Inter-System Communications/Networking

JOHN T. ROBINSON, MEMBER, IEEE

Invited Paper

Electric utilities require reliable data communications for power system control, operations, and maintenance. Utilities are among the largest users of data and, it has been said, the largest users of real-time data. In recent years, there has been an effort to apply the emerging technology of data communication networking to utility applications for real-time data exchange.

Emphasis in this paper is placed on techniques for modeling communication requirements and planning the development of an inter-system communications network to support power applications. We will also review where the industry is today with regard to link installations and protocol development.

THE STATE OF THE INDUSTRY

There is a growing requirement in the power industry to exchange data with external systems (neighborhing utilities, pools, and coordinating groups) for system security, power brokering, and real-time operation purposes. Applications such as operation of jointly owned power plants, pool coordinated AGC, power brokering, and state estimation, by their very nature, require the implementation of communication links between cooperating control centers.

The recent survey of System Control Centers (by T. E. DyLiacco and D. L. Rosa) [1] indicates that approximately 60 percent of the existing electric power control systems have external data links. Most of these are point-to-point communication channels using the BISYNC protocol or its variation. Several pools and coordinating centers exist based on simple network structures. A summary of these systems is given in Table 1.

THE PROBLEM

In the past, there has been considerable duplication of effort in the implementation of data links, and each link was unique with regard to link access procedure, method of data polling, application coordination, and message structure.

The most common method of exchanging data between two utilities (either neighbors or members of a pool), is via a direct leased line using a link access procedure such as ASCII or the IBM Binary Synchronous (BISYNC) protocol. BISYNC is one of the most popular data communication protocols and has been implemented by virtually every computer manufacturer.

In past years, this approach has been satisfactory because data amounts were relatively low and the structure of point-to-point links reflected the "structure" of the needs of the utilities involved (i.e., a utility wanted data from a single neighbor or was sending and receiving information from a pool over a single link). The need for greater coordination between utilities for such functions as jointly owned unit control or real-time data from external systems for state estimation has generated a need for ever-increasing amounts of data from multiple sources.

The traditional approach of installing a physical link for each new data exchange requirement is not feasible when the number of lines exceeds four or five. The lengthy schedule, duplicate implementation steps, and overall life-cycle communication costs for a "network" of single links become prohibitive in such a scheme.

Let us assume that five utilities desired to exchange data and several of these had existing Energy Management Systems (EMSs) (refer to Fig. 1). If all utilities connected directly there would be ten data links. The number of connections may be calculated by the formula

$$C = \frac{N \times (N - 1)}{2}$$

where n is the number of host computers in the network. Each link could conceivably be controlled by a different communication protocol, and there would be tremendous pressure to use a protocol friendly to the existing systems because of cost or limited capability and/or resources. These existing protocols might be inefficient or might not be suitable for the data exchange in question. The complexity of the software at each utility would increase correspondingly with the number of different links and interfaces needed at each host system.

In our hypothetical "growth" network, each link is a single point of failure (adding redundancy would double the number of physical links). The life-cycle communications cost for maintaining this network would be quite high since each link is a unique entity with its own hardware and software.

THE NETWORK SOLUTION

The solution is to install a data communication network using logical channels in place of multiple direct physical

Manuscript received January 13, 1987; revised October 6, 1987.

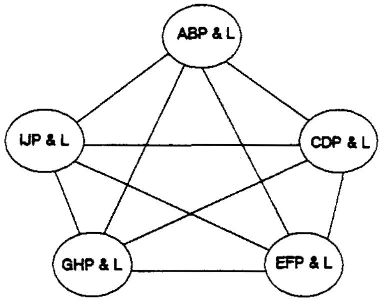
The author is with Energy and Control Consultants, San Jose, CA 95126-2388, USA.

IEEE Log Number 8718219.

0018-9219/87/1200-1670$01.00 © 1987 IEEE

Table 1 Major Networks

System	Nodes	Control Center Computer	Protocol	Comments
Penn.-N. Jersey-Maryland Interconnection, Norristown, PA	9 nodes	IBM 370's System 7's	BISYNC	upgrade to SDLC/HDLC planned
New York Power Pool, Albany, NY	8 members	Hitachi AS-9000	BISYNC	upgrading to DECNET
New England Power Exchange	4 nodes	IBM 370's System 7's	BISYNC	
Northeast Interpool Network	Ontario Hydro NYPP, NEPEX, PJM	Modcomp Classic 7810	MAXNET	links the U.S. systems with Ontario Hydro in Canada
Central and South West Services, Dallas, TX	4 members	Harris H800's	BISYNC/ISO Reference Model	X.25 future capability
Mid-Continent Area Power Pool, Minneapolis, MN	43 nodes	Honeywell 716's	ASCII	upgrade to DEC computer DECNET by 1987
National Control Center (Brazil)	5 nodes		SDLC	
ASELECTRICA (Spain)	9 members	CDC/CYBER	X.25	WSCC variant
SSPB (Sweden)	8 nodes	CDC/Xerox	TIDAS	



PROBLEMS:

- O PHYSICAL LINK FOR EACH EXCHANGE
- O EACH LINK IS SINGLE POINT OF FAILURE
- O MULTIPLE PROTOCOLS INVOLVED
- O COMPLEX SOFTWARE FOR MULTIPLE LINK HANDLING AT EACH NODE
- O POOR PERFORMANCE WITH HIGH COST

Fig. 1. Data communications system dedicated links. Typical network growth.

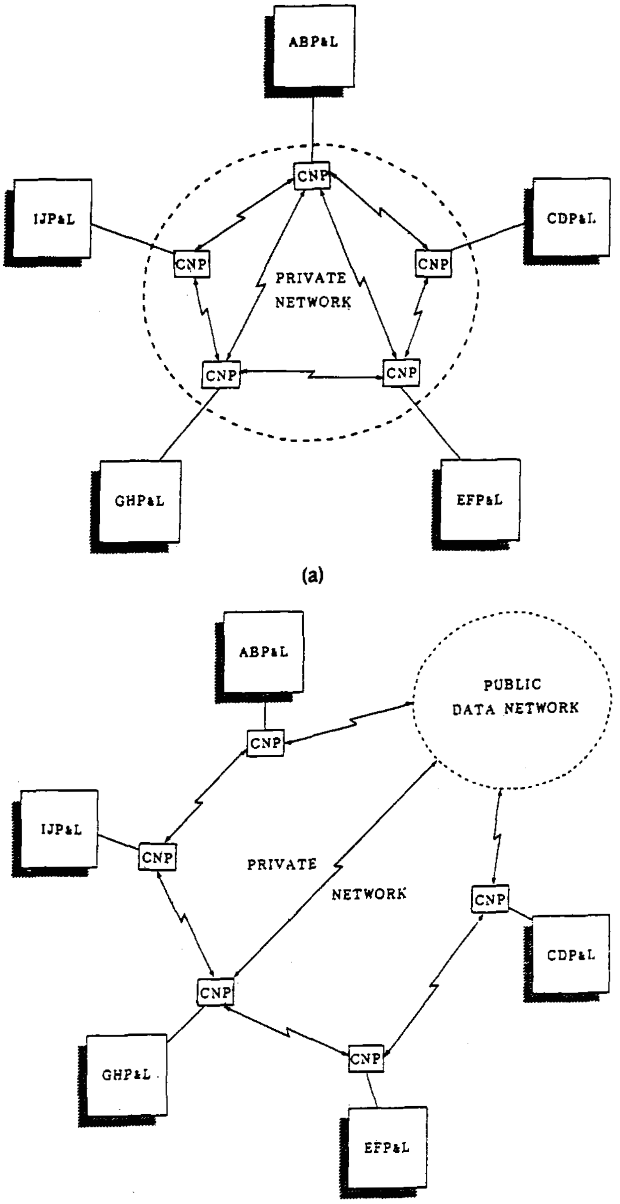
channels. (A logical channel is defined by the two end-to-end communicating entities and is independent of the communication medium. The network protocol takes care of the data routing.) There are several ways to procure the network. A value-added common carrier might be used (e.g., a public data network such as Telenet); a proprietary network could be purchased (e.g., IBM's SNA, CDC's CNA, DEC's DNA, Data General's ZODIAC, Modcomp's MAXNET), or a custom network developed. (Procurement alternatives are discussed later in this paper.)

There are many different network "structures" possible if private facilities are used, but they all are variations on four forms: hierarchical (or tree), ring (where every host or node is connected in a circle), star (every node connected through a central hub), and mesh (multiple connections to each node). Hierarchical structures are often seen in utilities with regional SCADAs, a central control center, and a pool center. Star networks are also common where several utilities are connected to a pool center. In the star, data are moved between the member utilities as a "database access" or a message switch.

A mesh network for our five-company example is shown in Fig. 2(a). Note that the number of physical links has been reduced to seven, yet the level of redundancy is very high since several links would have to be down before communications with a utility host would be lost. In addition, the given mesh structure provides for relatively fast message response as there is only one node hop between the furthest elements of a logical channel.

It is also possible to integrate a private network with a public network. This is illustrated in Fig. 2(b). Such "hybrid" networks are cost-effective where the ratio of high-priority time-critical data is relatively low in comparison to total data requirements.

In our example, front-end processors (also called communication network processors) would be used as the network implementation vehicle since the resources at the utility EMS host computers were inadequate for the network communications. The communication network processors (CNPs) at each utility company would handle the network protocol, message routing, communication media interface, connection to a value-added common carrier (if required), and direct channels to neighboring utilities or a pool for high-volume/time critical data. Although this solution requires a fair amount of hardware, it is particularly attractive since there is only one software package per CNP (duplicated at each utility node), a single external protocol is used (the CNPs would convert the local host protocol to



(a)

(b)

Fig. 2. (a) Distributed network architecture. (b) Hybrid network architecture.

the network protocol), and the CNP allows parallel processing of communications and EMS/SCADA applications.

The communications system life-cycle cost savings in our network example would be considerable over the fully connected approach. Two major components make up the savings: 1) the lower recurring communication media costs (between 20 to 60 percent depending on the redundancy), and 2) protocol and software savings of the CNP configuration.

Implementation and development strategies are discussed in more detail later in this paper. We turn now to a discussion of protocol issues.

Network Protocols

Communication protocols such as BISYNC and ASCII are inefficient, incomlpete, and not usable for communication networks without extensive modification. One of the main problems with these protocols is that they are designed to operate in a point-to-point configuration and have no provision for functions communicating across logic channels. Flow control (coordination of links and/or devices operating asynchronously) and end-to-end message control (including error handling and recovery) are major protocol issues that must be addressed in a networking environment.

The newer network protocols are usually based on the International Standard Organization Reference Model Standard of Open System Interconnection (RM/OSI). The RM/OSI breaks the communication and networking functions down into small manageable independent parts or "layers." (It also defines communication terminology and is the basis for on-going protocol development by ANSI, CCITT, and ECMA.) The layers are defined in terms of services and functions on behalf of adjacent layers and the internal structures of each layer are totally independent from other layers ("transparency" principle). An implementation based on the RM/OSI has the added advantage that it may be tested, implemented, and modified in parts with minimal (if any) impact to other parts of the model ("robust" principle). Thus it is possible to modify a well-designed network and take advantage of new communication technology and new protocols without making extensive software or system changes throughout the network.

The seven-level RM/OSI is illustrated in Fig. 3. As can be seen from the figure, "information" flows from one entity at the top or Application Layer, down through adjacent layers, across the connection media, up through the adjacent layers at the remote location until the "information" is received by the cooperating entity at the other end.

As an example of the use of this, let us follow the flow of a message between an entity (say, a State Estimator Program) in an Energy Management System to a corresponding entity in a neighboring utility. The first application program at Layer 7 would pass the message data to its Presentation Layer. Here the message would be formatted (according to "presentation" rules) and a Layer 6 header and trailer containing control information used by the Layer 6 services would be added and the message passed down to the Session Layer 5. (Each layer adds its control information header and trailer, takes appropriate action, and passes the message down to the next layer, and so on, until the message is transmitted by the Physical Layer across the interface media.) The "session" establishes and controls the data exchange, checks sequencing of messages, handles addressing, prioritizes messages, checks access rights, and guarantees data integrity. The Transport Layer provides media-independent communication services including "segmentation" (breaks messages down into parts) and "flow control" (coordinates exchange rates) for the agreed level of "service quality" (reliability). At the Network Layer, interface to the communication "media" is established and "packets" are routed through the physical channels of the network. The link access procedure handles the exchange of information over each point-point physical circuit (the familiar BISYNC protocol operates here). When the "message" is received by the other side, each layer acts according to its control information, strips its header and trailer, and passes the information up to the next layer until it reaches the proper entity in the Application Layer on the

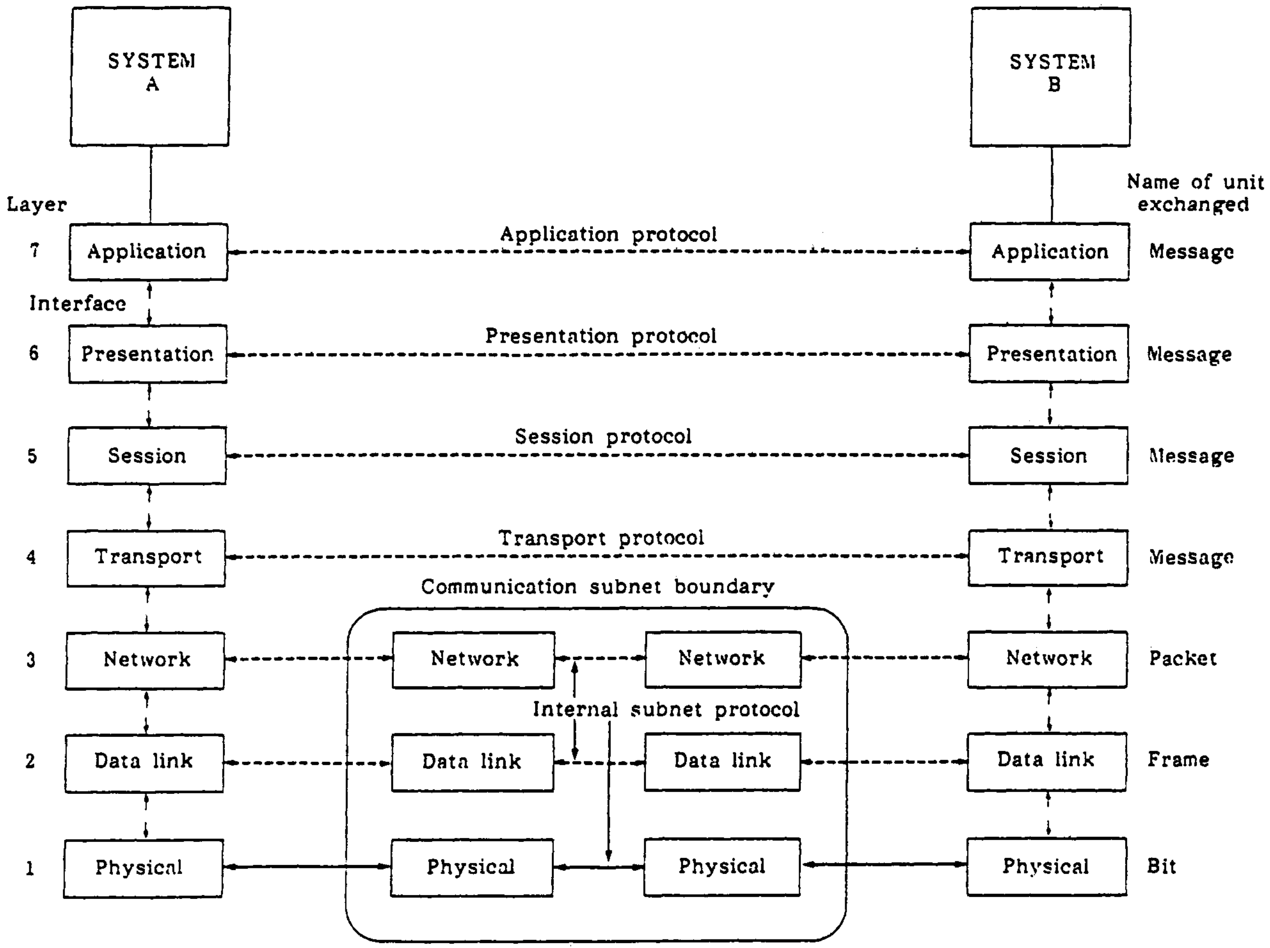


Fig. 3. International Standards Organization's (ISO) Reference Model of Open-Systems Interconnection (OSI).

receiving side. Note that there is a "protocol" or formalized set of procedures for coordination between each of the corresponding layers of the model. In our example, the State Estimator might use poll/acknowledge sequences to assure the secure and coordinated transfer of information between the two programs.

CCITT X.25 is one of the most commonly used protocols for networking [2]. It has three levels which correspond roughly to the lower three layers of the ISO/RM. X.25 is the protocol recommended by the WSCC [3]. It is an extremely popular protocol used extensively in many countries. It was intended primarily for use in interfacing to public data networks but has been adopted by several computer suppliers as their protocol of choice for all communications.

Several notable attempts at standardization for power system use have occurred in recent years. In the U.S., the Western System Coordinating Council published a communication standard in June of 1984 [3] that allows for networking via private or public facilities using the CCITT X.25 protocol. This standard also includes higher level protocols based on the ISO OSI Reference Model. (See [4] for a further description of the WSCC effort.)

At this time, several WSCC links are operational between centers at LADWP and SCE, and between Tuscon Power and Public Service of New Mexico. PG&E and the City of Santa Clara have implemented WSCC links using BISYNC at the Link Level with the higher levels based on the WSCC messaging and data format recommendations. Also, ASELECTICA in Spain has a variation of the WSCC standard in use. (CDC developed the first versions of the WSCC links, including the ASELECTRICA system.) (At this writing, only a subset of the WSCC recommended features have actually been implemented and tested. All of the operational links are point-to-point with predefined message formats.)

The utilities in Europe have had communication networks in use for some time. The TIDAS information system has been operational since 1975 in Sweden [6]. This message switching network is particularly interesting since it integrates several communication media methods including ECMA-24 digital data links, radio, and carrier frequency links. More recently, the Union for Coordination of Generation and Transport of Electrical Energy in Western Europe (UCPTE) has developed a data transfer protocol based on the ISO/RM [7]. This protocol uses X.25 at the lower three layers, EDF at the Transport Layer (the French recommendation), and specially developed procedures for the upper three layers.

A recent major effort was completed by 15 utilities in the Eastern U.S. to define "data communication capability" along with real-time data network feasibility and approach for their interconnected power systems. (See [9], Inter-Utility Data Exchange Committee Project.) The study effort included a thorough review of earlier utility projects and protocols. The decision was made to use existing ISO standards at the lower layers as follows:

- Session Protocol—ISO 8327
- Transport Protocol—ISO 8073
- Network Protocol—ISO 8878/X.25 Packet Layer
- Data Link—X.25 (HDLC).

At the higher layers (Application, Presentation, Management), protocols and requirements were specifically developed to meet IDEC needs (see [10]) including three levels of priority and access control via Bilateral Agreements.

IMPLEMENTATION CONSIDERATIONS

The implementation of a communications network to support EMS functions is a difficult and time-consuming effort. Several factors combine to make the job more difficult:

- The overall complexity of the EMS system functions using the network.
- Coordination requirement between different utilities having different needs (even for a single link, there are two host systems that must be "coordinated").
- Varied data communication needs (real time, high volume, high security, "on-line" versus "off-line" versus "interactive" processing, etc.).
- Fast changing technology in such areas as computer hardware/software, communication, and networking techniques, distributed processing/databases, the proliferation of value-added common carriers, etc.
- Upgrade/retrofit problem—the integration of communications into the existing EMS/SCADA systems with older technologies.
- Changing needs—the flexibility requirement to allow growth of the communication network to support new functions and the expansion/modification of existing SCADA/EMS functions.

We turn now to a discussion of implementation strategy methods, and look at ways to minimize the technical and coordination problems of developing a real-time data communication network.

In order to implement a network, the following task steps must be completed:

1) Identify those functions which have data exchange implications.
2) Finalize data exchange requirements (type, rates, timing constraints, priority, reliability needs, accuracy, data integrity, etc.).
3) Study and evaluate the feasibility of alternative approaches to meeting the data exchange requirements.
4) Select the best overall approach based on objective criteria (such as expected functional benefit, external constraints, cost, staffing, resource demands, and schedule).
5) Develop an implementation plan and schedule.
6) Carry out the implementation plan:
    a) Write procurement specifications where necessary (even if all the work will be done by the utilities, some type of internal specification is needed).
    b) Develop (or select) communication, networking, and application protocols.
    c) rite Interface Control Documents (ICDs) for the definition and control of all interfaces to the network.
    d) Evaluate protocols, select contractor(s) (for equipment and software procurements), and write a Work Statement(s).
    e) Modify/upgrade the utility host SCADA/EMS systems to interface to the network and to utilize the data on behalf of the given functions.

Data Requirements

Perhaps the single most important step is to identify all data needs for the participating utilities. Data requirements are defined in terms of the following characteristics:

- data types (analog, status, kWh, schedules, AGC data, etc.),
- supplement data (quality coding, data source, manual entry, alarm status, exception flags, etc.),
- data format (floating-point, integer, binary, ASCII, EBCDIC, etc.),
- amount of data,
- polling/exchange method (data request, periodic, event-driven),
- periodicity of exchange,
- allowable data delays,
- synchronization (method for synchronizing data or events).

These data requirements directly determine the size and type of communications needed.

Possible Procurement Options

There are essentially three procurement alternatives: public data networks (PDNs), proprietary networks, and custom networks. The Custom Network, as the name implies, is built especially to meet the communication needs of the utilities involved. This would be very expensive and is probably not feasible today considering the availability of standard communication products and services.

The proprietary networking products (such as SNA, DECNET, MAXNET, ZODIAC, etc.) all share similar characteristics:

- they are layered architectures
- they provide for program-to-program communications.

Some of these have enhanced features such as:

- protocol conversion,
- gateways (linking the network to a PDN, or another network such as SNA),
- allow the sharing of computer system resources (such as disks, files, printers, CPUs, etc.).

The proprietary products differ in the protocols available, the number and types of links available, software/network support, and monitoring devices. However, they are quite inexpensive considering the functions available and the software is "thrown in" for the cost of the hardware. (The average network product software runs about 1 percent above the list price for the hardware in the network configuration.)

Public data networks (such as Telenet or Tymnet in the

U.S.) are value-added common carriers that are tariffed to provide "added value" in the form of:

- protocol conversion,
- data format conversion,
- virtual terminal capability,
- message store-and-forward,
- speed conversion (interfaces may operate at different rates),
- gateways (between PDNs, i.e., a U.S. network could interface to utilities in Canada through a Telenet to Datapac connection),
- integration of private facilities (it is possible to use a utility company microwave system and also connect to other utilities over the public facilities),
- network management services (cost and billing services, reverse charging, and network resource monitoring).

Interfacing to a Network

Most computer manufacturers can handle the X.25 network protocol and have certified versions available for the various PDNs. Also, the PDNs have software interface packages available for lease. Another alternative is to have the PDN do protocol conversion. This is done either within the PDN (at the local control office in the network DCE) or in a PDN-provided local processor. The hardware and software for the local processor is maintained by the PDN and software changes are down-line-loaded to the local processor.

The third method, which was discussed earlier in our network example, is to use a Front End Processor (FEP), or, as it is called when used in a network, a Communication Network Processor (CNP). The CNP will handle all communication message queuing, protocol conversion, network interfaces, error control, message retry, and network performance monitoring. The CNP could even serve as a node in the network and route messages to adjacent nodes without host intervention. One of the major benefits of the CNP is that it provides parallel processing of network functions and related data link handling with utility EMS/SCADA functions. Therefore, separate growth paths for these functions exist and the network can be modified, or the EMS/SCADA functions modified, with little impact to other parts of the system.

Interface between the CNP and utility host is by some simple, existing, "host-friendly" protocol such as ASCII, BISYNC, a parallel interface, or a Local Area Network (e.g., Ethernet). Several of the network suppliers offer Ethernet or IEEE 802 LAN interfaces which operate as "intermediate nodes" at Levels 2 and 3 of the RM/OSI. These interfaces are particularly attractive because of their high throughput and ease of expansion and modification.

Network Real-Time Resource and Technical Design Control

Real-Time Resource and Technical Design Control (RTDC) is the process of budgeting, monitoring, unit testing, and controlling resource utilization, throughput, performance, and response on a real-time system. RTDC is particularly important in a communication network where the ability to exchange data in a timely manner is dependent on multiple resources (channel availability, CPU process time, memory, routing mechanisms, message queuing, etc.) at multiple nodes all along the virtual path.

It is very important to size the network properly during the early phases of the system design. As discussed earlier, this starts with a proper understanding of the data requirements and expected growth of the system. Budgets would be established for all resources on a function (EMS data user) and logical channel basis.

Budgets may be established for the network using queuing theory equations. It has been demonstrated that networks may be modeled conservatively using M/M/1 equations [8]. The equations, however, have to be modified to account for the error characteristics of the media, protocol overhead, and end-end response characteristics. (A set of recommended equations is given in Fig. 4.)

1) Maximum Line Throughput

$$MT = \frac{M(1 - P)}{\frac{M}{L} + D}$$

M: Average message length (bits).
P: Probability message is repeated (has errors).
L: Line rate (bits/s).
D: Delay between messages (due to polling, modem turnaround, message synchronization, etc.).

2) Line Utilization

$$U = \frac{\text{actual}}{\text{possible}} = \frac{A \times M \times P}{MT}$$

A: Average # Messages/second (based on required response)
P: Protocol Overhead Factor.

3) Queue Size (per line) (Gives an estimate of storage requirements.)

$$Q = \frac{U}{1 - U}.$$

4) Message Response (per line)

$$LR = \frac{M/MT}{1 - U}.$$

5) End-End Response (across the network)

$$R = PT + \Sigma LR$$

PT: Processing time at the EMS system/CNPs.
ΣLR: Sum of the line responses over the logical channel.

Fig. 4. Network performance equations.

For the study of large networks and/or complex EMS data exchanges, some type of computer-assisted analysis or simulation is preferred. Over the past several years, the author has used a communication network analysis program (CNAP—an ECC proprietary service) that provides a convenient way to plan, size, and budget complex networks. Using CNAP, a system designer can optimize network topology, automatically configure for backup of failed lines and nodes, determine logical channel message response, examine the network impact of using different protocols or polling techniques or message/data formats, tune the network with regard to data priority, and determine the traffic growth capability of a network.

As the system is built, the budgets would be verified by performance testing and the models, the corresponding utilization figures as well as message response times would be updated, and designs modified as necessary. After system startup, Network Resource Monitoring (NRM) software running on the network would provide information for tuning the network as it grows and changes.

High throughput and low data response are totally separate mechanisms in a network. We can see this by examining the equations for message response (Fig. 4). As utilization goes up, response increases dramatically. An increase of 10 percent (or an estimating error!) in utilization (say going from 80 to 90 percent) would result in a 100-percent increase in response. When applying RTDC procedures, these separate mechanisms would be monitored independently. The only way to assure that a message can be sent and received with high probability is to dedicate channels and associated resources for the message. (Public data networks, since they are subject to traffic congestion problems, may not be suitable for networks where high response is a key requirement.)

NETWORK INTERFACE CONTROL DOCUMENTS

The high need for coordination when developing a communication system dictates special coordination mechanisms.

Interface Control Documents (ICDs) are used to define and control all major interfaces and coordination efforts. They are particularly important in the definition of communication data links and networks where interfaces at several levels are needed and coordination between multiple departments, utilities, and computer systems is a primary concern during the implementation process.

It is important to recognize that existing network protocols are complex and cover a variety of communication situations. There are many options and parameters that are not defined. ANSI X3.28 (which defines BISYNC and ASCII protocols) has 14 Establishment and Termination Subcategories and 10 Message Subcategories. And all these combinations have optional control characters and various error recovery procedures or control procedures. X.25 and other layered protocols have alternatives and options for each protocol at each layer plus interfaces between adjacent layers. One of the reasons for the ICD is to define the *implemented* network communication protocols and to resolve all the options and define network parameters prior to start of design by the several participating utilities.

A checklist for a network ICD is given in Fig. 5.

1) Extension of the Network Standard (For Implementation and Coordination)
2) Defines the Complete, Network-Implemented Protocol for All Levels
3) Resolves All Options and Guidelines
4) Identifies Message Structures, Data Types, and Data Formats Supported
5) Provides Semantics (That is, The Meaning of all Messages and Data)
6) Provides Complete Error Handling and Recovery Procedures (Handling of Old Data, Missed Data, Link Reset, Network Restart, Application Program Actions)
7) Resolves Protocol (e.g., X.25) options:
    Level 1 (X.25 or X.21 bis?)
    Level 2 (LAP or LAPB? Selective Reject, T1 times? T3 times? N2/Retry Count? Frame Length? Flow Control Window? BSC Framing? Etc.)
    Level 3 (Reverse Charging? Packet/Time Accounting? Throughput Class? Packet Size? Closed User Group? etc.)
8) Resolves Interface (Between Host and Front-End) Features
9) Clarifies Exceptions or Alternatives
10) Sizes the Network, Number of Links, Amount of Data Exchanged, Gives Timing and Performance Parameters, and Identifies Growth Requirements.
11) Discusses Network Coordination and Operation Procedures, Assigns Responsibilities, and Gives Testing, Startup, and Maintenance Requirements
12) Provides an Implementation Plan Including a Schedule
13) Serves as the Control Document for Ongoing Maintenance of the Data Link
14) Identifies Data Link Coordinators (Utility Contact Individuals)

Fig. 5. Checklist. Network (data/link) Interface Control Document.

CONCLUSION

There is a definite trend toward the increased movement of data between neighboring utilities for several reasons. One is the need for data to support functions such as power brokering, pooling, operation of jointly owned units, and to improve the modeling of the interconnected power systems for security assessment purposes. Then there is the impact of technology growth: the maturing of communication technology and the lower cost of data link facilities/satellite communications, the emergence of protocols and techniques for data exchange, and the availability of the computer resources and inexpensive front-end processors to drive communication networks.

The trend is away from the low-efficiency, half-duplex, stop-and-wait protocols to the newer full-duplex protocols (e.g., HDLC, DDCMP) with features such as implied acknowledges, flow control, pipelining of messages, and combined data/control messages. Gains of 40 percent in link utilization are common with the new protocols. The trend is also away from point-to-point links and toward networks. Networking allows for efficient use of communication media and sharing of computer resources and common protocols.

The use of packet switching technology and public data networks is expected to increase for utility communications. The technology presently exists to integrate these networks for EMS applications and use dedicated links for high-priority, high-reliability data and to use the public network for lower priority data, terminal communications, and gateways.

The primary problem is one of coordination and planning. The marketing life of computer equipment, communications gear, and front-end hardware averages about 3 years. The operational life of EMS/SCADA systems seldom exceeds 10 years. Yet it may take 3 to 5 years to build a large communication facility to support utility functions. The EMS systems in the network will invariably be at different points in their life-cycle.

In this paper, we have presented ways to minimize the coordinated development problems associated with intersystem communications. The key is thorough and early planning of needs and expansion requirements. Particular attention must be given to communication resource budgeting and monitoring. Also, allowing independent and separate growth paths for the communication systems and the EMS/SCADA systems helps to guarantee fewer problems in the future.

REFERENCES

[1] T. E. DyLiacco and D. L. Rosa, Survey of System Control Centers, Edison Electric Institute, Jan. 1, 1986.

[2] *Packet Mode Interface to Public Data Networks*, CCITT X.25. Geneva, Switzerland, CCITT, June, 1980, no. 7-E, app. VII.

[3] *Western Systems Coordinating Council EMS Inter-Utility Communication Guidelines*, June 1, 1984.

[4] T. E. DyLiacco, W. A. Johnson, S. H. Buchey, M. D. Crouch, Paul Emmerich, S. A. Klein, M. D. Anderson, "Inter-utility computer data exchange," *IEEE Trans. Power App. Syst.*, vol. PAS-100, no. 12, Dec. 1981.

[5] "Proposed data structure for exchange of power system analytical data" (Draft Working Group Rep.), *IEEE Trans. Power Syst.*, vol. PWRS-1, May 1986.

[6] *TIDAS Network*, Pamphlet KG94-102E, Swedish State Power Board, 1979.

[7] H. P. Asal, "Information exchange between control centres in the West European high-voltage grid," *Elec. Power Energy Syst.*, vol. 5, no. 4, Oct. 1983.

[8] A. S. Tanenbaum, *Computer Networks.* Englewood Cliffs, NJ: Prentice-Hall, 1981.

[9] S. J. Wavrek and J. T. Robinson, "Inter-Utility Data Communication Committee Requirements Study Project," presented at Edison Electric Institute, June 1987.

[10] *Inter-Utility Data Communication Capability Protocol/Guideline*, version A.0, Apr. 1987.

John T. Robinson (Member, IEEE) received the B.S. degree in mathematics from the University of Wisconsin, Madison.

He is a Principal Consultant and is the General Manager for Energy and Control Consultants, Inc., West Coast Office, in San Jose, CA. He has twenty years of experience in real-time computer systems and control applications, the last fourteen of which have been primarily in electric utility SCADA/EMS environments. His experience includes direct technical participation in software development as well as overall design and specification of systems. His implementation background in real-time and computer systems includes operating systems design, SCADA/EMS applications, control systems, and communications. He has participated in over 40 electric utility SCADA/EMS and communication systems as either the project manager or technical consultant. In addition, he has been involved in several major communication networking projects and is one of the authors of the WSCC Inter-Utility Communication Standard, the Interutility Data Exchange Communication Protocol, and has participated in ANSI and IEEE communication standard work group activities. He has also presented papers at various conferences.