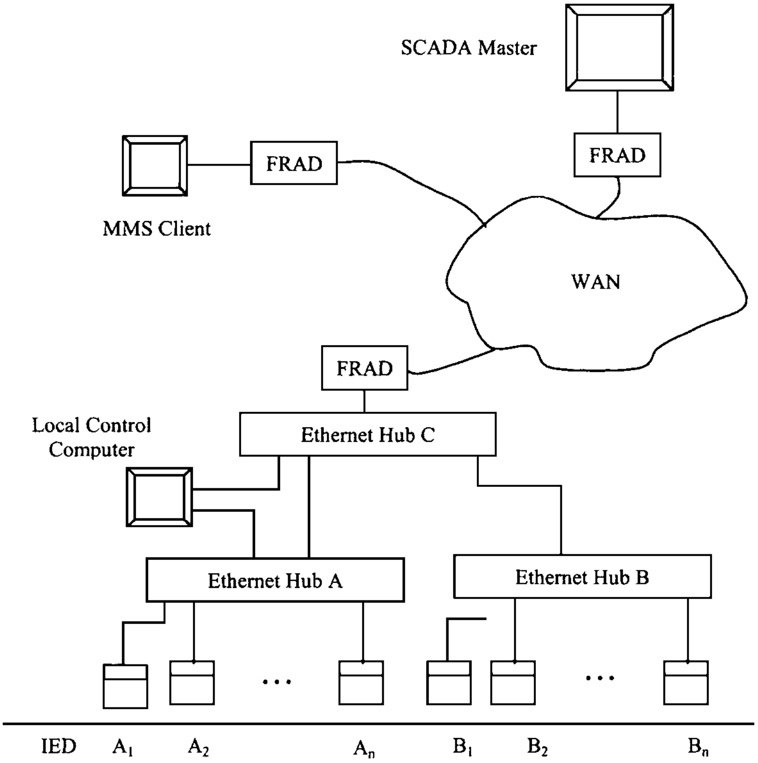


Figure 3.13 UCA Component Communications



FRAD: Frame Relay Access Device
IED: intelligent electronic device

Figure 3.14 Conceptual LAN of UCA

3.9.2 Fundamental Components

UCA has four major components: manufacturing message specifications (MMS), common application service model (CASM), generic object models for substation and feeder equipment (GOMSFE) and ICCP [EPR96, EPR01a]. All are described in this section.

MMS. is an internationally standardized messaging system as defined in the International Organization for Standardization 9506. It is the application-level messaging protocol which is used for real-time data exchange applications; it is also applied to a real-time networked data exchange and supervisory control. MMS is very robust and has the capacity to perform functions that are requested by utilities. As a top-level application in the seven-layer data communication model, MMS is independent of transport layers that are located below it. No matter what networking protocols are used, one UCA compliant device always provides MMS at the application level to other devices on the network, which makes the integration of network components much simpler. Therefore, MMS has emerged as a protocol for implementing the UCA functionality. Whereas UCA was concerned with identifying functions that utilities would like to perform, the UCA 2.0 version is more concerned with methods and languages that allow devices from different vendors to work together in an electric utility substation.

CASM. gives the details of the processes that a communication service must follow within UCA, and defines these within the step-by-step logic flow of UCA operations. CASM does not specify protocols for executing services and thus is independent of any protocol. UCA maps services to MMS when it needs to perform actions specified in CASM.

GOMSFE. defines information categories, hierarchy, and naming conventions for the electric utility substation, and it therefore serves as a dictionary of names for equipment and functions within a substation. An IED (intelligent electronic device) in a substation will have all of its data and functions available to respond to these names. For data to be viewed, the location of the data within the organizational hierarchy of GOMSFE must be provided. The data in UCA is set up in a series of groupings like file folders. The names of these folders and their information are listed as follows:

- Remote terminal unit
- Measurement unit

- Load tap changer controller
- Capacitor bank controller
- Switch controller
- Automated switch controller
- Circuit breaker controller
- Re-closer controller
- Bay controller
- Power monitor
- Distribution feeder protection and control
- 138 kV transmission line protection and control
- 345 kV transmission line protection and control

The hierarchy of data proceeds from the top application level of the seven-layer data communication model. Any protocol functioning in this layer must be able to handle this organizational structure and services. The basic organizational scheme can be described as follows: Say the voltage VBX of bus X is required for a commercial application. A device with a unique alphanumeric code should exist on the network with a domain like Power_server5 within this device. There would be a set of information like MVM within this domain, within MVM there would be another level of classification such as MVMX, and within MVMX there could be another level such as MVMY. Suppose that VBX is within MVMY, then VBA can be accessed at the following address:

Domain = Power_server5
Object Name = MVM$MVMX$MVMY$VBX

GOMSFE also defines the way information will be provided. For a voltage measurement, a device can provide it as an integer or a floating-point value in the appropriate unit and format. The domain name is used here instead of the physical address of the device. There could be multiple domains at one physical address, as this allows a user to create several logical devices within one physical device on the network.

ICCP. specifies database-oriented communication methods within UCA. It is particularly designed for data communication between power system control centers. ICCP is known as IEC60870-6 TASE.2 (Telecontrol Application Service Element Number 2) [Eri97]. ICCP provides methods for the data transfer between utility control centers and defines UCA services in terms of MMS in the application layer. ICCP uses neither CASM nor GOMSFE. Compared with CASM and GOMSFE, which deal with data in a device-centric view, ICCP defines the data similar to those in a SCADA system. ICCP is defined in terms of the client-server model of ISO/IEC 9506, and is modeled as one or more processes operating as a logical entity that perform certain communications [Gre92]. For example, for a model of a control center that includes several different classes of applications such as SCADA/EMS, DSM/load management, distributed application, and man/machine interface, the logical relationships of ICCP to the control center applications is that depicted by Figure 3.15.

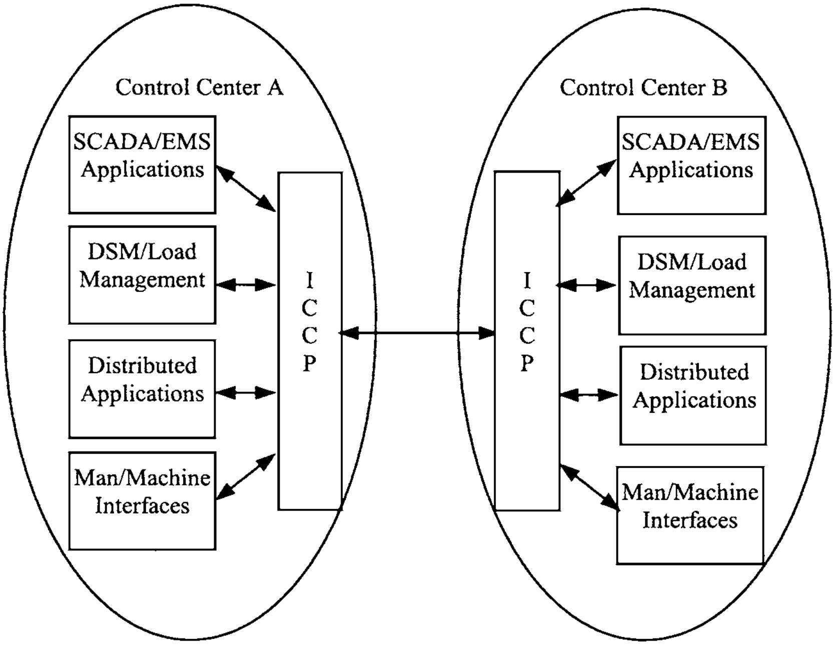


Figure 3.15 Relationship between ICCP and Control Centers

3.9.3 Interoperability

Previously one vendor could place bus X's voltage VBX in a register named XXXX when implementing DNP; other devices on the network such as RTU and PLC would need to be programmed with the location of this information. When a new vendor's product that uses the register YYYY to place voltage VBX of bus X is added to the network, all PLC, RTU, and the like, must be reprogrammed. There is no interoperability in this situation, since extensive changes have to be made to the existing system for each new device. Now with UCA 2.0 the integration of various products from different vendors becomes much easier. UCA solves this interoperability problem in the product design phase by applying many new integration-friendly concepts [EPR96, Web10-14].

Instead of specifying a register name for the VBX voltage of bus X, a variable named MVM$MVMX$MVMY$VBX is used for all devices on the network. Since every device refers to the data in the same way, reprogramming becomes unnecessary after a new vendor's product has been added. A UCA client can extract a list of self-describing objects from the server that it is trying to access; these objects detail the information and services the server can provide or perform, and thus reduce the need to specify how the clients should interact with servers. On the other hand, because of the separation of T-profiles from A-Profiles, a UCA client can be developed independently of the precise T-profile used. This implies that the client can access a device in the exact same manner because the difference in the T-profile is isolated from the application. UCA 2.0, CASM, and GOMSFE allow for more functions to be implemented in a standardized manner rather than just registering the exchanged value. Because MMS is the common language for all applications, new instructions for each involved device do not need to be translated, although instructions on how to use the new services would need to be provided. Moreover, the protocols used within UCA are international standards. They are well established and defined, and they benefit from economies of scale and a common knowledge base. Moreover the self-describing services of UCA greatly simplify the communication among devices.

EPRI and electric utilities sponsored a number of meetings where vendors of UCA compliant devices interoperated on an Ethernet LAN. For instance, the AEP LAN Substation Demonstration Initiative was a UCA proof-of-concept program centered on the substation. AEP installed a unified power flow controller (UFPC) at its Inez 765 kV station and utilized the UFPC to handle communication between the Inez station, six remote stations, area dispatching, and the corporate office [Edri98]. The communication medium was 10 Mbps Ethernet on a switched hub or 100 Mbps on a shared hub. To ensure timely response to control commands, a priority mechanism was implemented to give Inez LAN traffic the highest priority at each routing node on the AEP system WAN.

3.10 ICCS COMMUNICATIONS SERVICES

ICCS provides various communications services to support data exchange applications. Figure 3.16 shows the services used by participants to communicate with ICCS [EPR96, EPR01b, Cau96, Web10-14].

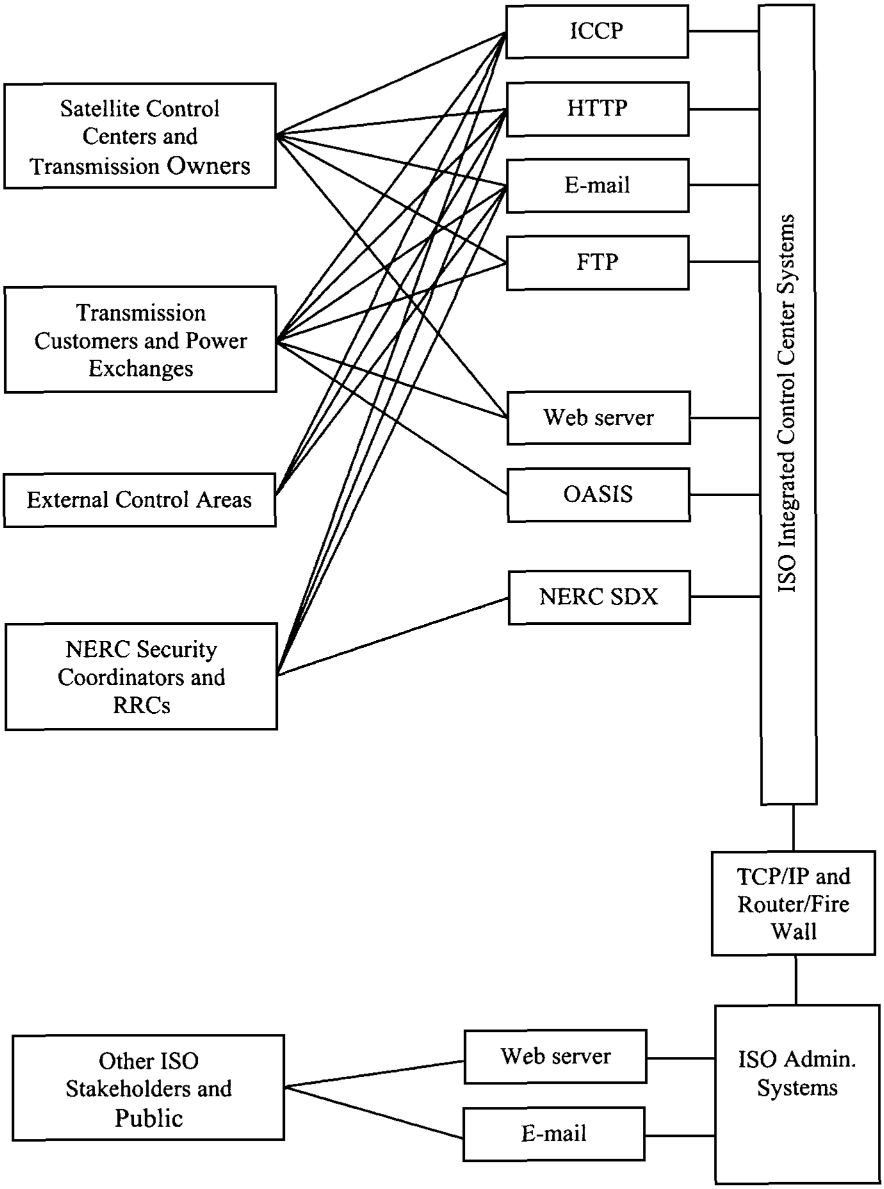

ICCP
HTTP
E-mail
FTP
Web server
OASIS
NERC SDX
Satellite Control Centers and Transmission Owners
Transmission Customers and Power Exchanges
External Control Areas
NERC Security Coordinators and RRCs
ISO Integrated Control Center Systems
TCP/IP and Router/Fire Wall
Other ISO Stakeholders and Public
Web server
E-mail
ISO Admin. Systems

Figure 3.16 ICCS Communications Services

One of the main objectives of these communications services is to ensure the interoperability across computing platforms as ICCS, transmission owners and transmission customers usually operate on different computing platforms. Moreover, a group of application interfaces that are necessary to automate the data exchange process are provided. The applications of each service are discussed next.

ICCP. As a special communication protocol, ICCP is mainly used to support data exchanges composed of values associated with fixed time increments. Practically, ICCP is used for a real-time data exchange between ICCS and transmission owners and satellite control centers, external control areas and other entities, as illustrated in Figure 3.8. ICCP can also support certain messaging types of applications.

TCP/IP. As a popular industry standard protocol for data transmission among computer sites, TCP/IP is also used as the communications service standard for ICCS and information systems LANs. A dedicated addressing domain is used for the communication services including, FTP, Web services, e-mail, and ICCP among other special communication services.

HTTP. As a support for information distribution, HTTP based on WWW servers is installed on ICCS LANs. HTTP functionalities are included in Web server tools. All activities occurring on Web servers, including data snapshots, are date and time stamped. The Web support tools also interpret HTML, and thus ensure the interoperability among heterogeneous systems in a network.

E-mail. As a convenient tool for users to send and receive messages at different sites of the public Internet, e-mail services are provided by ICCS for all ICCS users. Usually the SMTP and POP3 are implemented to provide mail-handling services for all e-mail clients. Auditable e-mail is provided as a means by which a process is initiated, tracked and archived. Both functions belong to non-interactive messaging and thus can take advantage of many existing standard software packages.

FTP. As a standard Internet protocol for data exchange among computer sites, FTP is used for the exchange of data both into and out of ICCS. ICCS can receive data files from user sites by downloading or being uploaded using FTP. ICCS users can receive data files similarly from ICCS. The privacy of FTP data exchanges is ensured by providing the necessary security measures like the user authorization password.

NERC SDX. The NERC SDX is developed for data exchange between ICCS FTP and NERC FTP sites via the Internet. NERC SDX also provides the mechanism for retrieving data files from NERC for the calculation of ATCs and PTDFs. NERC SDX provides the means for security coordinators to enter data on the peak load information; net exports and imports; operating reserves; and generation and transmission outages.

OASIS. OASIS is the communications system used by the power industry for the coordination of transmission services over the public Internet. All businesses associated with transmission services are conducted on OASIS nodes. ICCS LAN has a special node for OASIS. The OASIS input system provides pre-validated re-dispatch and ancillary service bids, as well as generator parameters and other information to ICCS. ICCS also provides some information to OASIS which includes ancillary service commitments and other data needed to support transmission service functions and participant information requirements.

3.10.1 Other Communication Services

Certain ICCS messages, which must be acknowledged and audited by the recipient, use ICCP to transfer messages other control centers. The messaging applications include: control functions, generation re-dispatch, voltage schedules, transmission loading relief, and the ISO's reserve sharing. The messaging process consists of the following steps:

- An instructive message is sent from the ISO to a designated satellite control center.
- The designated satellite control center confirms the receipt of the message from the ISO by sending confirmation back to the ISO.
- Messages involved in the first two steps are structured to allow intelligent processing and analysis. For instance, any error in the transaction process will generate alarms at the sending site.

3.11 ICCS DATA EXCHANGE AND PROCESSING

ICCS provides a group of functions for data exchange and processing. This section will discuss how these functions are realized by utilizing the data communication services discussed above.

3.11.1 Real-Time Data Processing

Through ICCP, power system real-time data can be transmitted from transmission owners' computers to ICCS. These real-time data include but not limited to the following [Cau96, Web01, Web10-14]:

- 2-second status data
- 5-minute status data
- 10-second analog data
- 60-second analog data
- 15 minute, 30 minute, and hourly digital data
- On-demand digital data.

In the SCADA system, the 2-second status data are reported by exception, and 5-minute status data and all digital data are transmitted within a predetermined time window. Usually every five minutes, the ISO prepares and deposits a file containing the results of the state estimation for each transmission owner and other NERC security coordinators. The file appropriate to each transmission owner is placed in the transmission owner's designated directory following the execution of state estimation. ICCS sends the data via ICCP to transmission owners and other entities that are connected to the ISO's private network. Data formats conversion applications will be invoked if the format of the incoming data is different from that of the local database. A network status processing application detects abnormal circuit conditions by automatically analyzing the network model database. Usually every five minutes, the ISO prepares and deposits a file containing the results of the state estimation for each transmission owner and other NERC security coordinators.

3.11.2 Transaction Scheduling and Processing

Transmission customers post their service requests to the OASIS Web server, and within a predetermined time limit, service confirmations will be published on the same OASIS Web server by the ISO. All of these requests and confirmations are accessible by transmission customers, whether they were issued over the public Internet or the ISO private network. ICCS uses a directory structure and a file naming convention to identify each schedule and its time association. Schedule files are sent to the ISO's FTP site according to the directory structure and file-naming convention, and at the same time an e-mail message will be sent to notify ICCS that the schedule has been deposited at the ISO's FTP site. Transmission owners must also send their maintenance schedules to the ICCS for approval. These transactions use the standard FTP with auditable e-mail techniques. Requests for ancillary services are also posted to the OASIS Web server by transmission customers requiring ancillary services. Ancillary services schedules are approved and posted on the OASIS Web server by the ISO. Whether they are issued over the public Internet or the ISO private network, all bids and schedules are accessible by transmission customers. In addition, billing data are transmitted to transmission customers by ICCS on a daily basis. On a monthly basis, ICCS transmits an invoice to each transmission customer by attaching the invoice to an auditable e-mail message. Appropriate user authorization security measures are provided by ICCS to ensure the privacy of the billing and invoice data.

3.11.3 Generation Unit Scheduling and Dispatch

Unit commitment schedules are usually prepared to cover the entire ISO's operating time horizon, which is up to two weeks in the future (i.e., the current day and the next 13 days). Unit commitment schedules consisting of availability status and desired MW output are prepared daily or even more frequently when necessary by each generation's control area. On a day-ahead and hourly basis, generation owners use ICCP to submit generation bids to the ISO. At a designated deadline within the hourly time window, ICCS uses the ICCP to retrieve these bids from each generation owner. All bids will be posted on the OASIS. Depending on the outcome of the generation re-dispatch processing of bids by ICCS, it may be necessary for generation owners to send a re-dispatch schedule to the generation control area. Generation unit owners must also send their maintenance schedules to the ICCS for approval. After the ICCS has processed these maintenance data, the approval or denial of the schedules is returned to the individual transmission and generation owners [Web01, Web05-07, Web10-14].

3.12 ELECTRONIC TAGGING

Electronic tagging applies to all transactions whether or not they cross control area boundaries [Tom01]. Both the ISO and its satellite control centers are responsible for staging, or contracting to stage, electronic tagging authority and approval services which receive and parse tags. As defined by NERC, the electronic tagging process consists of the following triple-A services [Web11]:

- Agent service
- Authority service
- Approval service.

The ISO and its satellite control centers are responsible for providing these services. Necessary functions used to accomplish tagging services are integrated into ICCS. The electronic tagging system of ICCS is totally compliant with NERC standards and specifications. Hence, although it can use any proprietary mechanism to convey the tag information, ICCS has to comply with technical standards and protocols for the exchange of transaction information with tagging related services. The detailed electronic tagging process is depicted in Figure 3.17.

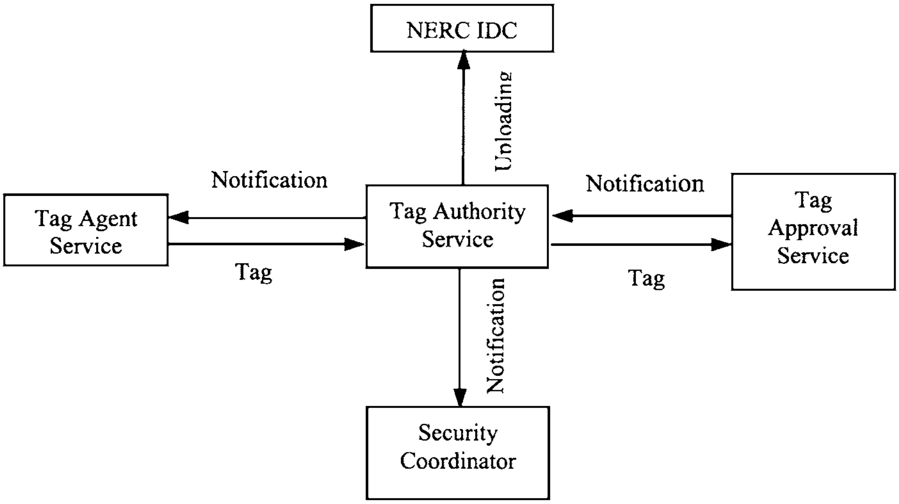


Figure 3.17 Electronic Tagging

During the process of information exchange, the electronic tagging system initially creates electronic tags that represent their respective transactions, and then disseminates these tags to all parties that are directly involved with these transactions. To achieve a good performance, the electronic tagging system must be able to identify parties in a transaction that have responsibility for the data exchange at every step and to ensure data integrity without duplicating the data entry or replicating errors. The time or the number of data transfers among parties should be minimized, and the electronic tagging system should be able to upload the approved tags to the NERC's interchange distribution calculator (IDC).

3.12.1 Tag Agent Service

The tag agent service provides the initial creation of an electronic tag representing an interchange transaction and the transfer of that information to the appropriate tag authority service. Purchasing-selling entities (PSEs) are responsible for providing this service directly or by arranging with a third party to provide this service as their agent. The tag agent service first validates the input tag data from the PSEs and then prepares all required tables and data elements as defined in the tag data model based on the PSE input data. Tags created by the tag agent service are forwarded to the tag authority service associated with the sink control area. The tag agent service assigns a tag ID and a tag key to each transaction and electronically communicates the tag ID, tag key, and tag data to the corresponding tag authority. A mechanism is provided by the tag agent service for PSEs to query tag authorities for the current status of their transactions either by simple polling or via an optional unsolicited notification mechanism. The tag agent service also provides the means for PSEs to withdraw, cancel, or terminate early any of their pending or active tags.

3.12.2 Tag Authority Service

The tag authority service provides the focal point for all interactions with a tag and maintains the single authoritative copy of record for each tag received from any tag agent service. Every control center is responsible for providing this service directly or by arranging with a third party to provide this service as its agent. The tag authority service manages each transaction's individual approval and overall composite status based on communications with tag agent and tag approval services. The tag authority service accepts input tag data from any tag agent service and identifies entities with approval rights over the transaction. All tags associated with entities identified as having approval rights over that transaction are transferred to the tag approval service for evaluation. Based on the approvals/denials received from these tag approval services, the tag authority arbitrates and sends the final disposition of the tag to the originating tag agent and all tag approval services associated with the transaction, and to that control area's security coordinator as well. The tag authority service verifies the identity of each approval entity attempting to approve or deny a tag based on the tag ID and the tag key, and updates the transaction's approval and composite status as appropriate. The tag authority service also provides the capability for both tag agent and tag approval services to review the current approval status of any transaction tag on demand. The tag authority service provides a mechanism for partial curtailment of transactions. All tags that are canceled or terminated will be forwarded to a designated location as identified by the information defined in the master registry associated with the sink control area.

3.12.3 Tag Approval Service

The tag approval service receives all tags submitted by tag agent services via the appropriate tag authority service, and communicates approval or denial information to the tag authority managing the transaction electronically in compliance with the protocol description. A mechanism is provided for the approval entity to send an approval or denial feedback to the tag authority service. The tag approval service can receive notification messages from the tag authority on each change in the composite status of the Tag. The current status of each transaction submitted for approval can be queried from the appropriate tag authority. Though initially the tag approval service is the responsibility of the control areas identified along the transaction's scheduling path, any entity that has the right to verify the contents of, and approve or deny, a tag is responsible for providing this service directly or for arranging with a third party to provide this service as their agent.

3.13 INFORMATION STORAGE AND RETRIEVAL

ICCS information storage and retrieval (IS&R) system consists of a commercial database management system that accommodates long-term archival storage and retrieval of information produced by ICCS. All ICCS data are available for collection, calculation, retention, and archiving by IS&R. The information to be stored and retrieved includes historical information required to meet regulatory archiving requirements, historical information required for audit purposes and for market dispute resolution, and some selected operational information required to support the ISO business process and decision support functions outside ICCS. Some types of information such as user log entries, ISO operator entries, functional control instructions, and alarms and events can even be automatically captured by IS&R, and the data to be captured and the periodicity can be defined through the IS&R database generation and maintenance function.

The IS&R provides services for a large number of information users. The IS&R database is capable of communicating with users through TCP/IP. The users' data can be exchanged with IS&R on a cyclic basis and on demand. All ICCS users with the appropriate authorization are able to access IS&R functions, review transaction scheduling and historical information, and even edit information [Web01-14].

3.14 ICCS SECURITY

ICCS manages all information system resources, including protocols, bandwidth, information, and address assignment. The ICCS has also become the server of communications functions, and information system users act as a client of ICCS services. In addition, some clients authorized by the ISO could have both reading and writing permission to ICCS computer systems. Hence, to protect ICCS from being violated of any security requirements, ICCS must be provided with necessary security measures. Most often the potential security risks to ICCS come from the following two areas: unauthorized access to ICCS by outside individuals and inadvertent destruction of data by individuals. In this section we will discuss these concerns and corresponding preventive measures.

3.14.1 Unauthorized Access

Because the ISO is actually connected with the public Internet, unauthorized access by outside individuals is a significant concern. The ICCS must provide security measures to prevent any unauthorized access. The generally desired security measures for this purpose mainly include user authentication, IP address authentication, system authentication, and Internet access via proxy servers. We discuss these measures below [Web 01-14]:

- **User authentication.** The ISO assigns a distinct identification and a password to each authorized user. Every user must supply its own identification and password in order to gain access to ICCS services. ICCS identifies the requestor's identification and password in the user login process; if the user identification and password are correct and matched, the login request will be granted, otherwise, the login request is refused

- **IP address authentication.** The ISO maintains an IP address assignment list for both its static and dynamic IP client address. In the user's login process, the IP address authentication function will check the user name against the IP address associated with the user on the list. If the user's name and IP address are matched, the access request will be granted. Because an IP address is globally unique to one user, this authentication function can help prevent illegal access when some unauthorized users masquerade as authorized users.

- **System authentication.** The system serial number of the user's machine is unique and is usually taken from the system hard drive. Like the authentication of an IP address, if the ISO maintains a system serial number list of all members, the system serial number of the user's machine can be used to validate the user identification. Because a system serial number is generally more difficult to forge than the IP address, the system authentication is more powerful to prevent an unauthorized user from masquerading as an authorized user.

- **Internet access via proxy servers.** Proxy servers can be used to limit the number of IP addresses required by the ISO for Internet access. All the ISO private network and LAN IP addresses can be hidden from the Internet. All access to the ISO's private network and LAN IP addresses further will be via particular proxy servers. This way not only the network security can be increased but also the entire IP address space can open up for use on the ISO's private network and LANs.

3.14.2 Inadvertent Destruction of Data

Inadvertent destruction of data can be minimized or even avoided through user access control and frequent system backup. The user access control can be realized by restricting the user's ability to read, write, delete, and execute files on ICCS and will be applied to all ICCS directories and files. In particular, to prevent users from accidentally deleting the output results of ICCS functions, users are given read-only access to some files. Meanwhile the system backup can be used as another effective approach to recover accidentally destroyed information. As a complementary tool, multi-generation backups are reserved to recover the lost data that are not detected soon after the loss [Web11].