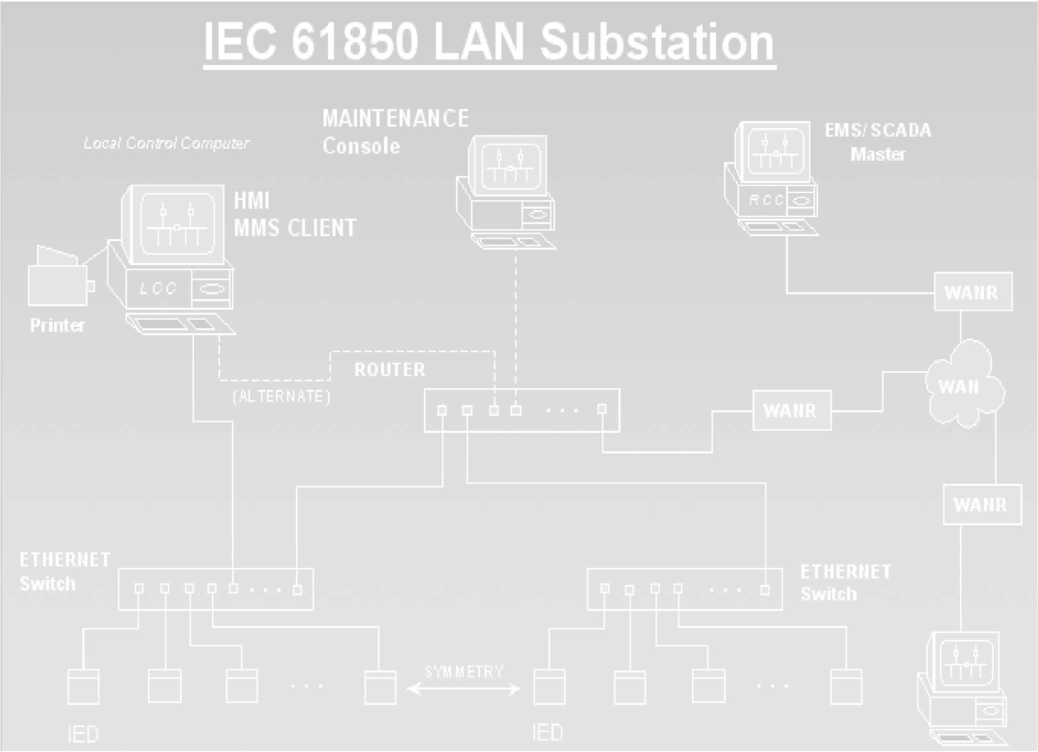
IEEE PSRC H6: SPECIAL REPORT

‘Application Considerations of IEC 61850/UCA 2 for Substation Ethernet Local Area Network Communication for Protection and Control’



IEEE PSRC H6 Special Report[1]

‘Application Considerations of IEC 61850/UCA 2 for Substation Ethernet Local Area Network Communication for Protection and Control’

Index:

[1] IEEE, PSRC, WGH6 paper Dated: 5-05-2005

The following is a list of members of WG H6 and those who have contributed to this Special Report;

John Burger- Chairman; Charles Sufana- vice Chairman

Mark Adamiak, Alex Apostolov, Brent Brobak, Christoph Brunner, Mason Clark, Raluca Capatina, Fernando Cobelo, Ken Cooley, Kay Clinard, Herbert Falk, Jeffrey Gilbert, George Gresco, Eric Gunther, Ameen Hamdon, Randy Heuser, Bill Higinbotham, Jerry Hohn, Dennis Holstein, Chris Huntley, Dick Krause, Steven Kunsman, Gary Michel, Bruce Muschlitz, Dan Nordell, Marzio Pozzoli, Dan Reckerd, Jack Robinson, Carlos Samitier, Richard Schimmel, Mark Simon, Veselin Skendzic, John Tengdin, Michel Toupin, Don Ware, Jim Whatley, Murty Yalla.

Chapter 1: SCOPE/INTRODUCTION

SCOPE:

The scope of this document provides the reader with sufficient information to consider all aspects for the application of IEC 61850 - COMMUNICATION NETWORKS AND SYSTEMS IN SUBSTATIONS and UCA2 for station communications projects. It provides UCA history, alternative protocols and advantages of UCA/61850 communications. It steps the reader thru the various services and features offered in UCA/61850 and provides the reader a number of choices and reasons to select the communications architecture necessary to meet requirements. The paper also provides a step-by-step application overview and finally a number of successful application examples. The application examples come from many of the protection vendors and utilities initially involved in this project.

INTRODUCTION TO UCA™

In 1986, under the Integrated Utility Communication (IUC) program, EPRI launched the Utility Communication Architecture (UCA) project.

Objectives:

The object of the project was to reduce the cost in substation automation and integration of data by providing an open architecture and a selection of standard protocols that will meet the needs and requirements of utilities and will also be accepted by manufacturers.

Requirements and specifications:

The project was initiated in response to utilities, with AEP as the leading utility, which realized that integration of data and optimization of costs of construction and maintenance should be implemented through a common communications structure and a common language. The previous effort of integration and intercommunication has demonstrated the high costs of development work as well as adaptation and converting a number of vendors with proprietary systems and protocols.

Around 1990, the need for integration increased as deregulation and global competition drove this requirement for utilities worldwide.

The major requirements/benefits of UCA^{TM} are:

- Interoperability
- Self-Defining Devices
- Time Sync
- Expandability
- Open Data Access
- Automated Reports
- Network Management
- Extensibility
- Remote Control
- Substation Events Handling
- Security/Integrity
- Easy of Maintainability
- Independent Functional Structure (Media_Transmission_Applications)
- Protective Function Response Time Capability
- Peer-to-peer communications

UCA ^{TM} 1.0 and 2.0

The first effort in developing an enterprise architecture resulted in UCA ^{TM} 1.0, which was a statement of utility requirements and a selection of existing standards and protocols that could be a solution to meet these requirements.
Since its beginning, the UCA project was results driven and initial phases included staging and benchmarking prototypes to verify that the proposed approaches would be able to meet the expected requirements and specifications.
Pilot projects were launched in 1993 and 1994 in order to experiment with the selected technologies in real applications. These pilot projects resulted in the development of UCA 2.0 that specifies more precisely the use of the MMS (Manufacturing Message Specification standard) and lead to the development of models in GOMSFE (Generic Object Models for Substation and Feeder Equipment). The substation implementation documents of UCA 2.0 were published in 1999 by the IEEE (Institute of Electrical and Electronic Engineers) as Technical Report 1550.

Over the past several years, the efforts and results of the UCA project were presented to the IEC (International Electrotechnical Commission) in order to be adopted as an international standard. This work has resulted in IEC 61850 – Communication Networks and Systems in Substations.

In the following chapters, we will see the current alternatives offered to utilities for integration of data and system in substations, and we will see in more detail what advantages and functionalities were offered by UCA 2 and now by IEC 61850.

CHAPTER 2: HISTORY/INTEGRATION ALTERNATIVES

HISTORY

In 1986, the Electric Power Research Institute (EPRI) began an investigation of network communications requirements, existing standards, and possible new approaches to providing enterprise-wide utility data communications for both business and system control applications through EPRI Project RP2949, "Integration of Utility Communications Systems". The first two phases of the project, "Utility Communications Architecture" (UCA) and "Database Access Integration Services" (DAIS), were completed by the end of 1991. Both projects were completed with the issuance of the UCA 1.0 Specification and the DAIS 1.0 Specification, respectively. To the extent possible, the UCA is built on current and emerging computer industry standards, with particular attention to electric utility requirements. Both UCA and DAIS recommend the use of standards which conform to the 7-layer International Standards Organization (ISO) reference model. Several standards are recommended for physical and data-link layers which allow utilities to use a wide variety of physical media in an interoperable manner. A narrow set of standards are recommended for the middle layers of the model so that enterprise-wide connectivity can be achieved at the network level, while a rich set of application layer standards are recommended to support both process and business functions. UCA and DAIS 1.0 specify the use of application layer standards for process control (Manufacturing Message Specification - MMS), file access (File Transfer, Access and Management - FTAM), Virtual Terminal (VT), Directory Services (DS), Electronic messaging (Message Handling Services - MHS), Network Management (Common Management Information Protocol - CMIP), and Remote Database Access (RDA).

With the release to the industry of the UCA and DAIS specifications, the industry needed a place to learn about, to challenge, and to discuss implementation issues related to the use of the recommendations. Therefore, in May of 1992 EPRI and Northern States Power Company (NSP) established a forum (meeting several times a year) called "The Forum for Electric Utility ISO 9506 (MMS) Implementation" (aka the "MMS Forum"). Working groups from the Forum focused on the use of the Manufacturing Message Specification (ISO 9506), which the UCA specification recommended for process control. Working groups were formed to address issues related to customer interface, distribution automation, substation automation, power plants, and control centers. A "profiles" group was established to address issues related to the use of MMS across multiple communication media and communication profiles.

Work originating in the MMS Forum and from a series of demonstration projects has resulted in more detailed specifications for three areas which address interoperable communications in the utility industry: communications profiles, application services and object models for Intelligent Electronic Devices (IEDs).

The UCA communications profiles specify a set of protocols that are used in specific application areas. All profiles for process control make use of MMS as the application protocol to provide real-time data access and supervisory control functions. UCA specifies the use of MMS running over a variety of different underlying network protocols depending on the needs of the particular system. For instance, in a distribution automation environment where point-to-point and multi-drop serial links used over MAS and SS radio systems must be supported, there are profiles of UCA that run over RS-232. For LAN environments, such as a substation or control room network, there are profiles using Ethernet with TCP/IP or ISO protocols. UCA supports the following basic profiles:

- A 3-layer reduced stack with MMS over an Asynchronous Data Link Control (ADLC) layer for operation over RS-232.

- A "Trim-7" 7-layer stack running over ISO/OSI transport over ADLC and RS-232 with a trim version of ISO Session and Presentation.

- A 7-layer stack running over TCP/IP over Ethernet.

- A 7-layer stack running over ISO/OSI over Ethernet.

The UCA application service model is referred to as the Common Application Service Model (CASM). CASM specifies a generic or abstract set of services such as reporting, select before operate, logging, etc. that were available for UCA applications. While the CASM model is designed to be generic enough to support a number of different application protocols, UCA provides a mapping of CASM to MMS only.

Device and object models were specified by the Generic Object Models for Substation and Feeder Equipment (GOMSFE) specification. GOMSFE provides detailed device models for common electric utility equipment such as relays, breakers, switches, meters, RTUs, load tap changers, voltage regulators, etc. Each GOMSFE object model contains a comprehensive list of predefined, prenamed objects that the device may contain. A manufacturer typically chooses a subset of GOMSFE models and objects to instantiate in a device. GOMSFE also provides the ability for vendors to add their own unique features to a device in a manner that still supports interoperability between devices and UCA applications. UCA and GOMSFE requires that the details of the object models be incorporated into the device. This allows the UCA client to download the object model and variable names directly from the device over the network making the IED "self-describing".

At the same time as the formation of the MMS Forum, a working group was established to define the next generation of control center protocols. After an initial feasibility study, that group chose to base its recommendations on UCA, and the details of the Inter-Control Center Protocol (ICCP), now standard IEC TASE.2, were worked out.
Along with the MMS Forum, a number of UCA demonstration projects were conducted beginning in 1992. In 1994 the EPRI RP3599 Integrated Substation demonstration was initiated to explore requirements and technologies for substation relaying and control.
The AEP Substation Initiative was started in 1996 and, after initial proof-of-concept testing, adopted UCA as the recommended practice for substation applications.
A new IEEE Standards Coordinating Committee 36 was formed in 1998 to coordinate IEEE standards work related to the UCA. Its first product was IEEE Technical Report 1550, based on the AEP Initiative work and the CASM and GOMSFE work initiated by the MMS Forum. TR1550 was published in late 1999.

HARMONIZATION - THE PROJECT TEAMS JOIN FORCES

In 1995, IEC commissioned a new project, 61850, to define the next generation of standardized high-speed substation control and protection communications. The main objective, as with UCA 2.0 project, was to have vendors and utilities work together in the definition of the communications infrastructure for substation monitoring and control. The generation of this standard would assure interoperability of the various vendors' IEDS avoiding the extremely complex incompatible systems.

By 1996, the EPRI UCA 2.0 and IEC 61850 groups were independently working on standards that address the interoperability of different vendor IEDS in substation automation applications. It was clear that both of these standardization efforts should be harmonized resulting into a single communication standard for the world market. In October of 1997, the Edinburgh IEC TC 57 WG10, 11 and 12 meeting concluded with the agreement that only one standard for Substation Automation and Communication should be developed and to merge the North American and European approaches. A joint task force composed of IEC and UCA experts was established to prove the feasibility of harmonization of certain parts of the UCA standardization.

Meanwhile, the UCA project continued pushing for vendor implementation, product demonstration, and increased interest from the utility base. The results from the North American specifications and modeling approach were offered to the IEC working groups for review and in January of 1998, the conclusion was positive and harmonization commenced. UCA modeling, data definitions, data types, and services were extended and adopted in the respective 61850 standardization parts. Therefore, IEC 61850 was intended to be a *superset* of UCA. In the end, the working group members in the joint task forces worked in a continuous writing, editing, and negotiating process to create a standard that embraces both the UCA and European utility and manufacturer directions and preferences.

The working group members involved agreed on the value of standardizing communications processes and protocols and different groups within the standardization effort focused on the other various objectives. These objectives included:

Comprehensive modeling of substation equipment communications and functionality. One intent is to describe devices thoroughly enough to allow one type of device to be replaced by another from any manufacturer. This is referred to as interchangeability. Replacement of one device by another must not affect the function of the coordinated system and will be difficult to achieve due to the different operating principles used by different IED vendors. Typically, vendors differentiate themselves by extending the functionality of a given model

Self description. The concept of self description is that of having the IED describe its capabilities and communication parameters thus reducing the engineering associated with configuration of data clients. This will be successful to the degree that the data client is equipped to make use of the information. Also, this process does not reduce the effort necessary to configure the IED itself or the effort necessary to maintain unique configuration software tools for each product or vendor.

Power apparatus communication capability. The expectation is that communication, data acquisition, and control capabilities will be directly imbedded into the power apparatus and that they will communicate on the LAN.

Reduction of conventional wiring. Power apparatus and merging units communicating over LANs also demonstrate the replacement of conventional wiring with simple communication connections. Data are communicated among devices via a single communication channel rather than the traditional method of a dedicated pair of copper conductors to sense every contact and measured value.

High speed LAN. Most communication applications will be served by substation hardened communication equipment meeting surge withstand, fast transient, high pot, an other substation environmental requirements. Applications requiring high speed and deterministic LAN communications will be able to take advantage of Ethernet priority and VLANs. Examples include peer-to-peer control (GOOSE) and high resolution common time-base synchronization for event recording, synchronized control, and high-speed data sampling.

The IEC 61850 Standard has been organized by content as listed in Table 1.

Table 1: IEC 61850 Standard Contents

Part	Title
1	Basic Principles
2	Glossary of Terms
3	General Requirements
4	System and Project Management
5	Communication Requirements – for functions and device models
6	Configuration Description Language for communications in electrical substations related to IEDs
7-1	Basic Communication Structure for Substations and Feeder Equipment– Principles and Models
7-2	Basic Communication Structure for Substations and Feeder Equipment–Abstract Communications Service Interface(ACSI)
7-3	Basic Communication Structure for Substations and Feeder Equipment–Common Data Classes
7-4	Basic Communication Structure for Substations and Feeder Equipment–Compatible Logical Node Classes and Data Classes
8-1	Specific Communication Service Mapping (SCSM) – Mapping to MMS (ISO/IEC 9506-1 and ISO/IEC 9506-2) and to ISO/IEC 8802-3
9-1	Specific Communication Service Mapping (SCSM) – Sampled Values over serial, unidirectional multi-drop point-to-point link
9-2	Specific Communication Service Mapping (SCSM) – Sampled Values over ISO/IEC 8802-3
10	Conformance Testing

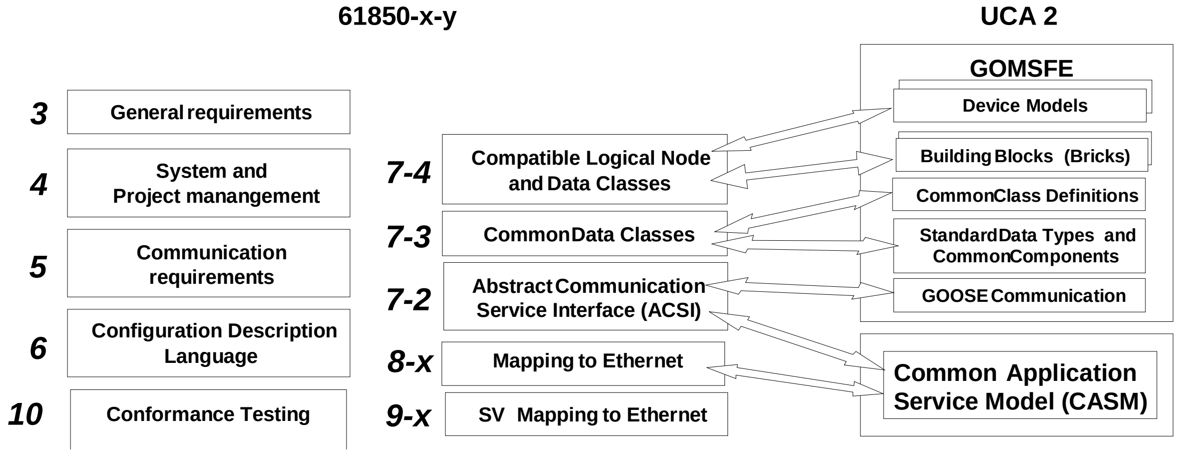

61850-x-y
UCA 2
3
General requirements
4
System and Project manangement
5
Communication requirements
6
Configuration Description Language
10
Conformance Testing
7-4
Compatible Logical Node and Data Classes
7-3
Common Data Classes
7-2
Abstract Communication Service Interface (ACSI)
8-x
Mapping to Ethernet
9-x
SV Mapping to Ethernet
GOMSFE
Device Models
Building Blocks (Bricks)
Common Class Definitions
Standard Data Types and Common Components
GOOSE Communication
Common Application Service Model (CASM)

Figure 2-1 – Relation between IEC 61850 and UCA

A UCA User's Group was formed in 2002 to both undertake new technical work items as well as to promote the use of UCA technology. The term UCA is now considered to be used in the generic sense of Utility Communications Architecture and the focus of the

Users Group is to promote the use of IEC 61850 and other related communication standards. New implementations of the concepts first pioneered by the EPRI UCA effort should now be focused on IEC 61850.

Ethernet Data Exchange Protocols:

Ethernet technologies have been in use since 1979. The first protocols used were vendor proprietary and supported only by the vendor's proprietary operating systems and computers. This technology worked well when the systems to be networked were from the same vendor but did not allow integration across dissimilar vendor platforms. Over time protocols were introduced that did allow mixed vendor support on Ethernet. Netbui, DECnet, LAT, OSI, and TCP/IP are the more familiar protocols that where supported by several vendors. The predominant transport and network protocol in use today is TCP/IP.

As communications costs decreased Ethernet communications became very cost effective. In the past an Ethernet connection could cost as much as $5,000. Today the typical Ethernet PC card is around $10. Today it is actually more costly to use serial communications adapters than Ethernet adapters and Ethernet is typically 100 times faster. It was clear that if the difference in cost did not replace the serial communications, the difference in performance would. Integrators now had a high-speed low cost dependable communications medium on which to implement data exchange.

The need for real-time data exchange over Ethernet was driven by market demands for higher performance at a lower cost. Protocol developers evaluated serial protocols used in the past and selected those that would be suited to migrate to Ethernet using TCP/IP. One of the first protocols to be implemented over Ethernet using TCP/IP was the Modbus RTU protocol originally developed by Modicon for use over serial communications. Modbus RTU is a byte oriented poll/response protocol which has been adopted by the industry as a defacto standard. Implementation of Modbus RTU over TCP/IP was very simple. Both the Poll and Response Modbus RTU messages were encapsulated into a TCP/IP protocol data unit (PDU). No modification of the protocol was required.

DNP 3.0 is another protocol that has been implemented in a similar manner as Modbus RTU. DNP 3.0 was originally developed by Westronics - a RTU manufacturer. Shortly after the implementation of Modbus RTU on TCP/IP, developers migrated DNP 3.0 to TCP/IP using the same encapsulating technique. DNP 3.0 can be used in either a poll/response mode, fully bi-directional data exchange, or report by exception.
While DNP 3.0 was implemented on Ethernet in the United States, the IEC standards group was writing another standard on how to use the IEC 870-5-101 RTU protocol on Ethernet. The IEC 870-5-104 standard outlines how the IEC 870-5-101 is to be encapsulated over Ethernet. There is very little functional difference between DNP 3.0 and IEC 870-5-101.

Adaptation of existing protocols such as Modbus RTU, DNP 3.0, and IEC 870-5-101 to Ethernet over TCP/IP was expedient and effective. Very little documentation and actual development had to occur to implement a data exchange function. The downside to the encapsulation on TCP/IP approach is that the adaptation of a technology that was designed for half duplex serial communications media does not take full advantages of the Ethernet bandwidth to enhance the protocol's features and functions. While developers where encapsulating RTU protocols into TCP/IP, other groups were developing standards to use the network bandwidth and features in a more functional manner.

Integration/automation approaches in substation

Integration and automation in substations have been realized from different points of view. But, before saying more about integration, let us define what is generally understood today as integration and automation in substations.

Substation integration: The collection of data from protection, control, data acquisition, monitoring devices, etc. in order to reduce the numbers of devices and systems, therefore reducing the capital and operating costs.

Substation automation: The automatic operation of substation and feeder functions and applications in order to optimize the management of capital assets and enhance operation and maintenance efficiencies with minimal human intervention.

From the previous definitions, we can see that substation automation is closely related to and relies on substation integration if its costs are to be minimized. In order to shorten the text, we will use in the following lines the sole term automation even if it can also be applied to integration.

Automation as seen from nature of protocols and architecture:

-Proprietary
-Public
-Standardized
-De facto

Proprietary:

Old way of doing things

Closed system

Standardized:

New tendency

Open

IEEE/ANSI, ISO, IEC. ITU

Ex.: Ethernet, IEC-60870, IEC-61850, ….

Public:

Past years and actual

More open than proprietary (low cost)

Ex.: DNP, Modbus, Internet(TCP/IP), XML, OPC, etc.

Nature	Time frame	Advantages	Disadvantages
Proprietary	Past years and today	-Manufacturer support -Optimize to application	-Tied to manufacturer -Closed to interoperability -Lifetime relies on manufacturer
Standardized	Past few years Future trend	-Open support -Open to evolution -Flexibility	-Less familiar to power specialist -New specialities involved(IT) -Lengthy approval/revision process
Public	Past years and today	-Easy support -Some flexibility -Availability of low-cost development tools	-Developed for specific applications -Limited in functionality -Limited in ability to evolve /flexibility

<u>Automation based on function or devices:</u>

Control function or PLC:

Past years
Limited in functionality and ability to evolve
Often tied to proprietary protocols
Ex.: Allen Bradley, Schneider, Texas Instrument, ABB, Siemens, Alstom, etc.

SCADA function or RTU:

Old way of doing and still applied today
Limited in functionality and ability to evolve
May include protocols conversion
Ex.: Automatec, Telegyr, QEI, D20 and D200(GE Harris), etc.

Communications functions or special devices:

These devices are diversified and their names and functionalities vary between devices and manufacturers. The most popular names for these devices are: communications processors, data concentrators, bay controllers, station controller, gateway, protocols converters, PC, etc.
Applied for past 7-8 years
More or less limited in functionality and ability to evolve
Often includes protocols conversion
Ex.: NIM (Tasnet), D25 (GE Harris), SEL-2020 and 2030 (Schweitzer), SMP (Cybectec), etc.

Protective function or modern IEDs :

New way and new tendency
Functionality, ability to evolve, flexibility if using adequate architecture
Ex.: UR relay (GEPM), EdisonPRO (Cooper), SEL-2701 card (Schweitzer), etc.

Function/devices	**Time frame**	**Advantages**	**Disadvantages**
Control function or PLC:	Past years and actual	-Manufacturer support -Flexible programmability	-Often proprietary protocols -Costly adaptation -Limited ability to evolve -Limited functionality (files transfer, ….)
SCADA function or RTU:	Past years and actual	-Protocols conversion generally available -Adaptive to existing devices and protocols -Some programmability	-More equipment -No interoperability -Costly adaptation -Limited evolution -Limited functionality (files transfer, ….)
Communication function or special devices:	Past years and actual	-Protocols conversion -Adaptive to existing devices and protocols	-More equipment -No interoperability -Costly adaptation/modification -Limited evolution
Protective function or modern IEDs: **Note:** **1-If associated with adequate architecture**	Recent years and future trend	-Minimize systems and devices (cost effective) -Easy access to data for automation[1] -Industry wide services[1] -Flexible and evolutionary[1] -Interoperability[1] -Peer-to-peer communication. [1] -Real-time protect. Scheme1 (Minimize wiring) -Programmable protective strategy -Ready for distance monitoring and configuration -Ready for easy adaptive control or settings[1] -Minimize commissioning time and costs[1] -Adaptive to existing devices and protocols -Convenient for energy market evolution[1] -Planned for industry wide and secure access[1]	-New technology -Training required -Possible changes in work organization -Require new or external competencies -Limited number of devices support new technologies (UCA™and CEI-61850) -Programmability limited but in progress

Automation viewed from protocols stack architecture:

Minimal (3 layers)
Intermediate (5-6 layers)
Full OSI (7 layers)

Minimal structure (3 layers)

Developed in the past to minimize overhead (low communication capacities), Based on enhanced architecture protocol (EAP); suitable for embedded systems with little processing power

Main examples:
IEC-60870-5-103 over serial
DNP3.0: over serial
UCA™ over serial

Intermediate (4-6 layers)

Modern approach imposed by the popularity of the Web applications

Main examples:
Internet (TCP/IP)
DNP3 over TCP/IP
Modbus over TCP/IP

Full OSI (7 layers)

Modern approach developed in order to facilitate decoupling between application's layers and the different layers of communications

Main examples:
UCA™, IEC-61850

Structure	**Time frame**	**Advantages**	**Disadvantages**
Minimal (3 layers)	Past 10 years and actual	-Optimize for low communication/processing capacities -Widely used in some countries	-Limited in functionalities -Reduced interoperability -Configuration required very skilled people -Costly changes -Limited in flexibility
Intermediate (TCP/IP)	Recent years	-Easily available expertise -Evolution assured by popular use -Some degrees of flexibility	-Security to be watched -Changes can be more costly -Less decoupling between functions
Full OSI (7 layers)	Recent years	-Based on a standardized structure (ISO) -Decoupling of functions -Flexible -Adaptive to changes -Cheaper adaptation -Open to different security measures	-Required more communications resources (power) -Required new competencies (power domain)

Chapter 3: UCA Integration Functionalities, Services and Benefits

The recommended solution using UCA (UCA is Trademark 2000 by EPRI) and IEC 61850 for the substation LAN is implemented based on existing standards. These standards include the Manufacturing Messaging Specification (MMS) for services at the top and Ethernet as the Data Link and Physical layer. MMS is the ISO standard 9506 which defines the services and semantics in the Utility Communication Architecture (UCA) as noted in Figure 3.1 below. The seven-layer stack is used with an Ethernet LAN as the primary connection method of devices in the substation. The intent is that the substation communications will be UCA-compliant in order to eliminate gateways and allow maximum interconnectivity among IEDs at minimum cost. By adopting existing standards, the utility can take advantage of the economies of scale of the electric utility and industrial control industry that has made extensive use of these protocols.

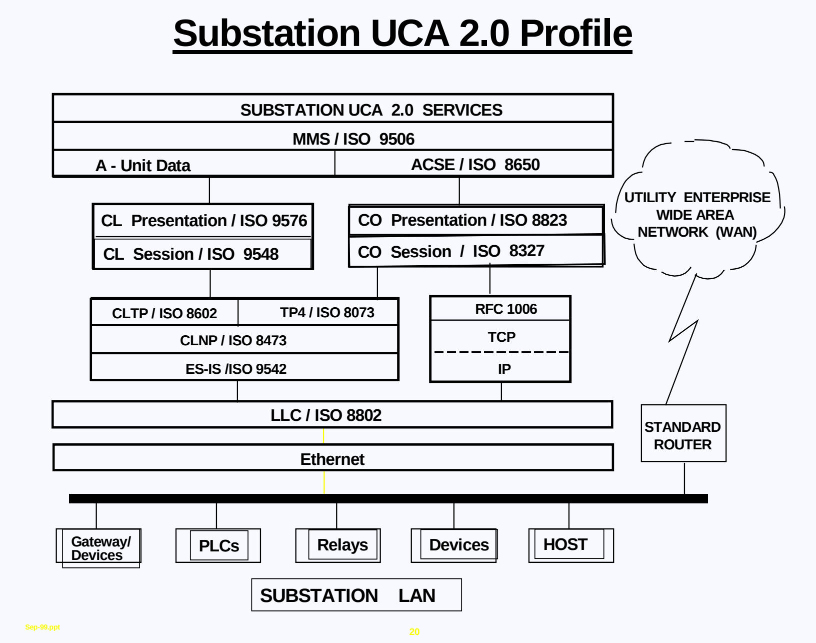


Fig 3.1

PERFORMANCE CONSIDERATIONS

Fast-Switched Ethernet can run at rates up to 100 Mbit/s, full-duplex, and can provide the demand responsiveness required for peer-to-peer communications between relays (intra or inter substation). Simulations and benchmark testing during earlier phases of the Substation Initiative Demonstration Project included staging of prototype protocols and topologies proved that that MMS with Fast-Ethernet and/or Switched Ethernet would meet requirements for protection commands over the substation LAN with typical IED counts under disaster overload conditions.

IEC 61850 ABSTRACT COMMUNICATIONS SERVICE INTERFACE (ACSI) AND BENEFITS

The IEC 61850 Abstract Communications Service Interface(ACSI), operating above the 7 layer model, provides a common set of communication functions for data access, reporting, logging, control applications and related support. Figure 3.2 lists the ACSI services most applicable in the substation environment. The use of a common set of services allows for 1) isolation of the models from service and communication details, 2) a high level of application interoperability, and 3) reduced integration and development costs through the use of common mechanisms for data access and communication establishment. The ACSI services are abstract and may be mapped into any number of communication application standards (existing today or tomorrow). Today, the MMS (ISO 9506) is the service specification of choice and mapping of ACSI into MMS is included in the IEC 61850 document. For example, the MMS Service “Write” is used for the ACSI Service “Operate” and “Set Data Values,” and the MMS Service “Read” is used for the ACSI Service “Get Data Values” and “Select” (the first step in a “Select-Before-Operate” control sequence).

METHOD	**IEC 61850 ACSI Application Communication Basic Services**
Data Access	GetDataObject Values/GetDataSetValues/SetDataValues/ SetDataSetValues
Control	Select/SelectWithValue/Cancel/Operate/TimeActivatedOperate?commandTermination
Create	CreateDataObject/DeleteDataObject/CreateDataSet/DeleteDataSet
Directory	GetServerDirectory/GetLogicalDeviceDirectory/GetLogicalNodeDirectory/GetAllDataValues/GetDataDirectory/GetDataDefinition/GetDataSetDirectory
Report/Events	Report (Unconfirmed)/GetRCBValues/SetRCBValues
Associate/ Security Check	Associate/Release/Abort
Setting Group	SelectActiveSG/SelectEditSG/SetSGValues/ConfirmEditSGValues /GetSGValues/GetSGCBValues
Log	GetLCBValues/SetLCBValues/QueryLogByTime/QueryLogAfter/ GetLogStatusValues
File Transfer	GetFile/SetFile/DeleteFile/GetFileAttributeValues
Generic Substation Event	SendGOOSEMessage/GetGoReference/GetGOOSEElementNumber/SetGoCBValues/GetGoCBValues
Sampled Values Transmission	SendSVMessage/GetSVCBValues/SetSVCBValues

FIG 3.2

GENERIC OBJECT ORIENTED SUBSTATION EVENT (GOOSE)

One of the most important aspects of the substation initiative was the development of the substation event message GOOSE that is incorporated in IEC 61850 ACSI. There are a number of issues that must be addressed for peer-to-peer communications of protective relay IEDs . In general, this type of communications:

- Is Mission Sensitive and Time Critical,
- Supports Variable Time Contact Closures,
- Must be Highly Reliable.

The Generic Object Oriented Substation Event (GOOSE) is based upon the asynchronous reporting of an IED's digital input and output status or a selected set of the IED's server data to other PEER (enrolled) IEDs. For the purposes of this discussion Input and Output status is from the viewpoint of the reporting IED. The associated IEDs receiving the message use the information contained therein to determine what the appropriate protection response is for the given state.

To achieve a high level of reliability, messages will be repeated as long as the state persists. Thus, GOOSE messages need not be acknowledged and so may be multicast. To maximize dependability and security, a message will have a time to live, which will be known as "Hold Time". After the Hold Time expires, the message (status) will expire unless the same status message is repeated or a new message is received prior to the expiration of the Hold Time. A GOOSE message may be priority tagged according to IEEE 802.1p.

The GOOSE message will contain information that will allow the receiving IED to know that a message has been missed, a status has changed, and the time since the last status change. The time of the last status change, called "Back Time", allows a receiving IED to set local timers (e.g., a BFI timer) relating to a given event even if repeat messages were missed.

A newly activated IED, upon power up or reinstatement to service, will send current status as an initial GOOSE. Any IED can request a specific IEDs status at any time. Also, all IEDs will send out their status message on a periodic basis (based on a configuration parameter). This will ensure that all associated IEDs will know the current status of their peers.

An important benefit of using substation events (GOOSE) is that new devices may be added to the substation without hardware (beyond the device connections) and without adding new software as the devices can simply enroll in the events and be able to act on the substation states according to their own internal algorithms.

TRANSMISSION OF SAMPLED VALUES

The communication services for the transmission of sampled values have been added by extended scope of IEC 61850. The scope of IEC 61850 includes the digital communication to switchgear with integrated electronics and to non-conventional current and voltage transformers with a digital communications interface.

Information transmitted from current and voltage transformers is a stream of digital, sampled data. The information is mission sensitive and time critical. The receiver needs to be able to detect missing samples and to correlate samples from different sources.

The sampling in the different devices is synchronized. The individual sampled values are identified with a counter value. This supports both the detection of missing samples was well as the correlation of the sampled values from multiple sources. The messages with the sampled values may be transmitted as unicast or as multicast messages. They are prioritized using IEEE 802.1 priority tagging.

USE OF OBJECT MODELS

In UCA/IEC 61850, as a result of the Substation Initiativ project, object models were developed for defining data formats and devices (aggregates of data and services). The combination of standardized device models and the rich services of ACSI (as noted above) provide even more benefits, in that the variables (and hence features, options, and additions) provided by each device are available through simple interrogation. UCA/IEC 61850 devices are therefore self-describing, allowing for very powerful tools and operator/maintenance interfaces, all of which are vendor, model, and revision independent.

UCA BENEFIT SUMMARY

The benefits of using open communications and the LAN architectures based on the OSI Model and Ethernet are summarized in the list below:

1. Open / Interoperable (Standards based)
2. Meets Substation Needs (UCA/IEC 61850 services and models were based on the list of substation application requirements)
3. Lower Cost (Through application of one set of common standards and ease of maintenance)
4. Parallel Operation/Redundancy (A benefit of the Ethernet LAN)
5. Freedom from Technical Obsolescence
6. Easier to Maintain (Use of GOOSE, and ability to add new devices with minimal change to Ethernet LAN)
7. Layered Architecture/Media and Application Independent (Layers allow changing out media and/or applications without changing software)
8. Object Oriented (Based on the substation device models)
9. Self Definition of Devices
10. Incremental Expansion (Only need to add devices, hardware and applications when needed)
11. Open Access (Ease of accessing information --- Subject to Security Constraints)
12. Shared Resources (Via the Ethernet LAN)
13. OSI Diagnostics/Network Management (Set of off-the-shelf products available)
14. Save 40% Capital Costs/15%-30% Recurring. (These savings percentages are based on the information gathered as part of the study of the Substation Demonstration Initiative.)

Chapter 4: UCA Communications Services

Using a standard UCA client program, objects defined in IEC 61850-7 can be read (or written) from UCA/61850 compliant server devices, such as the relays, over the high-speed, 10/100MB, Ethernet station Local Area Network (LAN). The client program, in addition to reading and writing 61850-7 data objects, may receive and display IED provided reports, sequence of events, alarms, targets, relay settings, oscillography and other logs/journals. This information can be viewed locally on the station HMI or remotely, via the company WAN, on an engineering office PC. Typically, the IEDs are given an IP or OSI network address before being connected to a given station LAN. Similar to a PC, the network address is usually area dependent and typically controlled and assigned by the company telecommunications group.

There can be a variety of applications that can make use of MMS within a substation with many different methods that can be used to invoke MMS services. However, there are several well-known application categories that can be discussed. Some of the common applications are shown in Fig 4-1. The applications shown are:

- HMI/SCADA: This represents a set of applications that perform data acquisition for the purposes of aggregation or display to a local human.
- CONTROL: This represents a set of applications that perform coordinated control algorithms/decisions within the substation.
- HISTORIAN/SOE: This represents a set of applications that record, store, and allow retrieval of sequence of events as well as archiving historical information regarding important measurements.
- DEVICES: These represent the actual applications that execute within a substation device. Devices are typically programmed in a proprietary manner.

Each application domain has its own set of unique issues and technologies that can be employed.

HMI/SCADA

These applications tend to process and/or display the current data values and quality. The off-the-shelf HMI display packages have similar architectures. These applications are constructed with one or more displays, a resident database, and the ability to support multiple device interfaces (including MMS). These applications typically support driver interfaces that: are developed using a proprietary interface, support the Dynamic Data Exchange (DDE interface, or support the OLE for Process Control (OPC) interface. Some utilities have then developed applications on the HMI PC, using these databases. As an example, programs can be developed to convert this data to match legacy SCADA protocols. This information could then used to supply RTU-type data to the corporate EMS Centers, directly from the station HMI PC, thus eliminating the need for stand-alone RTUs.

The selection of the appropriate driver interface technology requires an evaluation of the functions and performance required by the substation application. Typically, the proprietary interface yields the maximum performance and function. DDE typically yields the least performance, while the standardized OPC interface offers the flexibility of many choices for drivers. Different functions may be supported via different interfaces (e.g., OPC may support only Data Access whereas DDE may support Data Access and File Transfers). Therefore, it may be necessary to use multiple interfaces simultaneously. HMI and SCADA applications are used as an interface for operators (e.g., local or remote) that typically need to display and interact with the last known value and the quality of a particular data value. Maximum performance of this class of applications occurs when only the data needed for a particular display/function is acquired. Therefore, this class of application should be designed to acquire MMS information based upon application demand and not generalized polling of all available data (e.g., always obtaining all information within a substation).

Typically, the local HMI displays are used to show line values on a station one-line diagram screen. Line current, voltage, Mwatts, Mvars, breaker status, tagging, etc. can be displayed in real time on these HMI screens. Other screens may provide interface with virtual control switches, also developed by the user using the HMI program. Switches including breaker control, reclosing and carrier cutoff, local/remote, potential throw over, etc. have been developed. The switch positions shown on the displays provide data to the HMI display program control logic and the IEDS. The switches can be used to trip and close devices by issuing commands to PLC's or directly to relay IEDs. The HMI program can also be used to provide scaling, alarms and other requirements for various SCADA implementations. Special logic can be developed, for example, in advanced HMI programs to recognize start-up conditions and permit energization of station equipment

CONTROL

SCADA applications and IEDs have control functions. The design/application issues concerning the use of MMS and Generic Object Oriented Substation Event (GOOSE) are common to both. The major interface issue is how to deliver the latest value during a substation event.

In the case of GOOSE, it is possible to receive several messages within a short period of time (e.g., when two substation events occur within 10 msec of each other). This type of occurrence would typically generate a minimum of four (4) GOOSE messages being sent from each IED that detected a state change. It has been demonstrated that for a "worst-case scenario", in a large substation, this may result in over 150 GOOSE messages potentially needing to be processed. See Reference ? If a control application makes use of a pure event-based interface, the control application's processing and response time will be impacted due to processing the 150 messages worth of information. Even if the GOOSE interface is designed to process only changed information, this still means that 75 messages might need to be processed. An interface should be designed so that it allows the application access to a cache of the latest values.

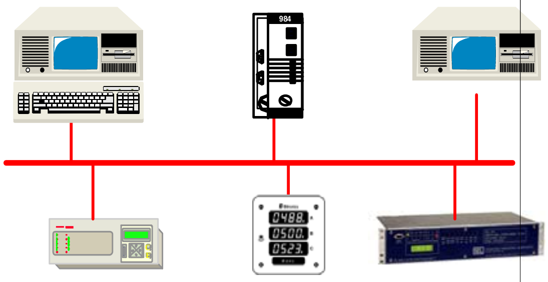
HISTORIAN/SOE

Unlike the CONTROL applications, HISTORIAN/SOE applications are designed to archive all data changes. This means that an MMS/GOOSE interface for this class of applications must provide a buffer of the information to be archived (as opposed to a cache of the latest values used by CONTROL applications). This type of buffering within the interface allows the application to process the information at its own rate. Since buffering requires some type of storage (e.g., a limited resource), the volume of information required to be buffered needs to be an application/system design concern.

DEVICES

IEDs have applications that are typically programmed via a proprietary mechanism. However, these applications are typically concerned with CONTROL or SOE. The same concerns discussed within the CONTROL or SOE application would need to be addressed by the device manufacturer.

In addition to that, devices may have a digital communications interface towards current and voltage transformers. Over that interface, the devices may receive the measured values already sampled and digitized using the communications service for the transmission sampled values. Depending on the sampling rate, the communications interface needs to be able to receive typically more than 1000 messages per second.



Chapter 5: SUBSTATION, DEVICE AND FUNCTION MODELING- OBJECT MODELING AND GOOSE

Object Modeling:

The documentation of these IED models for protective relay functionality along with all other anticipated IEDs in the substation are known as Logical Nodes and are defined in IEC 61850-7-4. This part of IEC 61850 addresses object definitions and object hierarchy for modeling the protection, control and data acquisition requirements of substations and feeders. Note that in the original UCA documentation, these models were known as 'Bricks' and were part of a concept known as Generic Object Models for Substation and Feeder Equipment (GOMSFE). Figure 5-1 depicts the GOMSFE as the interface between the remote client or user and the CASM services, and the interface between the CASM services and the server or field device controller. The use of the GOMSFE and Brick terminology in no longer commonly used and therefore will not be discussed in the remainder of this paper.

The 61850-7-4 object models were developed as a cooperative industry effort involving vendor and utility engineers. Starting with a base set of models, each vendor added draft models for one or two additional functions, which brought the total to thirteen models. After an in depth review two basic building block models evolved (Basic Relay Object and Basic Time Curve Object). After the existing models were reworked to use the basic building block objects, with extensions as necessary, it was concluded that an additional twenty three relays could be modeled using the basic building blocks. IEC 61850-7-4 provides the standard interface definition for the outside world to communicate with field device controllers, and their representation of the field devices. Figure 5-2 shows how the object models (Logical Nodes) fit into the overall context of a physical and logical device to represent the data associated with that device.

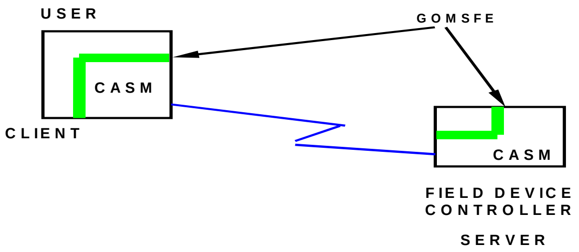


Figure 1 GOMSFE interfaces user to services

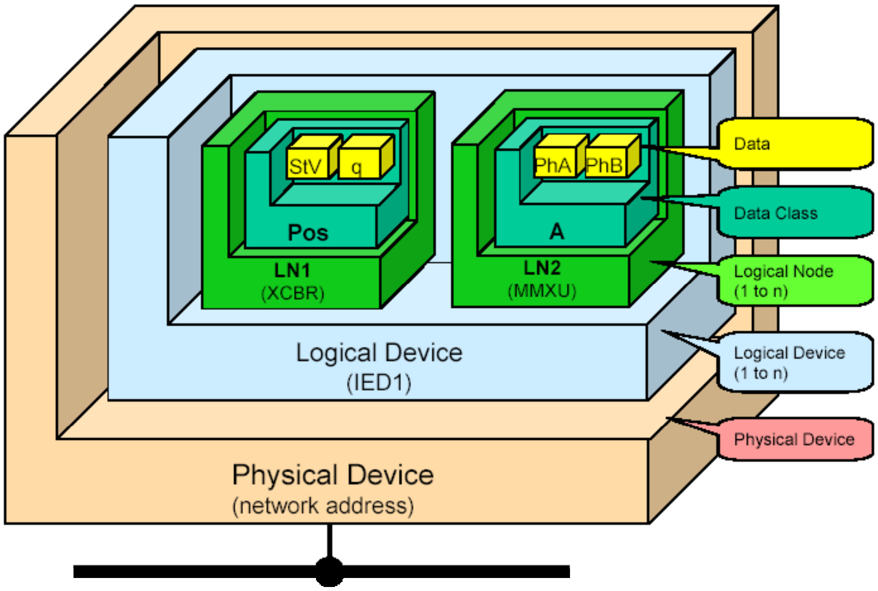
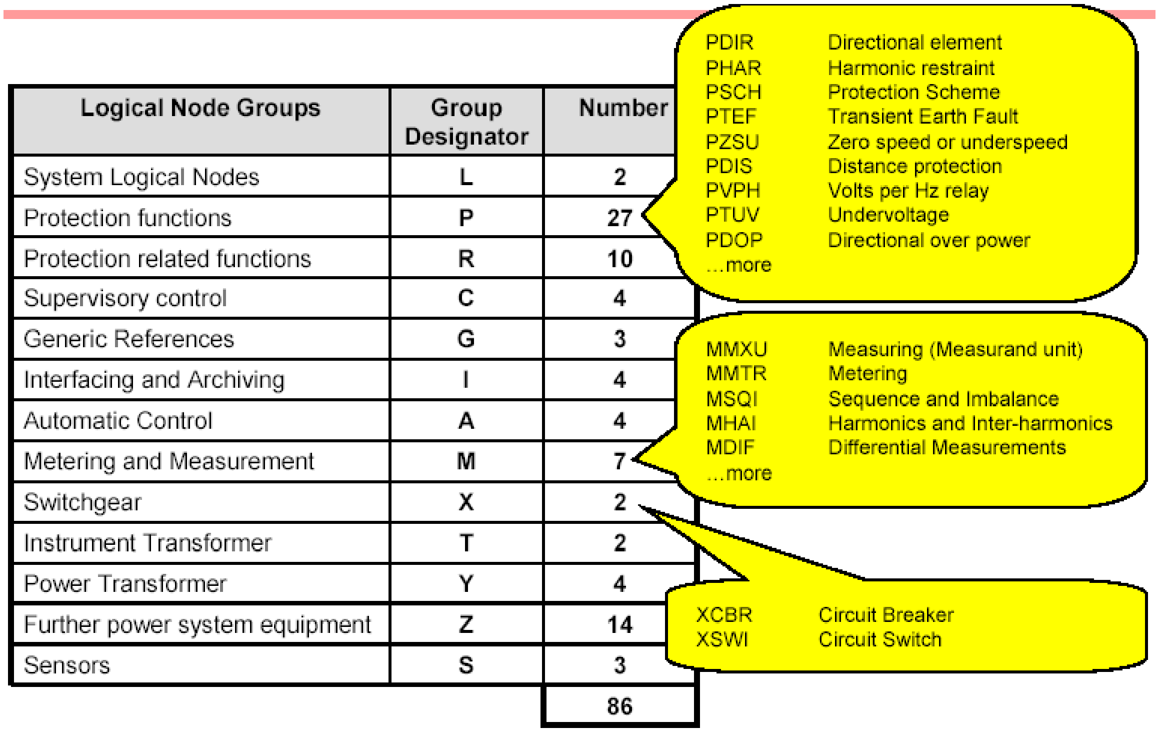


Figure 5-2 Logical Nodes in a device

Based on project work input from the original UCA effort and the current IEC working group activities, several high level groups of Logical Nodes were identified as shown in Exhibit 5-1. The individual Logical Nodes contained in these groups are standard collections of data objects; common components and structures based on Common Data Classes that logical device models are assembled from. These Logical Nodes are aggregated together to form logical device models that represent real world devices. The Logical Nodes are the standardized components, thus allowing vendors to form any number of logical device models that represent their various products from the standard building blocks.



Logical Node Groups	Group Designator	Number
System Logical Nodes	L	2
Protection functions	P	27
Protection related functions	R	10
Supervisory control	C	4
Generic References	G	3
Interfacing and Archiving	I	4
Automatic Control	A	4
Metering and Measurement	M	7
Switchgear	X	2
Instrument Transformer	T	2
Power Transformer	Y	4
Further power system equipment	Z	14
Sensors	S	3
		86

PDIR	Directional element
PHAR	Harmonic restraint
PSCH	Protection Scheme
PTEF	Transient Earth Fault
PZSU	Zero speed or underspeed
PDIS	Distance protection
PVPH	Volts per Hz relay
PTUV	Undervoltage
PDOP	Directional over power
...more	

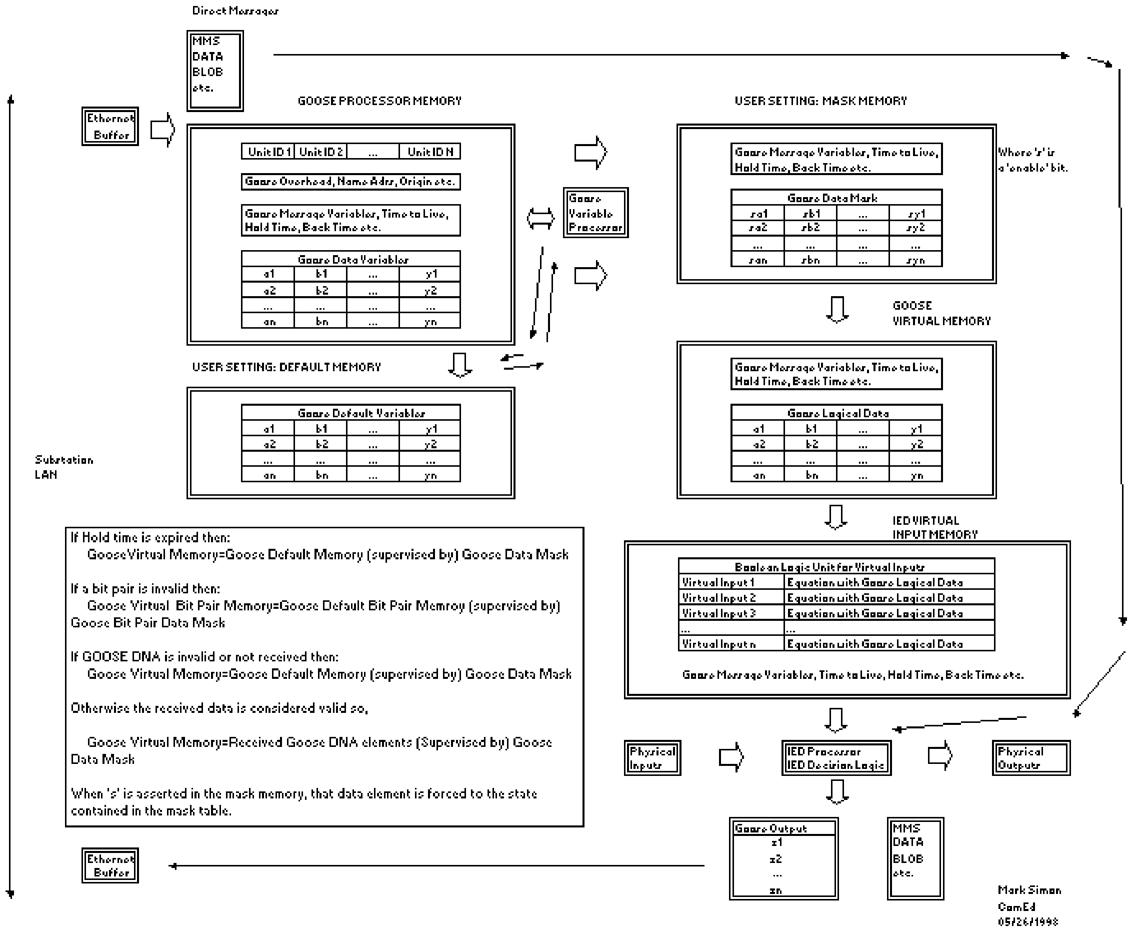
MMXU	Measuring (Measurand unit)
MMTR	Metering
MSQI	Sequence and Imbalance
MHAI	Harmonics and Inter-harmonics
MDIF	Differential Measurements
...more	

XCBR	Circuit Breaker
XSWI	Circuit Switch

Exhibit 5-1 High Level Logical Nodes

UCA GOOSE

The pictorial in Figure 5.3 represents a possible methodology in which the UCA GOOSE messaging technique can be utilized within an IED. The diagram is intended to show an IED's logical and functional operation rather than the exact method in which the UCA GOOSE would be handled. The arrangement here provides for default memory to handle initialization conditions along with bad data situations. In addition, data masking allows the user to force particular data elements to specified states for test purposes.



Goose Data Variables			
a1	b1	...	y1
a2	b2	...	y2
...	...	...	...
an	bn	...	yn

Goose Default Variables			
a1	b1	...	y1
a2	b2	...	y2
...	...	...	...
an	bn	...	yn

Goose Data Mask			
sa1	sb1	...	sy1
sa2	sb2	...	sy2
...	...	...	...
san	sbn	...	syn

Goose Logical Data			
a1	b1	...	y1
a2	b2	...	y2
...	...	...	...
an	bn	...	yn

Boolean Logic Unit for Virtual Inputs	
Virtual Input 1	Equation with Goose Logical Data
Virtual Input 2	Equation with Goose Logical Data
Virtual Input 3	Equation with Goose Logical Data
...	...
Virtual Input n	Equation with Goose Logical Data

Goose Output
z1
z2
...
zn

If Hold time is expired then:
GooseVirtual Memory=Goose Default Memory (supervised by) Goose Data Mask

If a bit pair is invalid then:
Goose Virtual Bit Pair Memory=Goose Default Bit Pair Memroy (supervised by) Goose Bit Pair Data Mask

If GOOSE DNA is invalid or not received then:
Goose Virtual Memory=Goose Default Memory (supervised by) Goose Data Mask

Otherwise the received data is considered valid so,

Goose Virtual Memory=Received Goose DNA elements (Supervised by) Goose Data Mask

When 's' is asserted in the mask memory, that data element is forced to the state contained in the mask table.

Figure 5.3 Possible UCA GOOSE technique

Operation:

The IED is continuously listening to the Ethernet for either directed messages or multicast messages. Directed messages that are intended for this IED, as defined by the destination identifier, would be sent directly from the communication receiver’s memory buffer to the IED's processor and serviced separately from GOOSE messages.
The IED shown in figure 5.4 maintains a GOOSE subscription list shown in the block diagram as Unit ID 1 through Unit ID N. When the receiving Ethernet memory buffer contains a GOOSE message that originated from a subscribed IED, the appropriate DNA elements from that GOOSE will be copied to the GOOSE Processor Memory. The GOOSE Processor Memory only maintains the DNA elements that the IED needs to function, although, it would be nice if the IED stored the entire DNA for diagnostic purposes.

A GOOSE Variable Processor continuously examines the GOOSE message variables such as time to live and hold time while making a judgment as to the validity of the GOOSE DNA. The GOOSE Variable Processor uses the information in the Default Memory to replace the GOOSE Processor Memory in a predictable manner. The user would have some sort of control over this. The key here is for an IED to have predictable data if the received data from a particular IED is either invalid, missing or too old. The GOOSE Variable Processor would be responsible for notifying the IED processor that there is new data. An area called MASK Memory is provided for test purposes. It allows, via programming, the user to force any elements of any of the subscribed GOOSE DNA to a particular state. This allows the testing of individual protection elements, logic functions and the disabling of certain elements without having to change the IED's Boolean logic set. This is meant for short-term testing. An alarm flag is sent by the IED to indicate that the IED is in a test mode. All of the preceding is used to form the IED's GOOSE Virtual Memory. Here resides the GOOSE DNA elements that the IED uses for processing. The IED has Virtual Inputs that are made up from the elements in the GOOSE DNA's that are retained in Goose Virtual Memory. The IED would have the ability to form Boolean Logic functions on any location in Goose Virtual Memory, allowing logical equations across a single GOOSE DNA or from multiple GOOSE DNAs. This allows a correlation to the series/parallel and diode logic that is used externally today. An example would be [(a1 'or' b1) 'and' (c1)]. The IED Processor monitors the IED's Virtual Inputs along with the IED's Physical Inputs, such as CTs, PTs and contacts, and forms its output depending on the functionality that it is designed for. The IED's output can be a contact, a GOOSE with its corresponding DNA, in addition to direct messages.

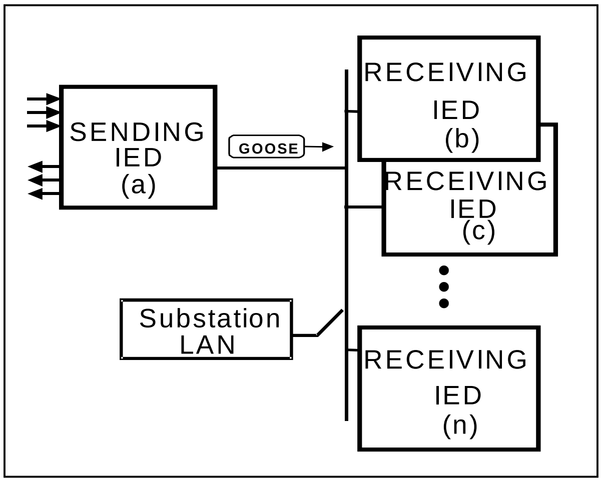


Figure 5.4
GOOSE Multicast Model

Origin of the "GOOSE"

One of the unique functional requirements identified for UCA was high-speed (goal of 4ms) device to ***multi***-device communications of simple binary state information. Inasmuch as sending multiple messages to multiple devices would incur an unacceptable time delay, an implementation was chosen that could send the same message to multiple devices simultaneously in a communication mode known as "multicast" (see Figure 5.4). As a multi-cast layer-2 message, the GOOSE is **not routable** however, it can be **"bridged"** over a wide area. The implementation of this function was done through the MMS information report service. The information report was used to deliver a binary object model (a collection of binary states of the device), known as the **G**eneric **O**bject **O**riented **S**ubstation **E**vent or **GOOSE**. It should be noted that when this concept migrated to IEC61850, the same name – GOOSE was used to describe a "user definable" dataset that could carry any type of data. Details on the new GOOSE can be found in the IEC GOOSE section below. In IEC61850, the Generic Substation Status Event (GSSE) is the bit-for-bit equivalent to the UCA GOOSE described herein.

GOOSE works in a model type known as "Publisher / Subscriber". In this model, the sending device "publishes" the user-selected state bits in the device. Any device interested in any of the states of the publishing relay is programmed to "subscribe" to the publishing device's GOOSE message.

The GOOSE message is launched under one of two scenarios. The first scenario launches a GOOSE on a change of state of any of the binary variables in the message. The second scenario launches a GOOSE message on a user-selectable periodic basis. The reason for the latter scenario is that in absence of a state change, there is no way for the subscribing device to determine that the publisher is alive. When the subscribing device fails to receive an expected GOOSE message, it can declare the publisher as "dead" and set default states on the binary variables expected from the publisher.
One risk in the multi-cast GOOSE is the potential lack of assured and timely message arrival and processing due to "Best Effort" protocol quality of service (QOS) and the variable communications latency associated with a shared medium network. Coexistence of mission critical control signals with non-mission critical data causes variation in the QOS for the mission critical data that must be managed carefully. UCA GOOSE achieves reliability through the use of repeated unacknowledged messages. This paradigm produces specific challenges in that repeated messages add to the network load and device processing. Network collisions problems have been eliminated with use of Layer 2 Ethernet switches when interfacing with full duplex devices. Message filters implemented in hardware can address device overload concerns by giving priority to mission critical messages related to a specific device and discarding others. Still, care must be taken to ensure that oscillography and other non-time critical data sent on the network are correctly managed at the application layer to prevent overloading the network or device buffers and delaying the control messages. In order for UCA GOOSE to be effective as a method to send mission critical data throughout the network, all of the above concerns must be addressed and enforced by all devices on the network.

The content of the GOOSE message can be broken down into three areas: a header, Dynamic Network Announcement (DNA) state information, and User State information. The header contains operational information about the GOOSE message such as the name of the sending device, the time that the GOOSE message was constructed, and the maximum time until the next GOOSE message. The Max Time until next GOOSE is used to detect failure either in the sending device or in the network itself.

The DNA and User State Information bits are the "payload" of the GOOSE message. The GOOSE defines 32 DNA bits and 64 User State bits for a total of 96 bits of state information in one message. Inasmuch as 96 bits may be restrictive in some applications, the documents allow for expansion of the User State bits up to 512. Note that there is no restriction on the number of GOOSE messages that a device may launch.

The Dynamic Network Announcement bit pairs were originally designed to facilitate connection between devices through the definition of "standard" bits. Examples include Trip, Close, BFI, etc. The ability of today's IEDs to provide multiple device/line protection made such standard assignments limiting. As a result, the DNA bits have become user-definable.

The delivery of the GOOSE object is through the connectionless ISO stack, which means that there is no specific destination address. As such, some address must be entered for the Ethernet receiver to resolve. Note that all multi-cast messages need to be evaluated by all receivers to determine if the message is to be evaluated. Typical Ethernet receivers can optimize this function through the creation of an address mask and subsequent hardware filtering of the Ethernet address. Only if the address passes the filter test is it sent on for additional processing. Performing this function in hardware minimizes software involvement and also allows for prioritization of multicast message. One implementation technique requires the user to set the send and receive addresses in each device (a 48-bit address is required for each publisher, and each subscriber must also be configured with the 48 bit addresses it is to receive). A second technique is to use logical names in the configuration of the publishers and subscribers and then allow each IED to automatically detect the devices on the network and create a logical name to address mapping.

GOOSE Applications

The UCA GOOSE message has followed the adage necessity is the mother of innvention". The availability of GOOSE based virtual wiring has spawned many applications that use GOOSE both locally within a substation as well as between substations.

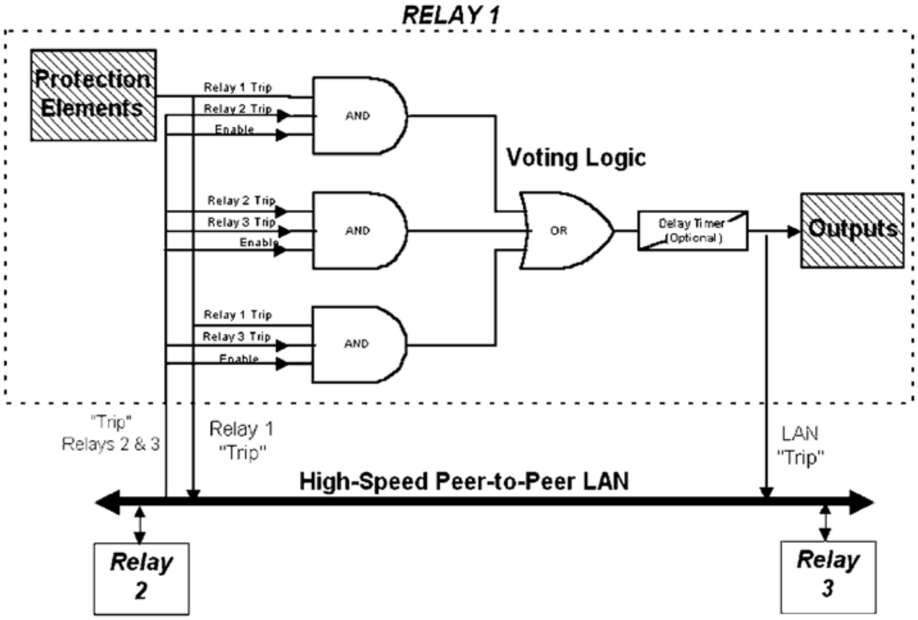


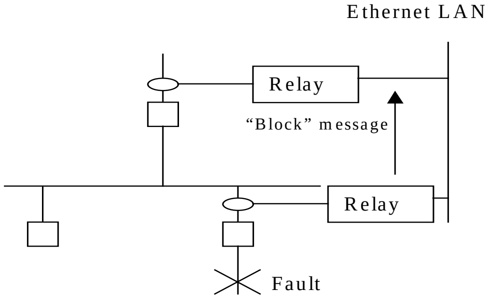
Figure 5.5

Voting: In the art and science of protection, part of the "art" is creating a balance between the security and dependability of a protection scheme. One technique that is used in mission critical application is the concept of voting (see Figure 5.5). Voting says to issue a trip only if 2 out of 3 relays say trip. To implement this function, relay 1 needs to get trip information from relays 2 and 3, relay 2 needs to get trip information from relays 1 and 3, etc. Each relay is required to implement the voting logic internally and each relay has to subscribe to the other's trip messages. Since each relay has the voting logic internal to itself, failure of a single relay does not fail the voting scheme.

What is interesting to note is the performance of the scheme under a "dead GOOSE" scenario – that is – when a particular relay fails to send a GOOSE message in the allotted time frame. When this happens, a default state is assigned to the expected data. Depending on how the default is set by the engineer, the voting scheme will default to be more secure or more dependable. For example, if relay 2 fails and the trip input to relay 1 is defaulted to "no trip", for a trip to occur, both relays 1 and 3 must issue a trip thus defaulting to a secure state. On the other hand, if the failed input from relay 2 is set to "trip", the system defaults to a dependable state in that if either relay 1 or relay 3 say trip, the system will trip.

Bus Blocking

In many distribution station applications, an incoming feeder has a breaker feeding a bus with multiple feeders exiting from the bus (see Figure 5.6). Typical protection calls for an instantaneous overcurrent function that is coordinated with the overcurrents on the underlying feeders.

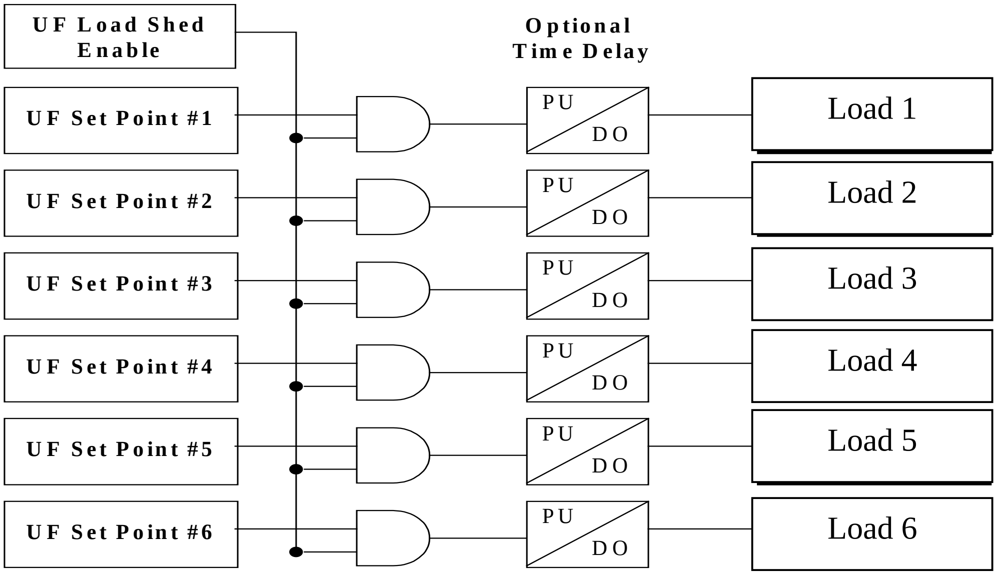


Bus Blocking Figure 5.6

Coordination typically can be translated as "time delay". Application of GOOSE messaging between the underlying feeders and the incoming feeder breaker can optimize this situation. When any of the feeders detects an overcurrent, it sends a "block" message to the incoming feeder telling it not to trip. Such communication can speed up protection for bus faults and add security for feeder faults.

Load Shedding

Typical load shedding applications in a substation require the addition of a separate under-frequency relay followed by wiring from the load-shed relay to any breakers to be tripped under an under-frequency condition. Reality is that most breakers in a substation are connected to the tripping output of at least one relay in a substation. Connecting these relays via an Ethernet network, load shed becomes a GOOSE message to trip the



Distributed Load Shedding Figure 5.7

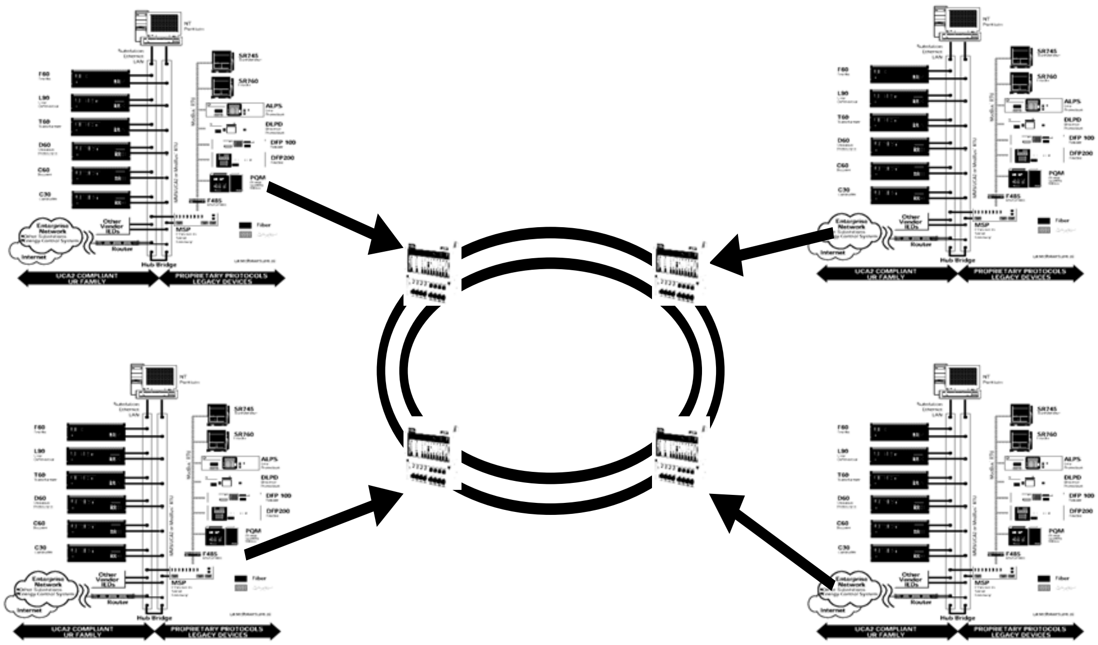
appropriate breaker (Figure 5.7). With some additional logic, the engineer could actually create a rotating schedule of loads to shed. Clearly, a restoration scheme could be created in similar manner. Since this scheme could be loaded into any relay, redundancy is also easy to implement.

Wide Area GOOSE (WAG)

As mentioned earlier, the GOOSE message is not routable, however, a number of multiplexers, switches and routers are capable of "bridging" GOOSE messages between substations over Ethernet. With this configuration, one is able to perform functions such as transfer tripping, pilot based protection, high speed data transfer, and in general, have a foundation for next generation power system control. Caution need be taken when implementing such a scheme as too many GOOSE messages can clog the network. The IEC GOOSE resolves this issue through the use of VLANs (see IEC GOOSE section below). Application of these protocols will eliminate non-essential GOOSE traffic in a wide area application as shown in Fig 5.8.

WAG timing tests have shown that Ethernet bridging over SONET only adds 1ms plus fiber delay to GOOSE messaging times. Typical fiber delay is 5 usec/km. For example, if a connection to a substation 100 km away is desired, the time delay can be calculated as:

GOOSE Time + Multiplexer Time + Fiber Delay = Total Time Delay
(4ms +   1ms   +   0.5ms = 5.5 ms)



Wide Area GOOSE (WAG)
Figure 5.8

Using GOOSE to transmit other types of digital information

The UCA GOOSE message is optimized for reliable exchange of binary state information, and does not specify how to transmit more complex data types such as bytes, integers, strings, floating point numbers, or advanced data structures.

In the UCA GOOSE, first 32 bit pairs are reserved for transmission of DNA information. The remaining 64 bit pairs (User State) can be used freely, making it possible to transmit other types of digital information (up to eight bytes, four 16 bit integers, or two single precision floating point numbers etc.).

In order to use advanced data types, the protective device must be equipped with an adequate set of programming tools for encoding / decoding and using various data types. This can be achieved through simple, ASCII based logic equations, or more conveniently through a graphical user interface based logic programming environment. Figure 5.8 shows a simple example (screen capture) illustrating how user programmable logic blocks can be used to transmit single analog values by using a UCA 2.0 compliant GOOSE message. The process starts by taking individual phase current magnitudes (1), and adding them up (2) to calculate total current magnitude. The resulting single precision floating point number is then fed to a special purpose "bit pair encoding block" (3) necessary for mapping the 32 bit floating point number into 64 bits compliant with the GOOSE User State field definition. The 64 bits (32 bit pairs) are transmitted (shown as four 16 bit integers) to the GOOSE output block (4).   It should be noted that although this functionality can be implemented, it does preclude interoperability. The ability to send analog data through this multicast message is addressed in the IEC GOOSE section below.

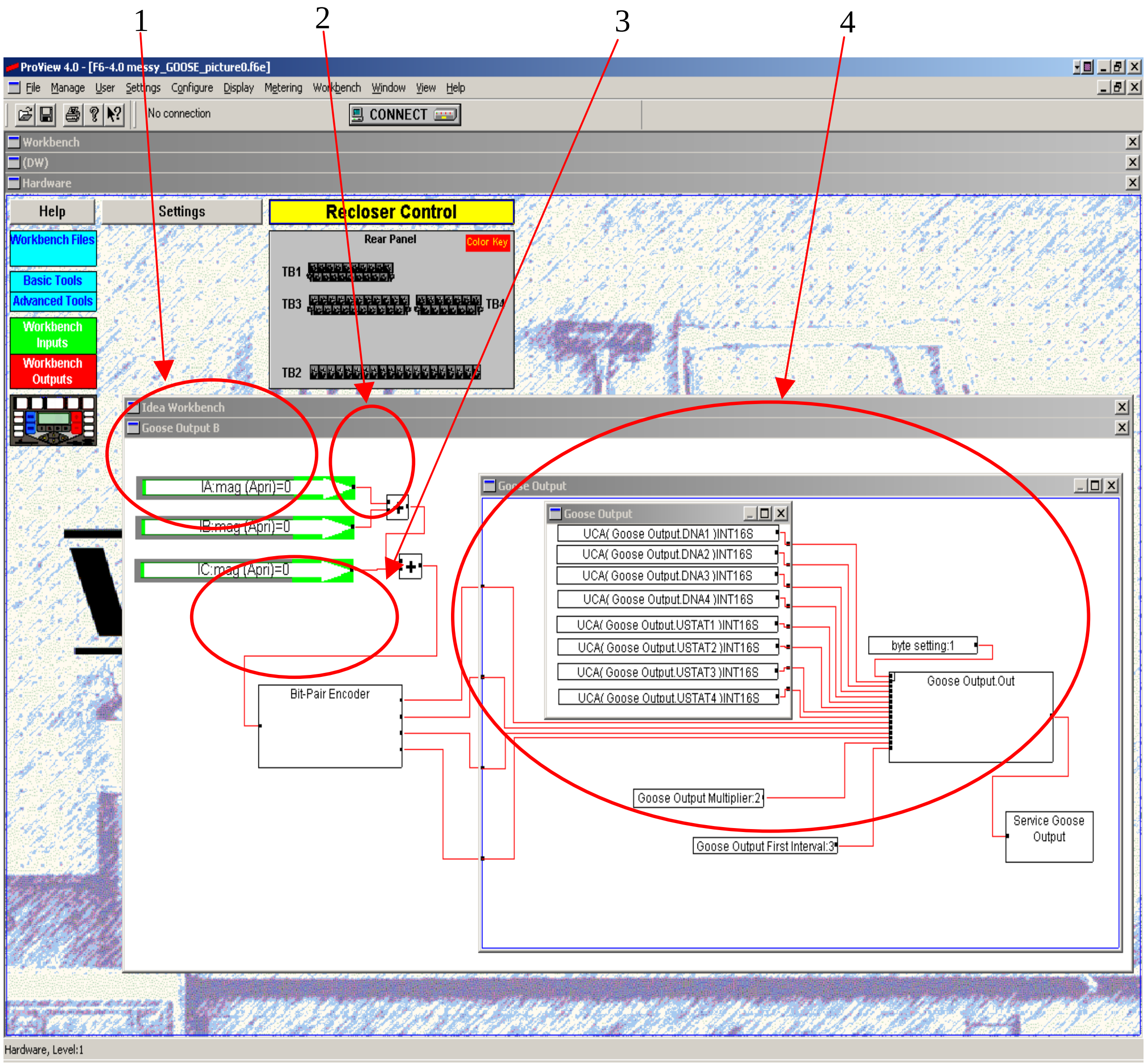

1
2
3
4
ProView 4.0 - [F6-4.0 messy_GOOSE_picture0.f6e]
File Manage User Settings Configure Display Metering Workbench Window View Help
No connection
CONNECT
Workbench
(DW)
Hardware
Help
Settings
Recloser Control
Workbench Files
Basic Tools
Advanced Tools
Workbench Inputs
Workbench Outputs
Rear Panel
Color Key
TB1
TB3
TB4
TB2
Idea Workbench
Goose Output B
IA:mag (Apri)=0
IB:mag (Apri)=0
IC:mag (Apri)=0
Bit-Pair Encoder
Goose Output
Goose Output
UCA(Goose Output.DNA1)INT16S
UCA(Goose Output.DNA2)INT16S
UCA(Goose Output.DNA3)INT16S
UCA(Goose Output.DNA4)INT16S
UCA(Goose Output.USTAT1)INT16S
UCA(Goose Output.USTAT2)INT16S
UCA(Goose Output.USTAT3)INT16S
UCA(Goose Output.USTAT4)INT16S
byte setting:1
Goose Output.Out
Goose Output Multiplier:2
Goose Output First Interval:3
Service Goose Output
Hardware, Level:1

Figure 5.9 Analog GOOSE data formatting and transmission block

The analog GOOSE transmission mechanism shown in Figure 5.9 has successfully been applied to dual tap changer load balancing applications and demand current based load shedding in a loop based distribution system protection application. When convenient, floating point data can be scaled and converted into 16 bit integers thus increasing the total number of transmitted analog variables to four.

It is important to note that analog data in general, changes very rapidly, making it appropriate to abandon the default ‘change of state’ triggered GOOSE transmission in favor of a better suited “User-selectable periodic” GOOSE. The GOOSE update rate can be selected to match the dynamics of the analog data being transmitted, and can, when appropriate, be combined with the “change of state” approach. In the IEC implementation, the periodic transmission of data is addressed by the Process Bus.

Example shown in Figure 5.7 emits a new GOOSE message 4 times per cycle. Such an analog information update rate creates additional Ethernet network traffic, which must be taken into account during the communication network planning stage. Currently available 100MBps, managed switch based Ethernet technology, can easily cope with the typical 0.2% load increase generated by each GOOSE emitting device (4 frames per 60Hz cycle). Once combined with IEC GOOSE 'layer 2 priority tagging' periodic GOOSE update strategy ensures timelines and reliability of the analog GOOSE message delivery.

The IEC GOOSE

The original UCA GOOSE message uses the OSI type Ethernet Frame, and lacks provisions for priority tagging normally found on Ethernet II type systems. Regardless of its short length, UCA GOOSE is relatively inefficient, using a total of 259 bytes to transfer only 96 bit pairs / 24 bytes of user-controlled information.

Recent standardization efforts within the International Electrotechnical Commission (IEC61850-7-2) resulted with a number of enhancements to the original GOOSE specification. Details of this work can be summarized as follows:

- Unique Ethernet frame type was reserved with IEEE
- Layer 2 priority tagging was added to the specification making it possible to isolate time critical protection traffic from HMI, SCADA, and other lower priority network traffic.
- The IEC GOOSE supports Virtual LANs or VLANs. A VLAN is a group of devices that reside in the same broadcast domain, that is, if an Ethernet Broadcast message is sent on a particular VLAN, only the devices configured on that particular VLAN will see the broadcast message. The new feature facilitates the transmission of information from one location to only those devices on the same VLAN.
- Message was split into two sub types and renamed as follows:
  - GSSE is a new name for the message format, which is backwards compatible with the UCA 2.0 GOOSE.
  - GOOSE is a name given to a new enhanced IEC data frame (Although very confusing, this naming approach should not have major impact on the user community, and is expected to be handled by the device manufacturers.)
- New IEC GOOSE was made leaner by eliminating some of the data overhead associated with the original UCA GOOSE specification.
- New IEC GOOSE has removed the DNA block and "bit pair" specification, converting the entire user data payload into a data pool that can be freely configured to transfer any type of information (logic bits, characters, bytes, integers, floating point numbers etc.).
- The new IEC GOOSE allows message length to be configurable, thus extending IEC GOOSE length from the original 259 bytes up to a maximum

permitted Ethernet frame size (1518 bytes). The original limitation that all information must be contained within a single GOOSE message has been retained.

- New GOOSE supports additional services for interrogation of individual data set elements names (self description).

Chapter 6; Network Management

The first part of this chapter documents some of the requirements for testing and monitoring a substation LAN system from the utility application user's point of view. Although the individual tasks necessary to test and maintain an all-digital substation may well be different from conventional hard-wired installations, it is assumed that the basic activities of isolating power apparatus, invoking backup schemes, verifying configurations and investigating power system operations will remain much the same regardless of the technology employed. Future enhancements of these requirements may evolve to incorporate the advanced native features intrinsic to the LAN technology.

IED Configuration Software

It is assumed that all IEDs will continue to require either a direct physical or a virtual connection to be made between a proprietary software configuration package or generic terminal emulation program and the IED in order to configure the device parameters and gain access to all of the internal functions supported. Although the present practice of connecting a notebook computer directly to the front port of the IED will likely be eventually phased out in favor of remote access solutions via the LAN, it is assumed that some activities will continue to need to be performed at the relay, particularly during initial commissioning. It is also assumed that each individual vendor's IED configuration methodology will continue to be unique to each device or product family. Continuous innovation in IED design and competitive market forces would tend to preclude standardization of individual IED configuration software, though some activity is underway in this regard.

Substation LAN Application Management Software(SLAM)

The management of an overall substation LAN consisting of a number of separate IED applications from a variety of vendors is a totally separate issue from individual device configuration. At a system level, substation LAN application management software is required to monitor and control the logical linkages between separate protection and control schemes implemented with distributed IEDs. These logical linkages are directly analogous to the individual physical connections and test/interface devices used with existing technology and are the means of interconnecting physical "black boxes" into protection and control systems. An implicit requirement of the SLAM software is the ability to view/alter the configuration variables and/or bit masks in the GOMSFE models associated with individual messages. The SLAM software is essentially the user interface to permit configuring the inter-scheme GOMSFE object connections in a substation network.

Scope of SLAM Functionality

It is assumed that the scope of SLAM software functionality will include overall network management and configuration, MMS object browsing, end-to-end application continuity and exception monitoring, and detailed examination and control over all configuration variables and bit masks contained within individual objects. Examination and control implies identifying logical states, isolating individual points or bits, and forcing the state of individual points or bits. The overall SLAM package would allow the user to monitor, isolate and test all discrete (Boolean) inter-device messages and status.

The SLAM software is not expected to support or be a replacement for analog test and fault simulation equipment used to emulate and measure power system conditions for the purpose of IED testing. An exception might be a LAN interface to control the operation of automatic protection and control test equipment. Similarly, SLAM is not necessarily required to support the recovery and display of IED captures of sampled analog data such as DFR reports; other applications are already available for these purposes. (SLAM could in fact support this function or could be the user interface to launch these applications.)

SLAM Implementation

Such a substation LAN application management software package would typically run on a PC connected to the substation LAN and would be physically located at the station. Remote access via a WAN or other connection to the engineering office would also be supported. SLAM is a local function running continuously. Remote access would consist of running the user interface portion of SLAM only at another location. Because of its generic nature, the SLAM software would only interact with each IED via the implemented GOMSFE models and, by definition, would not support any custom variations or features not supported in GOMFSE. All signals over which users would exercise control, either during commissioning, routine testing, system re-configuration or any other likely operational circumstance, would have to be visible to the SLAM software via each IEDS network interface. The status of all off-nominal configuration data, especially off-nominal changes, would still be reliably maintained within each individual IED.

By its nature, the SLAM software would be separate from the regular station operational Human Machine Interface (HMI) software and only would be used by qualified staff with appropriate access security privileges. The SLAM software itself requires its own HMI designed to support local and remote access. At the local station, the SLAM software and/or its HMI could possibly be another multi-tasking application running on the main operational HMI PC.

SLAM Functionality

The SLAM software functionality could be limited to IED object configuration, but ideally it would be an integrated package consisting of a number of generic and specialized functional modules, tailored for the specific requirements of a substation LAN. In addition to a generic Ethernet network management tool and an MMS browser, the SLAM software would support all of the functionality required to emulate existing systems, with LAN-equivalent capability to identify and alter the state of all isolation and test variables used to interconnect separate schemes and power equipment.

The SLAM software would have a hierarchical structure beginning with a screen to allow the user to establish access rights to the substation LAN. The following screen presented would then identify and display graphically the present configuration of the LAN along with key summary information about the operation of each device such as on-line, off-line, test mode, etc. This part of the SLAM functionality would essentially incorporate the features of a commercial network management software package. An important aspect at this level, particularly for LANs employing redundancy, is the ability to manage the network infrastructure including hub and switch configuration and fail-over status. In this context, SLAM is essentially the user interface to a commercial network management tool.

Subsequent screens would allow the user to access any individual IED and identify and view all of the objects configured. This functionality would essentially incorporate the features of a MMS browser software package. SLAM utilizes the available security features in the network infrastructure and individual IEDs to prevent unauthorized access to devices, especially from remote users.

The user would then be offered screens permitting read/write access to the actual configuration variables, bit masks, flags and other attributes of each object model within a particular IED. Again, this access would be limited to those IED features which are network-visible. At this level, the SLAM HMI would be used to provide appropriate human interpretation in the power system application context of the objects to be examined or altered. One way to do this would be via tag name descriptions in the SLAM HMI.

System Integrity Monitoring

Another important aspect of SLAM functionality is the continuous end-to-end integrity monitoring between IED applications. One approach would be to establish a monitoring application to “listen” to all of the pre-determined IED logical interconnections. Any discrepancies would be reported by generating appropriate operator alarms for delivery to the SCADA system. However, from an operational point of view, this could lead to a system at least equal if not greater in complexity to the primary logical interconnections between fundamental IED applications. The creation this type of monitoring system requiring separate complex configuration and maintenance in parallel with the primary IED applications would therefore be costly and undesirable.

A better solution would be to establish an “exception page alarm object” in each IED. Each individual IED would keep track of message failures due to lost connections or sessions, LAN congestion and other disturbances. Assuming the system was originally set up correctly and thoroughly verified during commissioning, it therefore becomes necessary to know only about exceptions that subsequently occur during the course of normal operations and maintenance. Exception conditions would encompass everything from gross failures to performance degradation (e.g., excessive message delivery times). Any off-nominal condition or configuration change due to a test activity in progress would be logged as an exception. The SLAM software may also be used to collect statistical information about normal system operation such as average message delivery times, number of retries, etc. Appropriate enhancements to the GOMSFE objects or IED linkages to a network management protocol may be required to accomplish this.

The time, type of message, pending operations and other useful diagnostic information could be recorded at the time the failure or off-nominal configuration was detected. Multicast message failures for applications with inherent end-to-end continuity verification, such as the GOOSE object, would also be logged in the IED alarm page. For example, an IED, upon determining a GOOSE sequence number was missing, could place an exception in the alarm page. In certain situations, this exception data might also be read directly from the IED by the main operations SCADA system and used to generate appropriate alarm messages for the HMI.

In other, more complicated situations, it is anticipated that programmable logic built into the SLAM software may be required to interpret the significance of an end-to-end failure between IED applications and then generate an appropriate alarm for the SCADA operations HMI. An interface mechanism would be required to transfer the alarms to the operations HMI, depending on whether the SLAM software is resident in the same or a separate computer. Programmability at this level in the SLAM could also be used to initiate contingency actions, such as automatically re-configuring part of the network or establishing some other backup strategy. This, however, evolves into a form of “adaptive relaying” at the network level, which for now will be left for future study and exploration.

Protection and Control Signal Test Generation

The SLAM software should also support the capability to incorporate user generated test patterns to “exercise” a particular IED or group of IEDs under test to simulate power system events of interest. These tests would be to verify the overall functionality of the IED(s) as applied in a particular protection and control scheme, not to perform object model conformance testing or device type testing. The test patterns would be organized in a script or equivalent format and saved as files. The ability to synchronize the issuing of individual scripts with the system clock, external triggers, results of previous events, etc., and also specify the intervals between successive scripts is also a requirement.

As a minimum, the responses received from the IED(s) under test would be stored in a readable format similar to a SER report along with the time received and other pertinent information. In some situations, especially those schemes involving multiple IEDs, it could be necessary to use programmable logic to properly decipher the responses, especially in automatic test setups.

Optional Features / Enhancements

The user interface for the SLAM software could also be used for other peripheral purposes. For example, an optional feature could be integrated into the overall SLAM functionality to permit launching the individual IED vendor configuration packages where appropriate. Links could be established to supporting documentation covering the installation such as engineering drawings, configuration files, test-procedures for specific IEDS, power equipment data, etc. The real-time status of inter-device messages could also be displayed on the SLAM HMI. In this way, the SLAM computer could be considered to be a general maintenance resource point for a substation as well as a particular tool to manage the network and all of the individual devices.

The above SLAM concepts are intended to serve as a basis for further thought and discussion, leading to a formal specification for a generic SLAM software package. SLAM software is essential for the successful deployment of a substation LAN system in order to provide users with the same degree of control and monitoring over the basic infrastructure as we presently have with conventional technology. A well integrated SLAM implementation could also offer significant improvements in efficiency over the conventional manual systems presently in use. The ease with which substation LAN systems can be configured and maintained in a secure power system environment will be the key to user acceptance.

Network management and application development tools

Network analyzer

Network analyzers are used to capture packets or frames of information flowing through the network. A packet (or frame) typically includes three fundamental types of information: source and destination addresses, data, and control bits. Different network protocols have different packet formats. Analyzer features required for C37.115 include:

- Packet capture, including address filtering, which ensures that only packets with specific source or destination addresses are captured.
- Packet decode, which is specific to each protocol. The level of decoding varies from simple decoding of packet type and address to sophisticated decoding, which interprets the data portion of the packet for commands, such as file open or file read.
- Packet playback or generation, which transmits packets from the analyzer onto the network.
- Other functions, such as graphical displays, current and trend statistics, and programmable operations, which assist the user in displaying and interpreting captured data.

Network management stations

Network management stations are used to provide graphical representation of the network configuration and to enable the network engineer to monitor the network and collect utilization statistics, alerts, and other pertinent information from all network nodes. The network management stations should be based on SNMP standards, and SNMP agents running on the network nodes shall collect and summarize statistics that are sent to the management station's management information base.

Vendor supplied resource management and test configuration tools should be used to reconfigure the test configuration on the network.

Monitoring software

Vendor supplied monitoring software running on the individual network node should be used to collect intranodal information; e.g., cache hits, send/receive buffer utilization, memory utilization and file open/reads/writes.

The monitoring software shall be used to confirm that a baseline test load is representative of the real-world operating load (it creates the same level of activity for key system parameters) on a comparably configured node. It shall also be used to measure the impact on that particular node as the test load is increased to reflect more IEDs or network activity.

Server-based databases

Server-based databases should be used for monitoring the resource utilization of the database. Similar to monitoring software running on a server, database utilization vendor supplied software shall be used to collect statistics pertinent to the database, such as cache utilization, file read/writes, connected IEDs, average response time for database queries and average record size.

Test Methods and Measurements

C37.115 requires the following test methods and measurements.

Application response time testing

Application response time testing shall be used to measure how long it takes an application to complete a series of tasks, and it best represents the utility's perception of the network system (application network operating system and network components). For a presentation layer, the test shall measure how long it takes to switch between different applications tasks or to load new overlays. Tests shall be run at various loads, with differing numbers of real or emulated IEDS, to create a load versus response time curve for each application tested.

Application tests shall use a series of commands that execute typical network activity, such as file opens, read, writes, searches, and closes to provide a representative load model. The time it takes to complete commands shall be measured for each workstation running under test.

Response time testing shall include monitoring the system for reliability. A reliability problem, such as a high number of dropped packets at a router or server, or a high number of bad packets because of a malfunctioning network component, can significantly impact response time measurements. Network analyzers shall be used to monitor the system for errors during testing.

Application feature/functional testing

Feature testing shall be used to verify individual commands and capabilities of the application. Feature testing shall be performed with minimal to light loads to measure the IED's interface and application operations or transactions invoked by the client IED. Functional testing shall be used to verify that the application's multi-IED characteristics and background functions work correctly under heavy loads. Functional testing shall be performed under loading that closely models the substation's real-world operating environment.

Regression testing

Regression testing shall be used to compare the performance, reliability, and functionality of new release of hardware or software to the current release to ensure that the product upgrades will not adversely impact the operational network.

Throughput testing

Throughput testing shall be used to measure data transfer rates (e.g., kilobits per second or packets per second) to evaluate performance, find bottlenecks, compare different products, and size individual components of the network.

Acceptance testing

Acceptance testing (including response time, reliability, and feature/functionality tests) shall be used to ensure that the new system is stable and provides acceptable performance in its initial release.

Configuration sizing

Results from application response or throughput tests shall be used to size network components by evaluating load versus response time for alternative configurations. A target response time shall be specified by the utility to select the configuration that provides the best cost/performance margin for the maximum number of IEDs on the network.

Reliability testing

Reliability tests shall be run for an extended period of time (24 to 72 hours), under medium to heavy load to monitor the network for errors and failures.

Bottleneck identification and problem isolation

Maximum sustainable throughput on each system component shall be measured or calculated to component capacity limits. The difference between the maximum capacity of individual components and the maximum sustainable throughput of the system shall be used to determine where system bottlenecks and excess capacity exist.

Chapter 7 Security

The purpose of this section is to provide an overview of security options that should be considered when implementing UCA2. Security should always be matched to the utility's communication architecture and operating procedures. In this context security is first addressed from a communication architecture point of view with emphasis on entry points that represent a security concern.

An example security policy is provided so that the reader can tailor the policy to match specific requirements for a utility's communication architecture and operating procedure. Implementing the security policy focuses on password authentication and encryption, which must be matched to the tailored security policy.

Communication Architecture

UCA is adaptable to many communication architectures, but it is most commonly implemented over those architectures that require peer-to-peer communication between IEDs. The emphasis on interoperability between these IEDs is implemented in accordance with IEC 61850. An overview of the communication architecture is discussed in the next Chapter.

SCADA and protection networks:

SCADA and protection can be implemented on the same network, but to enhance security many utilities use separate networks. If implemented on the same special network, the security policy must address the possibility that a SCADA engineer or operator can access protection IEDs if they gain access to the protection engineer's passwords.

If implemented on separate networks, security is enhanced because SCADA engineers and operators are communicating over physically separate networks. This implementation requires dual communication ports to the IEDs that serve SCADA functions as well as protection functions.

As an alternative to physically separate networks, the judicious use of Ethernet 802.1q VLANs can provide this security through isolation, by having the critical traffic on its own VLAN. This approach requires that for all the network's connections to non-secure data sources, the ingress (switch) ports must either assign the frames' VLANs (called "port-based" VLANs), or must only accept allowed-VLAN frames; this makes it difficult for a hacker (at a non-secure source) to emulate a critical-traffic message.

This "port-based' VLAN feature of switches is simple and attractive as it avoids the major issues of finding IEDs which support VLANs, and then configuring their VLANS correctly; however for the teleprotection IEDs, life is not so simple as these devices will require at least 2 VLANs (for their critical and non-critical communication functions).

One solution for these teleprotection IEDs would be to use devices with dual communication ports connected to separate ports of a "port-based" VLAN switch; one port would be configured for the protection traffic's VLAN and the other for its TCP/IP services' VLAN (browsers etc.).

A more attractive solution for teleprotection IEDs would be to use devices with sufficient processing capability so they can be programmed to include "native VLAN tag" support. If properly implemented, this approach enhances security by tagging (and filtering) individual frames, and effectively implements "protocol based VLANs". For example, (protection) engineering access using FTP/Telnet protocols can be assigned to one VLAN, real time protection traffic (IEC 61850 GOOSE and IEC 61850-9-2 process bus) to the second, and the SCADA traffic (DNP3 or SCADA portion of IEC 61850) to the third. Native (protocol based) VLAN support is the most advanced form of VLAN capability. It eliminates the need for separate physical ports by implementing all security functions on the logical level. Actual presence of the second Ethernet port is still desired, but can instead be delegated to a redundant network connection. As with the use of port-based VLANS, "native VLAN tagging" also requires the use of VLAN capable Ethernet switches (layer-2 infrastructure). In addition to the above, VLANs can also be used to provide multicast domain partitioning (not necessarily a security function).

Requirements for deploying network security in the substation:

Communication network security may be required in the substation when data is exchanged between substation IEDs and nodes external to the substation. If remote access to the substation IEDs does not require a substation gateway, but is instead implemented through a router, then communication security should definitely be considered.

The user should define where in the communication stack security will be implemented. Irrespective of where in the stack security is implemented, the following basic services should be provided. Depending on where in the stack the security is implemented, it is possible to provide some or all of the services described. In some cases, it does make sense to provide some capabilities at one layer and other capabilities at a different layer.

- Key management, including the negotiation of keys and storage of keys.
- Confidentiality.
- Nonrepudiation.

- Integrity/Authentication.
- Authorization

Communication entry points of concern:

Although more expensive, Virtual Private Networks (VPN) and leased-lines are inherently more secure than operating over public networks; e.g., Internet. However, in either case it is always wise to include an Intrusion Detection System (IDS) to monitor all communications and be able to determine and quantify potential security attacks. Typical substation vulnerabilities to cyber attack are access to modems and network interfaces that connect to the substation controller or directly to an IED. Cyber attacks and electronic sabotage targeted against these vulnerabilities have the capability to change protection settings and metering data.

Consequences of an electronic intrusion into a SCADA system, controller, or IED could be as severe as physical sabotage. Once an intruder gains access, it is possible to:

- Shutdown the SCADA system, either immediately or in a delayed manner.
- Steal or alter metering and management data gathered by the SCADA system.
- Shut down a substation, or any portion of a subsystem controlled by the compromised IED, either immediately or in a delayed manner.
- Change protection device settings to degrade the reliability of the IED and, subsequently, the electric service provided by the substation.
- Gather control and protection information that could be used in a subsequent attack.
- Change or perturb the data in such a manner as to trigger an inappropriate action by an IED.
- Plan malicious code that could later trigger a delayed or coordinated attack.
- Use the SCADA system as a back door into the corporate IT system to obtain customer credit and personal identity information used in electronic theft.

SECURITY POLICY

All security policy statements should include purpose, scope, policy requirements (sponsoring organization, application), enforcement, and definition of terms. Security policies should be defined for application service provider, acquisition assessment, acceptable use, risk assessment, audit, server security, encryption, password, dial-in access, remote access, router security, virtual private network, wireless, etc.

Secure remote access (any access to the utility's corporate network through a non-utility controlled network, device, or medium) must be strictly controlled. Control should be enforced via one-time password authentication or public/private keys with strong pass-phrases. At no time should any employee provide his or her login or email password to anyone, not even family members. A strong security policy for remote access requires the following:

- Employees and contractors with remote access privileges must ensure that their personal computer or workstation, which is remotely connected to utility network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.
- Employees and contractors with remote access privileges to utility network must not use non-utility email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct business; thereby ensuring that official business is never confused with personal business.

- Routers for dedicated IDSN lines configured for access to the utility network must meet minimum authentication requirements of CHAP (Challenge Handshake Authentication Protocol) is an authentication method that uses a one-way hashing function. Data Link Connection Identifier (DLCI) is a unique number assigned to a Permanent Virtual Circuit (PVC) end point in a frame relay network. DLCI identifies a particular PVC endpoint within a user's access channel in a frame relay network and has local significance only to that channel).
- Reconfiguration of a home user's equipment for the purpose of split-tunneling defined as the simultaneous direct access to a non-utility network (such as the Internet or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into the utility's corporate network via a VPN tunnel. Virtual Private Network is a method for accessing a remote network via "tunneling" through the Internet. Dual homing is not permitted at any time.
- Frame Relay must meet minimum authentication requirements of DLCI standards.
- The utility’s organization that is responsible for managing Remote Access Services must approve non-standard hardware configurations, and the organization responsible for managing Information Security (InfoSec) must approve security configurations for access to hardware.
- All hosts that are connected to the company’s internal networks via remote access technologies must use the most up-to-date anti-virus software. This includes personal computers.
- Personal equipment that is used to connect to company's networks must meet the requirements of utility-owned equipment for remote access.
- Organizations or individuals who wish to implement non-standard Remote Access solutions to the utility’s production network must obtain prior approval from the utility’s organization that is responsible for managing Remote Access Services and InfoSec.

PASSWORD AUTHENTICATION

Security transformation is used to provide various security services such as peer entity authentication, data origin authentication, confidentiality, integrity and non-repudiation. Security transformations include encryption, hashing, digital seals and digital signatures.

ENCRYPTION

Compliant implementations should support the Data Encryption Standard (DES). Compliant implementations should also support both HMAC-MD5 defined in RFC2403 and HMAC-SHA defined in RFC2404 as authenticators with an output of 96 bits(96 bits was chosen because it ensured alignment for IPv6). Other cipher documents include Blowfish-CBC, CAST-CBC, and 3DES-CBC (all optional to implement). FIPS 197 defines an Advanced Encryption Standard (AES) which provides enhancements to DES.

Software solution

Software encryption can be the most efficient solution for new IEDs. But if software encryption must be added to existing IEDs, it can be very expensive. Furthermore, existing IEDs may not have sufficient computer processing or memory to add encryption software.

Hardware solution

Affordable hardware encryption is available today. These hardware components are inserted between an existing modem and the communication processor of an IED. Some encryption hardware is designed for a specific communication protocol; others are designed to operate over several communication protocols.

UTILITY APPLICATION CONSIDERATIONS FOR SECURITY FOR REMOTE ACCESS

Station Security is a growing issue within Utility Companies. However, many feel it is important that password security does not adversely impact productivity. Typically, the Utilities Field Relay Department is responsible for servicing the relays and they are also responsible for managing the passwords that are applied to these relays. If anything other than a factory default password is used on the relay, then the password(s) needs to be documented and stored in a secured but accessible location. A commonly held view within Utility Relay Groups today is that password protection is not necessary for relay equipment (use default passwords instead).

For a given Station, it is argued that one must have access to the company communications, know the communication parameters (i.e. LAN, WAN, Dial-up), have proper password/secure ID and also have the proper relay software (and version). This would seem to make remote access inherently secure without the addition of a relay password(s). This psychology and procedure could change as Utilities become more concerned about improper access to station equipment via outside communications.

Chapter 8: Architecture, Hardware Performance and Reliability

Physical layer hardware

LAN Topology

The manner in which LAN devices are interconnected is described by its topology. The most common topologies in use are the bus and star. In a bus arrangement, all devices are connected along a single type of media, generally coaxial cable. In a star arrangement, all devices are connected individually to a central hub device that distributes the LAN information to all other connected devices. This arrangement allows additional devices to easily be added to the LAN.

LAN Media

The physical media that allow devices to be arranged in a LAN are generally copper wire based or fiber optic cable based. The copper wire may be coaxial cable, either *thick Ethernet* using RG8 coaxial cable or *thin Ethernet* using RG58 coaxial cable, or as now much more widely used unshielded twisted pair (UTP) where two copper pairs per connection are required. UTP is terminated in a connector known as an RJ45.

UTP is used in 10 Mbps (10Base-T) and 100 Mbps (100Base-Tx) LANs. The 10 Mbps LAN UTP must be rated at least a Category 3 cable, as defined by the EIA/TIA-568 and ISO/IEC 11801 standards. The 100 Mbps LAN UTP must be rated at least a Category 5 cable. Any other attachments, i.e., connectors, much also be similarly rated.

Fiber optic cable can be either single mode or multi-mode. Multi-mode fibers tend to have larger diameter cores and are used for short distance data transmission. Multi-mode fibers may also be made from plastic or glass strands. Single mode fibers have a smaller diameter core and are typically used for longer distance data transmission. Fiber is terminated using ST or SC connectors, though other connectors are suitable and can be used. Although fiber optic cable may be more expensive, its immunity to electrical interference may be a suitable cause for its use in a substation environment.
Practical applications may contain both types of media within the same LAN.

Mixing Media

Practical network design can use a variety of media. Several devices are available to join these media types in the configuration of a LAN.

Hubs or repeaters are simple devices that can interconnect different media types but only at a single speed, i.e., 10 Mbps or 100 Mbps. Hubs and repeaters operate at the OSI layer 1. Any data that is received at a port is simultaneously repeated to all other ports.

Switches and bridges are devices that can interconnect different media type and different speeds. Switches and Bridges operate at the OSI Data Link layer, which provides protocol independence. Data received on a port is only forwarded to those ports requiring that data through the use of routing tables. Switches tend to operate at near wire speed, which means they can process frames at the same speed that they arrive. Bridges tend to store and forward frames.

Routers operate at the OSI Network Layer and are protocol dependent devices. They are often used to forward data from one network to another based on network layer information.

Media converters are devices used to convert copper media to fiber. Often these devices are based on non-standard coding.

As more critical functionality is implemented through the Ethernet network, reliability of the communication infrastructure becomes more of a concern. Reliability of the Ethernet network has been enhanced in two ways. First of all, several manufacturers have developed “substation hardened” Ethernet switches and hubs. An Ethernet hub operates at the Physical layer of the ISO 7-layer communication model as a repeater. In this mode of operation, connected devices are subject to data delivery delays due to “collisions” of data packets.

Ethernet switches, however, operate at the Data Link layer (Layer 2). In this capacity, switches perform a “store and forward” function. In addition, switches allow the operation of Ethernet in a “full duplex” mode, that is, the Ethernet transceivers can both receive and transmit at the same time. As such, collisions are eliminated and data delivery times are consistent and repeatable. Note that on a shared hub, Ethernet can only operate in half-duplex mode, that is, only transmitting or receiving at any point in time.

Hardware Environmental Issues

Communications networking devices installed in electric power substations require careful application. Devices such as modems, auto dialers, hubs, switches and routers are subject to interference and electrical discharges that have been well documented.

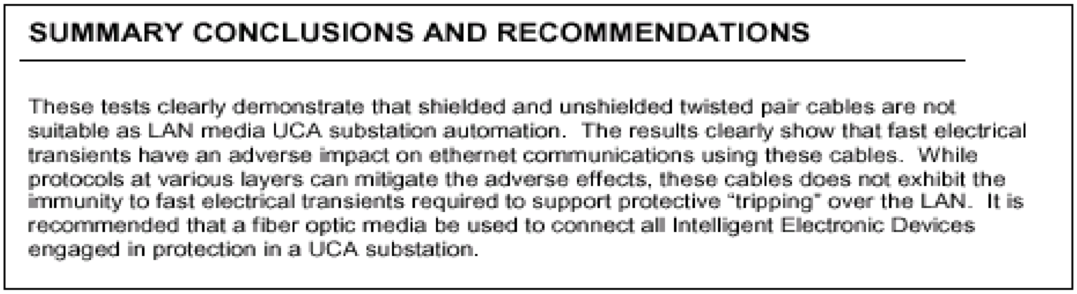
NEW ENVIRONMENTAL STANDARDS FOR ETHERNET IN THE SUBSTATION

In 2002 there were several new standards issued which address the environmental requirements of networking equipment deployed in substations:

- ***IEC 61850-3 Communications Networks and Systems in Substations*** was issued in January 2002 and addresses the climatic, EMI immunity and reliability requirements of networking devices such as Ethernet switches deployed in substations. The EMI Immunity requirements described in section 5.7 are of particular interest since they require the same type tests that are performed on protective relays to be performed on the networking equipment with the similar requirement that no damage or mis-operation occurs. This translates to no loss or delay of communications for critical communications functions being performed over the network.
- ***IEEE 1613-2003 Standard Environmental and Testing Requirements for Communications Networking Devices in Electric Power Substations*** that was developed by the IEEE PES Substations Committee also addresses the environmental and EMI immunity requirements of network ing equipment in substations. This standard was based on IEEE C37.90 (voltage and temperature ratings, dielectric tests), C37.90.1 (oscillatory and fast transient tests), C37.90.2 (RFI immunity), and C37.90.3 (electrostatic discharge tests) standards, which were developed for protective relaying devices. IEEE 1613 requires that the same type tests be performed on the networking equipment. There are two classes of networking equipment defined in the standard:
    - ***Class 1 –*** allows communications errors and delays during type tests
    - ***Class 2 –*** allows NO communications errors or delays during type tests

PERFORMANCE OF COPPER VS. FIBER IN NOISY ENVIRONMENTS

Tests were conducted back in 1997 by AEP under the auspices of EPRI to determine the performance characteristics of CAT-5 unshielded and shielded twisted pair cable in substation environments. The executive summary of a report titled “Electro-Magnetic Immunity Tests of Shielded Twisted Pair Copper Cable for 100 MBPS Ethernet” dated January 31 1997 concluded the following:



SUMMARY CONCLUSIONS AND RECOMMENDATIONS

These tests clearly demonstrate that shielded and unshielded twisted pair cables are not suitable as LAN media UCA substation automation. The results clearly show that fast electrical transients have an adverse impact on ethernet communications using these cables. While protocols at various layers can mitigate the adverse effects, these cables does not exhibit the immunity to fast electrical transients required to support protective “tripping” over the LAN. It is recommended that a fiber optic media be used to connect all Intelligent Electronic Devices engaged in protection in a UCA substation.

More recently in 2002, Rockwell Automation published a paper detailing the performance of Ethernet copper cabling systems in noisy industrial environments and concluded that in cables which ran adjacent to high current carrying conductors normally found in factory environments it was shown that BER (Bit Error Rates) of up to 22% could be encountered due to induced RFI resulting from adjacent noisy cables. This would effectively render the network useless.

In noisy environments where it is desired to have reliable communications then fiber optical media should be used to ensure immunity to the myriad of EMI sources found in both substation and industrial environments.

MANAGED SWITCHES AND ADVANCED LAYER 2 FEATURES

Managed Ethernet switches offer advantages over their unmanaged counterparts. Through the use of SNMP (Simple Network Management Protocol) they allow reporting of fault conditions such as loss of link, frame errors, and a variety of other statistical data about the network that can be used to monitor and detect problems early in their evolution. Furthermore, managed switches offer advanced Layer 2 features that are useful for real-time control and substation automation. These include:

- IEEE 802.1p Priority Queuing which allows frames to be tagged with different priority levels in order to ensure that real-time critical traffic always makes it through the network even during high periods of congestion.
- IEEE 802.1Q VLAN which allows for the segregation and grouping of IEDs into virtual LANs in order to isolate real-time IEDs from data collection or less critical IEDs.
- IEEE 802.1w Rapid Spanning Tree that allows for the creation of fault tolerant ring network architectures.
- Vendor-specific path-protection algorithms for ring network architectures can be faster than the generic Rapid Spanning Tree algorithm that has to handle Mesh networks as well.
- Filtering that allows for multicast data frames, such as GOOSE frames, to be filtered and assigned only to those IEDs which request to listen to them.

NETWORK ARCHITECTURES;

There are three basic network architectures (Cascading, Ring, and Star) that are commonly implemented with Ethernet Switches with numerous variations and hybrids of the three. Each of the three basic architectures offers various performance vs. cost trade-offs.

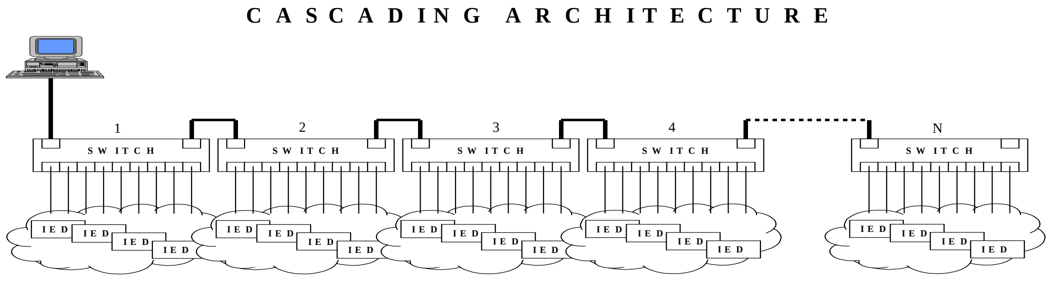


Fig 8.1 Cascading Network Architecture

Cascading (or Bus);

A typical cascading architecture is illustrated in Figure 8.1. Each switch is connected to the previous switch or next switch in the cascade via one of its ports. These ports are sometimes referred to as *uplink* ports and are often operating at a higher speed than the ports connected to the IEDs. The maximum number of switches, N, which can be cascaded depends on the worst case delay (latency) which can be tolerated by the system. For example, consider the case where an IED connected to *Switch 1* sends a frame to an IED on *Switch 4*. The frame must endure the retransmission delays of Switch 1, Switch 2, and Switch 3 of the cascade, or three 'hops'. Furthermore it will also be delayed by the internal processing time of each switch; a parameter commonly specified as the Switch Latency. Let's workout this example for a 64 Byte message frame assuming the following:

- Message Frame size = 64 Bytes
- Speed of Uplink ports (i.e., the ports forming the cascade) = 100Mbps
- Internal Switch Latency = 5us (typical for 100Mbps ports)

Therefore:

- The frame transmission time = 64 Bytes * 8Bits/Byte * 1/100Mbps = 5.12 us.
- The total delay from *Switch 1* to *Switch 4* = (Frame Transmission Time + Internal Switch Latency) * (# of 'Hops') = (5.12us + 5us) * 3 = 30.36us
- The total delay from *Switch 1* to *Switch N* = (5.12us + 5us) * N = N*10.12us

Advantages:

- Cost effective - allows for shorter wiring runs vs. bringing all connections to a central point.

Disadvantages:

- No Redundancy – if one of the cascade connections is lost every IED downstream of that connection is also lost.
- Latency – worst case delays across the cascading backbone have to be considered if the application is very time sensitive

Ring;

A typical ring architecture is shown in figure 8.2. It is very similar to the Cascading architecture except that the loop is closed from *Switch N* back to *Switch 1*. This provides some level of redundancy if any of the ring connections should fail. Normally, Ethernet Switches don't like "loops" since messages could circulate indefinitely in a loop and eventually eat up all of the available bandwidth. However, *'managed'* switches (i.e., those with a management processor inside) take into consideration the potential for loops and implement an algorithm such as the Spanning Tree Protocol that is defined in the IEEE 802.1d standard. Spanning Tree allows switches to detect loops and internally block messages from circulating in the loop. As a result, managed switches with Spanning Tree logically break the ring by blocking internally. This results in the equivalent of a cascading architecture with the advantage that if one the links should break the managed switches in the network will reconfigure themselves to span out via two paths.

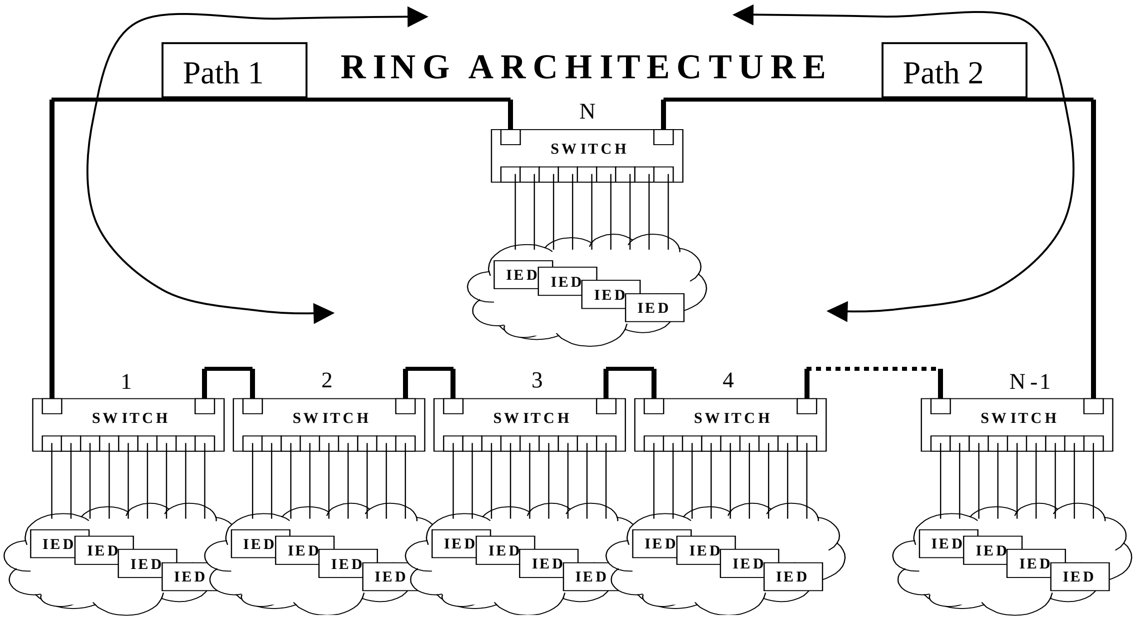


Fig 8.2 Ring Network Architecture

Consider the following example:

- Switches 1 to N are physically connected in a ring as shown in Figure 8.2 and all are managed switches supporting the IEEE 802.1d Spanning Tree protocol.
- Typically, network traffic will flow in accordance with Path 1 as shown in Figure 8.2. Switch N will block message frames as they come full circle thereby logically preventing a message loop.

- Now, assume a physical break in the Ring occurs, let’s say between Switch 3 and 4.
- The switches on the network will now reconfigure themselves via the Spanning Tree Protocol to utilize two paths, Path 1 and Path 2 as shown in Figure 8.2 thereby maintaining communications with all the switches. If the network had been a simple cascading architecture the physical break between switches 3 and 4 would have resulted in two isolated network segments.

While Spanning Tree Protocol (IEEE 802.1d) is useful for Ring architectures or in resolving inadvertent message loops it has one disadvantage when it comes to real-time control. Time! It simply takes too long anywhere from tens of seconds to minutes depending on the size of the network). In order to address this shortcoming, IEEE developed Rapid Spanning Tree Protocol (IEEE 802.1w) that allows for sub-second reconfiguration of the network.

Advantages:

- Rings offer redundancy in the form of immunity to physical breaks in the network.
- IEEE 802.1w Rapid Spanning Tree Protocol allows sub-second network reconfiguration.
- Cost effective cabling/wiring allowed. Similar to Cascaded architecture.

Disadvantages:

- Latency – worst case delays across the cascading backbone have to be considered if the application is very time sensitive (similar to Cascading)
- All switches should be Managed Switches. This is not necessarily a disadvantage per se but simply an added complexity. However, the advantages of Managed Switches often far outweigh the added complexity.

Star;

A typical Star architecture is shown in Figure 8.3. Switch N is referred to as the 'backbone' switch since all the other switches uplink to it in order to form a star configuration. This type of configuration offers the least amount of latency (delay) since it can be seen that communication between IEDs connected to any two switches, e.g. Switch 1 and N-1, only requires the message frames to make two 'hops' (i.e., from Switch 1 to Switch N and then from Switch N to Switch N-1.

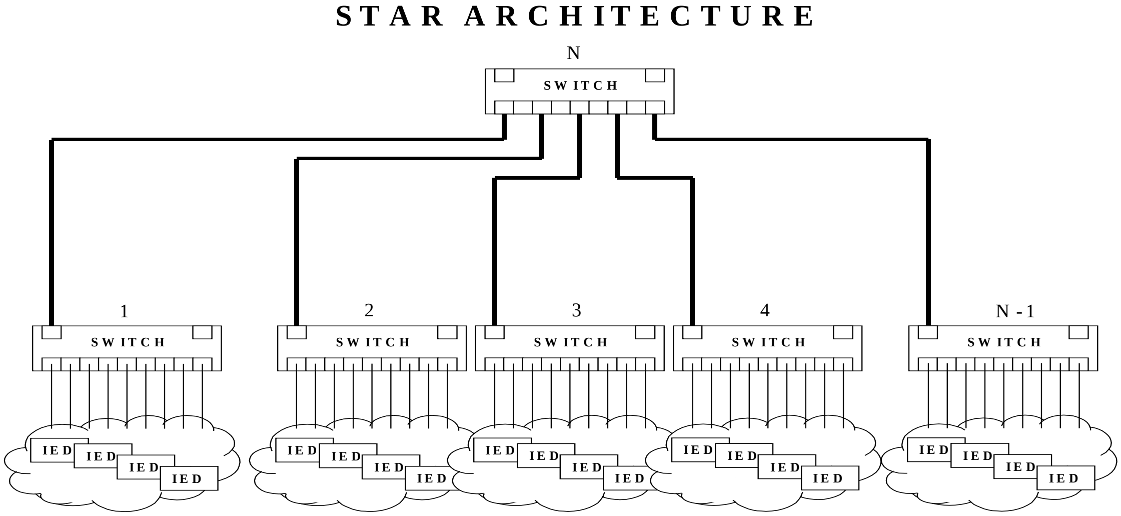


Fig 8.3 Star Network Architecture

Advantages:

- Lowest Latency - allows for lowest number of 'hops' between any two switches connected to the backbone switch N.

Disadvantages:

- No Redundancy – if the backbone switch fails all switches are isolated or if one of the uplink connections fails then all IEDs connected to that switch are lost.

Fault Tolerant Hybrid Star-Ring Architecture;

A hybrid fault tolerant architecture, combining star and ring architectures, is shown in Figure 8.4. This architecture can withstand any of the fault types shown in Figure 8.5 and not lose communications between any of the IEDs on the network.

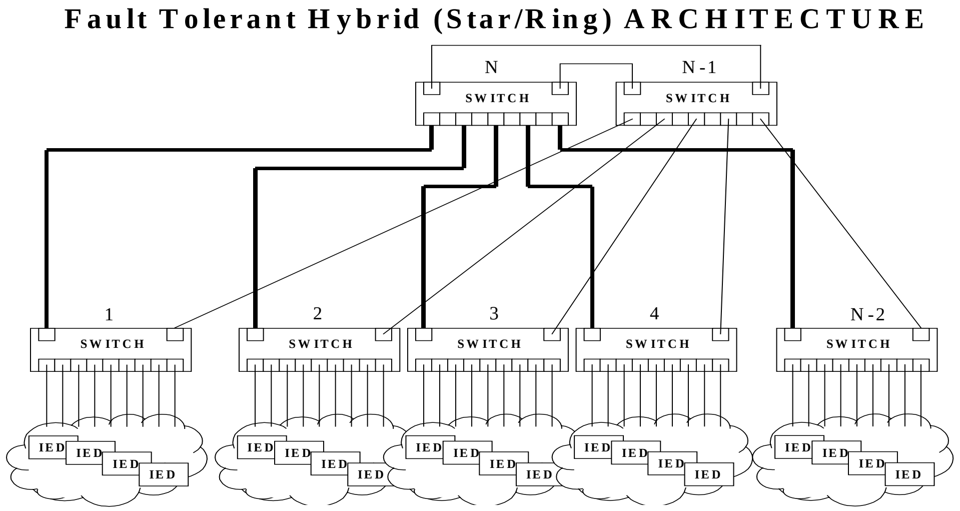


Fig 8.4 Fault Tolerant Hybrid Network

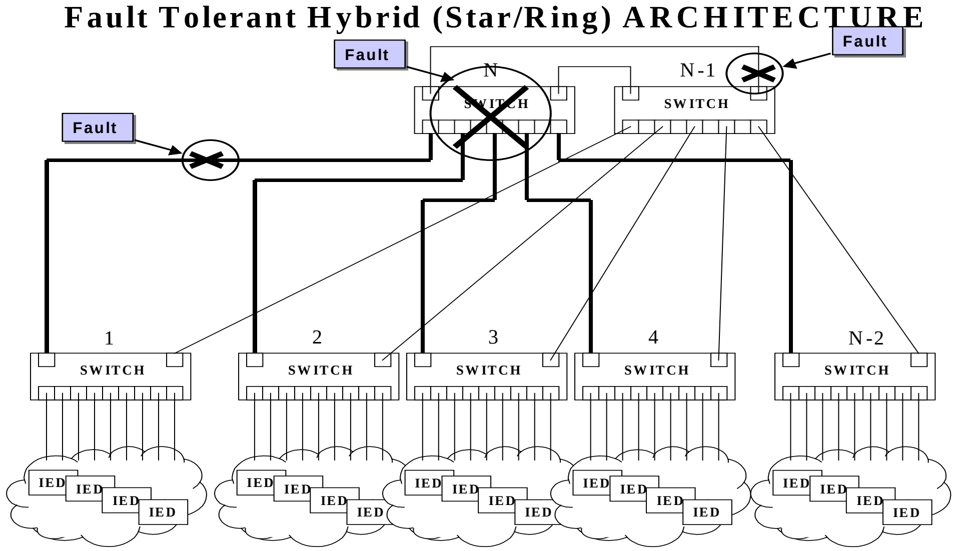


Fig 8.5 Fault Types Handled

Fault Tolerant Architecture For IEDs With Dual Ethernet Ports;

A fault tolerant architecture is shown in Figure 8.6 when IEDs with dual Ethernet ports are used. This architecture provides a high level of availability (uptime) and is immune to numerous types of faults as shown in Figure 8.7.

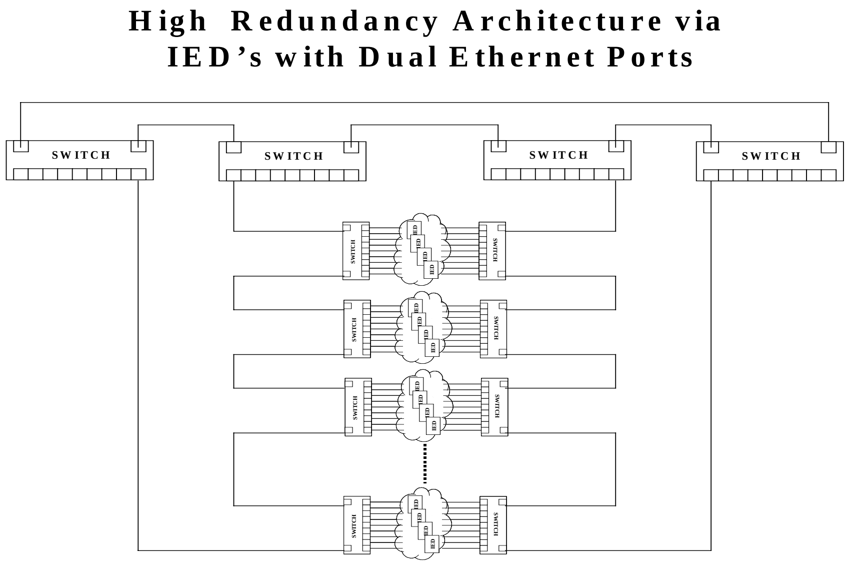

High Redundancy Architecture via
IED's with Dual Ethernet Ports
SWITCH
SWITCH
SWITCH
SWITCH
SWITCH
IED

Figure 8.6 *(edit headline to read "IEDs "*

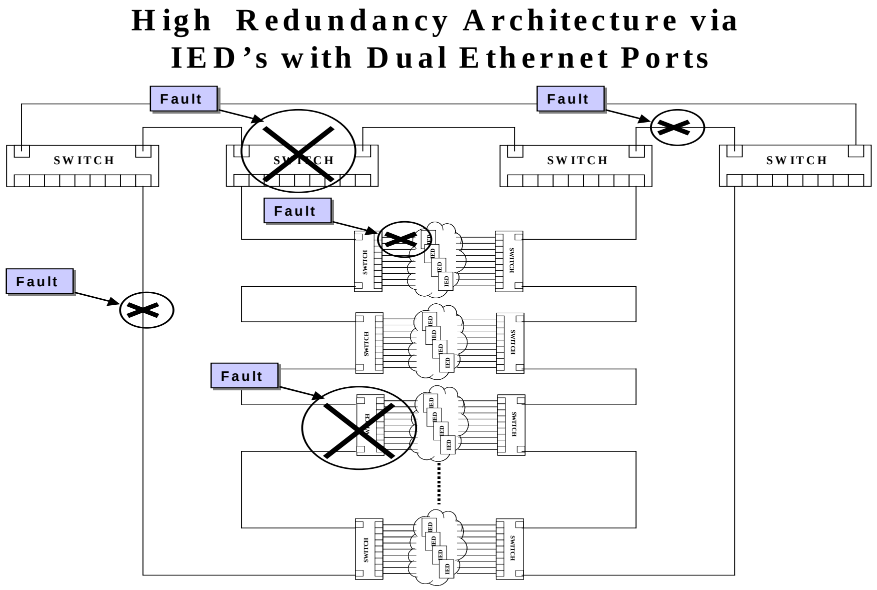

High Redundancy Architecture via
IED's with Dual Ethernet Ports
Fault
Fault
Fault
Fault
Fault
SWITCH
SWITCH
SWITCH
SWITCH
SWITCH
IED

Figure 8.7 *(edit headline to read "IEDs "*

Chapter 9; Conformance Testing

Conformance testing of a UCA based device will provide independent verification that the protocol specifications and modeling specifications have been implemented correctly according to the UCA 2.0 or IEC 61850 standards.

The objective of conformance testing is to give utilities and system integrators, in advance, maximum confidence that certified devices (from different vendors) will interoperate flawlessly. Hence, conformance testing is an important part of the quality assurance process.

What will be tested during a conformance test?

The conformance tests are designed to evaluate the device from the communications standpoint only and not address the functional characteristics of the device itself. The communication interface of the device will be tested under normal, error and stress situations. The error situations are especially important because these can cause interoperability risks that can't be tested during the factory or site acceptance tests. The conformance test can also check non-standardized issues and utility/project specific requirements like redundancy, performance and specific device configuration.
Subjects of the UCA 2.0 conformance tests are the implemented GOMSFE object models and the implemented CASM services to exchange data. Subjects of the IEC 61850 conformance test are the implemented object models (part 7-3 and 7-4), ACSI services (part 7-2 and 8-1), the substation configuration language files (part 6) and documentation (part 4).

Conformance test configuration

Figure 9.1 gives a schematic view of the test configuration to test a protection / control device.

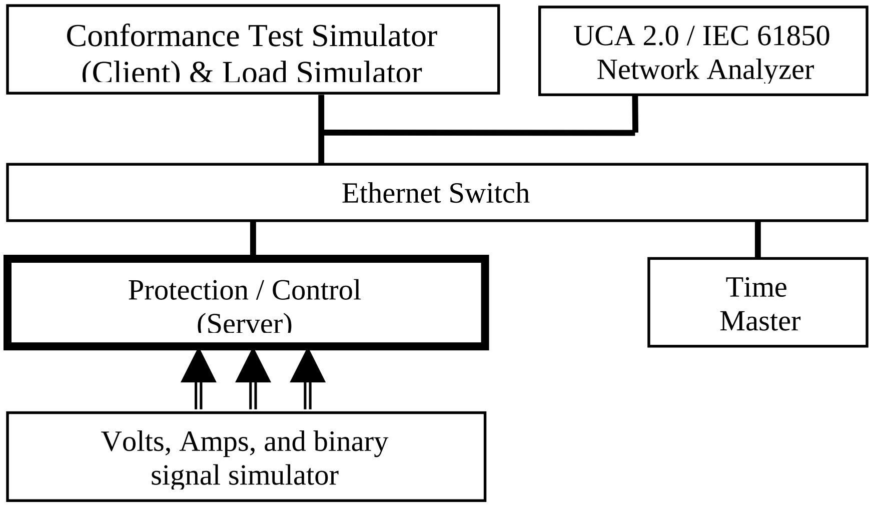

Conformance Test Simulator (Client) & Load Simulator
UCA 2.0 / IEC 61850 Network Analyzer
Ethernet Switch
Protection / Control (Server)
Time Master
Volts, Amps, and binary signal simulator

Figure 9.1

To reproduce all kinds of error and stress situations, test facilities need an optimized & automated protocol conformance test simulator. An accurate UCA 2.0 / IEC 61850 network analyzer is used to report incorrect behavior and measure response times. Also, the necessary analogue/binary inputs of the device under test need to be simulated.

Test approach

To start the conformance test the test facility needs:

- a sample device, configured for the test
- any ancillary software/hardware and engineering support during the test to control and configure the device when necessary
- a Protocol Implementation Conformance Statement (PICS);
- a Model Implementation Conformance Statement (MICS).
- a Protocol Implementation Extra Information for Testing statement (PIXIT) ;

Utilities with a UCA based substation automation strategy will/should have PICS, MICS and PIXIT statements to specify utility specific substation automation requirements. This process is shown in Figure 9.2. The PICS and MICS specify which parts of the standard are required. The PIXIT specifies additional requirements like reliability, redundancy, communication & device architecture and performance. When utility specific statements are not available, the test facility can use the device-specific statements provided by the vendor. The test facility uses these statements and the formal/standardized test procedures to tailor the test plan.

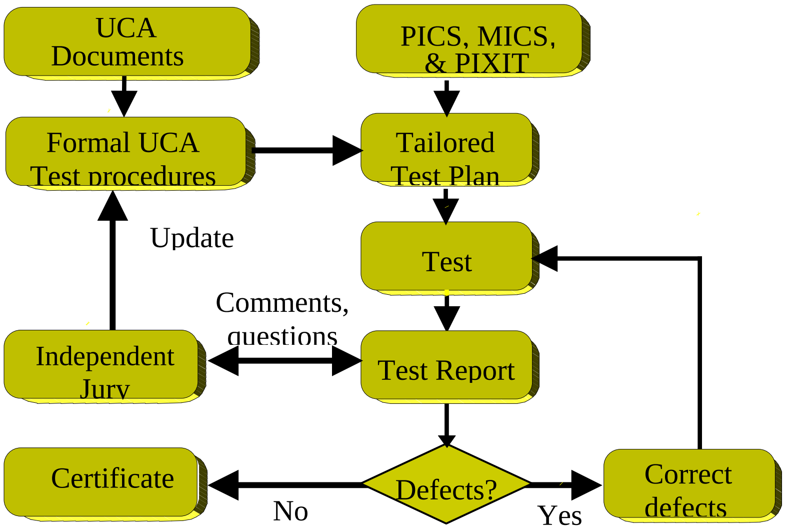


Fig 9.2

The test facility can perform the test in their test lab or at the vendor’s premises. The non-time critical part of the conformance test can be performed remotely via the world-wide-web. When defects are detected the vendor can correct it and the applicable test cases should be re-tested. The test results will be documented in the test report. When the result of a test is unexpected and ambiguously defined in the standard an “independent jury” can give recommendations. The jury consists of some members of the standardization body and some members of a user group. This jury collects comments from all test facilities and proposes updates of the formal test procedures. When no defects are found an independent third party test facility can reward a certificate.

Who can do conformance tests?

Of course the manufacturers will/should do conformance tests during the development of the devices. Some large utilities have their own test lab and qualified personnel that are capable of doing protocol conformance tests. Utilities without a protocol test lab can rely on specialized impartial third party test houses that can perform conformance tests according the utility specific PICS, MICS, and PIXIT statements.

Conformance Testing from a Utility perspective

To assure maximum benefits of a utility communication architecture utilities should have or define a substation automation strategy and define all utility specific communication requirements, the so-called PICS, MICS and PIXIT statements. To assure maximum quality we recommend utilities attach these statements to the request for quotation and require that each IED pass a conformance test performed by an unbiased third party test house before the factory acceptance test.

Conformance testing of UCA based devices will provide independent verification that the protocol specifications and modeling specifications have been implemented correctly by a vendor. The conformation tests should be designed to evaluate the device from the standpoint of communications only and should not address the operational characteristics of the device itself. Vendors will submit their device for testing and include:

- a sample device;
- installation and operating manuals;
- any ancillary software required;
- a Protocol Implementation Conformance Statement (PICS);
- a Protocol Implementation Extra Information for Testing Statement (PIXIT) ;
- a Model Implementation Conformance Statements (MICS).

Figure 9.3 below provides a conceptual view of the testing environment for various device configurations. Testing of a device designed to operate as a UCA Server would employ an Engineering Workstation (on the left) using commercial software packages from a variety of vendors configured to operate as a UCA Client. Testing of a device designed to operate as a UCA Client would employ an Engineering Workstation using commercial software packages from a variety of vendors configured to operate as a UCA Server. For devices designed to operate as both UCA Clients and UCA Servers, the Engineering Workstations (on both the left and the right) will be employed and configured in their appropriate modes to test the vendor’s device. In all cases, the device will be evaluated based on its behavior and presentation of data “on- the-wire”.

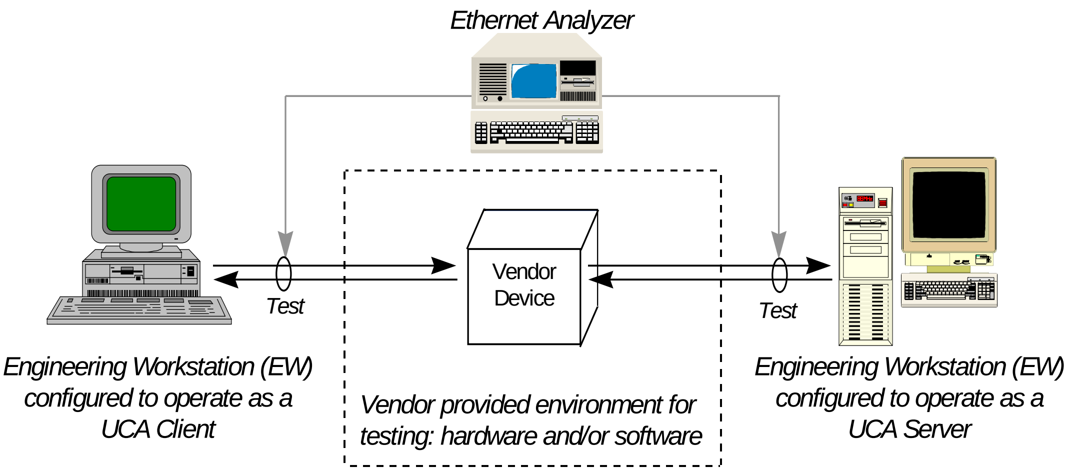

Ethernet Analyzer
Test
Vendor Device
Test
Engineering Workstation (EW) configured to operate as a UCA Client
Vendor provided environment for testing: hardware and/or software
Engineering Workstation (EW) configured to operate as a UCA Server

Figure 9.3. Conceptual test environment for the products designed to operate as a UCA client device.

A single set of conformance tests to be conducted for any and all devices would be an ideal approach to the testing of UCA based devices. However, the wide range of devices expected to be implemented based on the UCA specifications precludes such a simplistic approach. For example, the functions of a Load-Tap-Changer differ significantly from those of a Reclosing-Relay. To address this diversity, conformance test sets must be tailored to meet the specific functions and capabilities of each device based on the vendor’s implementation statements (the PICS, PIXIT and MICS).

All devices will be expected to support services to open, maintain and close associations with other UCA devices, whether as servers, clients, or client/servers. Therefore, conformance testing would be expected to include tests of the device’s association services such as:

- the establishment of any association
- the repetitive initiation and release of an association
- the initiation of an association with an abort response
- the repetitive initiation of an association with an abort response
- the initiate associate, abort and initiate recovery and release
- the initiate associate plus one more than supported associations
- get capabilities
- get identity

Beyond the basic association services, conformance testing should proceed to verify the services and objects specified in the PICS, PIXIT and MICS provided by the vendor. For example, consider a Load-Tap-Changer with a PICS that indicates that it supports services to manage lists of data, all of the mandatory data-objects and a number of optional data-objects. Conformance testing of such a device would include:

- get logical device list

- get data sets list
- get data object values (all mandatory data objects & all optional objects supported by the vendor)
    - for example, with a Load-Tap-Changer:
        - get LTCC/MX/CtlV
        - get LTCC/MX/SrcV
        - get LTCC/MX/LodA
        - get LTCC/MX/CircA
        - get LTCC/MX/TapPos
        - get LTCC/MX/ HiTapPos
        - get LTCC/MX/ LoTapPos
        - get LTCC/MX/ CntOper
        - get LTCC/MX/PriA
        - get LTCC/MX/PF
        - get LTCC/MX/PriVA
        - get LTCC/MX/PriW
        - get LTCC/MX/PriVAr

And for Set Point (SP) data-objects, conformance testing would include setting as well as getting of all data-objects.

- for example, with a Load-Tap-Changer:
    - get/set LTCC/SP/FPFBctr
    - get/set LTCC/SP/RPFBctr
    - get/set LTCC/SP/FPFBwid
    - get/set LTCC/SP/RPFBwid
    - get/set LTCC/SP/FPFTimDel
    - get/set LTCC/SP/RPFTimDel
    - get/set LTCC/SP/IntpDel
    - get/set LTCC/SP/FPFLDCR
    - get/set LTCC/SP/RPFLDCR
    - get/set LTCC/SP/FPFLDCX
    - get/set LTCC/SP/RPFLDCX
    - get/set LTCC/SP/FPFLDCZ
    - get/set LTCC/SP/RPFLDCZ
    - get/set LTCC/SP/VRedStep1H
    - get/set LTCC/SP/VRedStep2H
    - get/set LTCC/SP/VRedStep3H
    - get/set LTCC/SP/VRedStep1S
    - get/set LTCC/SP/VRedStep2S
    - get/set LTCC/SP/VRedStep3S
    - get/set LTCC/SP/VRedStep1A
    - get/set LTCC/SP/VRedStep2A

Additional conformance tests for:

- the event model services,
- the report model services, and
- the log model services

will be included or excluded based on the vendor’s PICS, PIXIT and MICS statements.

Chapter 10: Step by Step Application Overview

Application Overview

To develop a station automation application(s) there are certain basic procedures that should be followed to make the job easier. There is a need to gain a thorough understanding of the intended scheme operation before any development effort begins. A first step toward this goal is developing a detailed sketch, flowchart and/or write-up of how the scheme is to operate. Defining the overall scheme input and output requirements and the logic programming requirements are necessary. The application needs may dictate to some degree what IEDs are needed for the project. However, the IEDs used for automation will typically be part of what the utilities apply for their standard protection requirements. The IED automation programming is usually an extension of and included with the protection logic. Hardened station Personal Computers (PC), modern digital relays and LAN switches are typically the major components needed for both station protection and automation projects.

Digital relays, in addition to providing line protection, will typically provide or serve the UCA based line data, breaker status, system disturbance/fault recorder and alarm data needed in an automation project. Digital relays will also have the necessary input/output (I/O) including pushbuttons, high-speed communications and logic programming capability required for developing station automation application logic. All major protection vendors of modern digital relays support UCA and have programming logic capability. A UCA OPC server is needed to retrieve the above noted IED information for use in the applications on the Station PC. Lastly, the Man-Machine Interface (MMI) including the Graphical User Interface(GUI) package satisfy the requirements for programming, local database development, data display and station control. The above noted hardware and software are all the necessary pieces for beginning UCA based station automation projects.

Therefore, it should be identified in the beginning of the project which station IED devices and software applications are available and needed for the information, logic programming, the IED and LAN communications requirements, display requirements, etc. The preparation of a sketch of the overall scheme architecture, including communications and logic requirements, is a good way to start. Logic flow charts, etc., are also desirable before beginning programming. Typically, sufficient backup is usually provided so that the loss of any one IED will not disable the application.

The logic equations for the application can be developed in one or more of the following areas: 1) using the digital relay, 2) using the UCA OPC server, when programming is done on the station PC, or 3) using the PC MMI application programming. Some logic such as alarming levels, math functions and scaling can be easily developed in the PC MMI application. It can also be used to poll and request data from the IEDS.

A UCA OPC server can be used for retrieving files such as relay alarm logs and oscillography from IEDS for display on the station MMI or engineer's desktop PC. MMS commands such as read, copy, delete and file transfers are used for this procedure. Typical metering quantities such as voltage, current, power, etc., are obtained from the UCA MMS objects provided in the relay. Other objects obtained include breaker status, relay alarms, relay ID, communications status, etc.

Modern digital IEDS, including relays, offer the logic programming and I/O capability usually provided by the programmable logic controllers in the past. IED programming provides many of the digital and analog functions required for most complex logic programming needs. Because of familiarity with IED programming and due to other protection setting requirements, much of the application logic is typically developed in the IED.

Applications for station automation are varied and depend on need. Applications can be classified in many categories and can be developed to automate equipment testing, protection scheme logic, communications, database development, SCADA, oscillography, etc. The application can reside on one IED or on various IEDs and the station computer using UCA and GOOSE messaging to communicate between the IEDs on the station Ethernet LAN. These applications are readily applied and are typically used in conjunction with the station MMI and IED pushbuttons.

Typical and widely used control logic applications include those for capacitor bank controls, breaker reclosing, and breaker failure. Potential throw-over (i.e. reconnecting from one relay voltage source, if it is dead, to another live source) is another application that can be readily accomplished using the IED logic and pushbuttons. The logic for the operation of motor operated disconnects for various line opening and reclosing schemes has also been used considerably. An example of this would include the automatic isolation of a faulted section of line and the restoration of the un-faulted sections. The hardwired manual panel control switches that have typically been used with these schemes have all been incorporated in logic to take advantage of the station MMI and IED pushbutton capabilities. The IED pushbuttons are a useful backup to the MMI control functions and can help in the justification of not requiring hard-wired station switches.

Some specialized test applications developed in IED logic for protection equipment include those for carrier testing. Many routine carrier tests can be developed in logic and operated on the MMI or IED via pushbuttons such as check back(half and full level), loop back, level and status tests.

Communications applications have been developed to send IED alarms or commands on the Station LAN to other IEDS. Some applications include annunciation, turning on other

IEDS oscillography, etc. This peer-to-peer messaging is readily accomplished using UCA GOOSE messages configured in the IEDs.

After the automation application is developed it is necessary to test and verify the results. As an example, values displayed on the MMI should be checked with relay quantities to be sure that the correct quantity has been chosen, the scaling is correct, communications is connected, etc. This verification can be done using a 3-phase relay test set or actual line quantities. Scheme testing should be done in the lab during development and in the station prior to actual in-service.

Documentation of the logic and scheme is typically last but not of least importance. For the scheme to be tested and used by others it is important to develop a write-up of the intended operation. Depending on the detail and complexity of the scheme, an Application Guide may be essential. It has been found that for the scheme to be widely used and accepted in the field, detailed documentation is almost always required.

Summary of steps for automation projects:
1) Understand the scheme you want to automate
2) Determine IED hardware available for use
3) Review scheme I/O requirements
4) Develop an understanding of the IED protection and automation programming needed
5) Program the automation logic in the IEDs
6) Develop associated station MMI or IED pushbutton interface controls
7) Test logic and communications in the lab and at the station
8) Documentation/training of scheme logic and operation

Chapter 11; Examples of Applications

Example #1: AEP Orange Station using UCA communications and devices;

AEP UCA Orange Substation Communications Research Project Status/Objectives:

Extend Open Real-Time UCA into Substations

Tasks Completed

–Survey
–Requirements Specification
–Benchmark/Performance Analysis
–Demonstration Statement of Work
–GOMSFE Models
–Testing of Vendor Conformant Devices

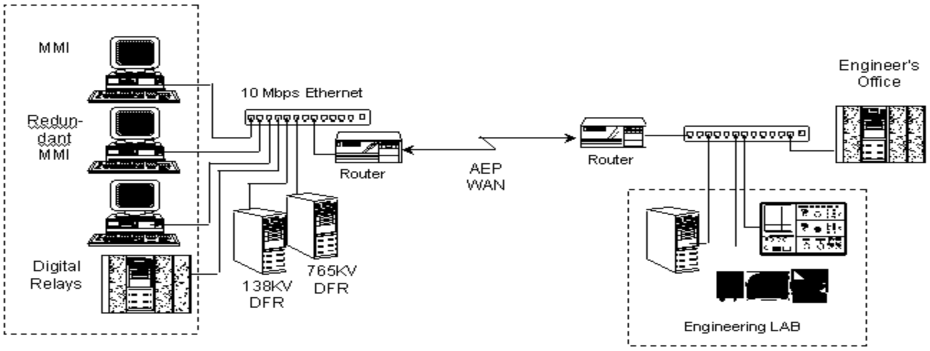
Ongoing Coordination Efforts: UCA Forum;
- IEEE; IEC -TC57/WG10,11,12

Documents: FTP. Sisconet/EPRI/Subdemo•Tasks Completed

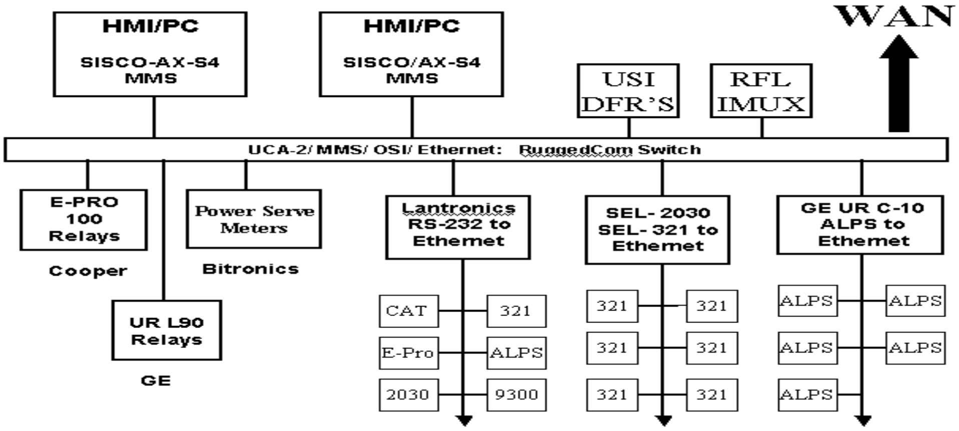
The AEP Approach to UCA at Orange;

A UCA approach was proposed and adopted to reduce the development of custom software and introduce a standards-based communications solution. The plan incorporates PCs, digital relays and communications equipment to support the exchange of MMS messages using commercial off-the-shelf software.

Conceptual Architecture;

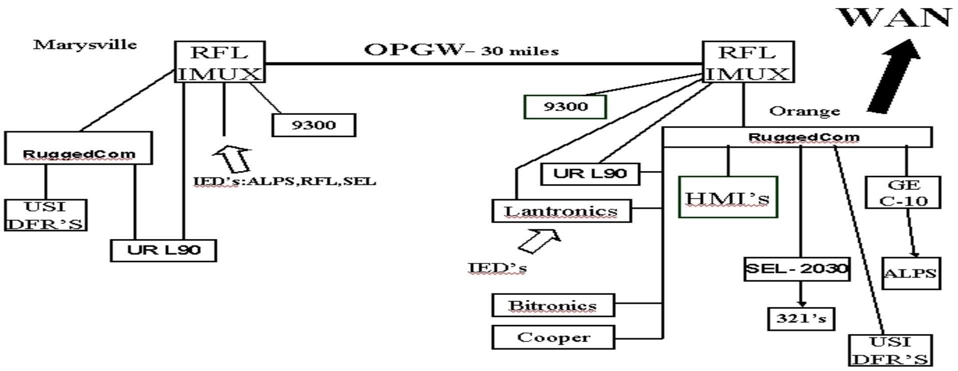


Actual Orange 765KV Station UCA LAN Architecture employed;



Orange- Marysville OPGW UCA LAN;

An existing optical ground wire was utilized and a fiber multiplexer was added to extend the Orange LAN to another 765KV station. This approach resulted in significant communications cost savings allowing high-speed access to additional IEDs.



Orange Station LAN Highlights;

•All controls through the station MMIs with no physical switches
•UCA MMS/Ethernet communication
•Fiber Optic connections to IEDs
•Completely Automated 765/138KV Station
•All IEDs have redundant communications
•Complete IED interoperability- plug and play
•AEP WAN/LAN connections via OPGW (Orange and Marysville 765 KV Stations)

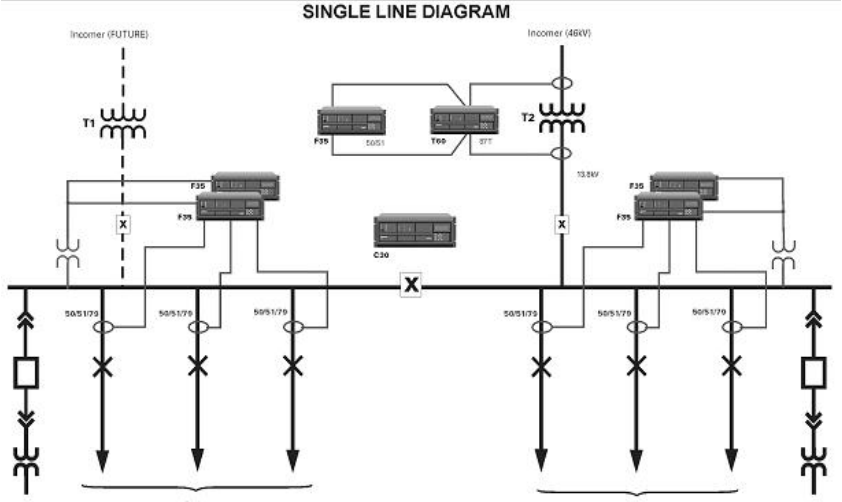
Station LAN Data;

•Marysville Station IED data also available using the 765 KV line optical overhead ground wire and RFL IMUX
•Engineer desktop PC access to all IED station data via the AEP WAN
•Data available: Station one lines, equipment and line loading, oscillography/DFR, PMU, CAT and IED settings, events/alarms, power quality, etc.

Example#2; GE Automation Projects using UR relays
Hydro Mississauga – Stillmeadow Automation project;

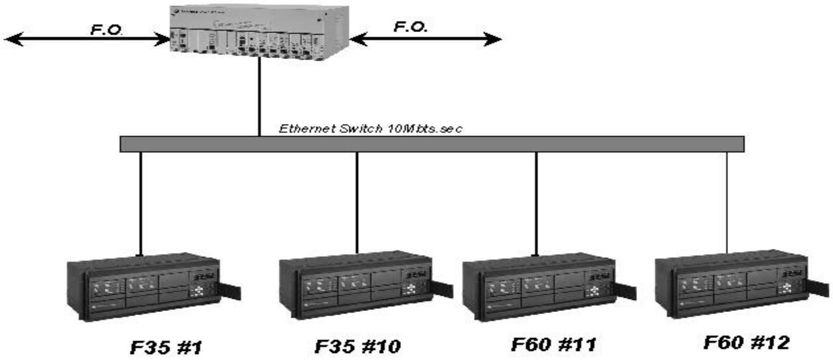
- Reviewed Protection, Monitoring and Communication needs with the customer
- Used Modularity + Flexibility to reduce IED Count
- Accommodated future expansion
- Understand remote monitoring needs
- LAN architecture application design
- Local and remote Monitoring function support

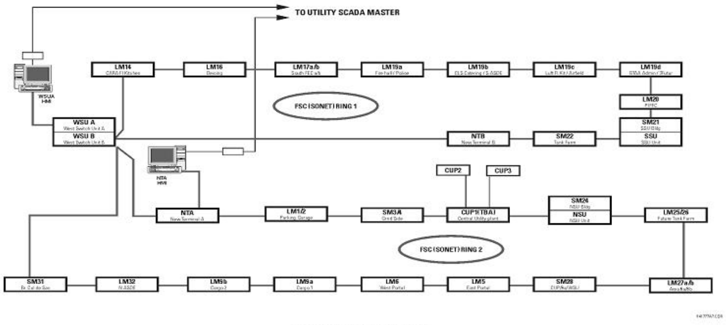
SINGLE LINE DIAGRAM



Greater Toronto International Airport Automation project;
New Airport – Total Electrical Power Distribution Supervision & Control.

- Integrated approach to Protection, control, monitoring using UR multifunctional IED
- 26 substations, 85 UR relays, 27 SDH/SONET Multiplexers, 2 HMIs
- Typical Tripping time based on comparative blocking scheme:
- Inherent time delay for blocking scheme: 40ms
- Relay plus communication network response time: 20ms
- Total Tripping time: 60ms
- LAN and WAN architecture reviews

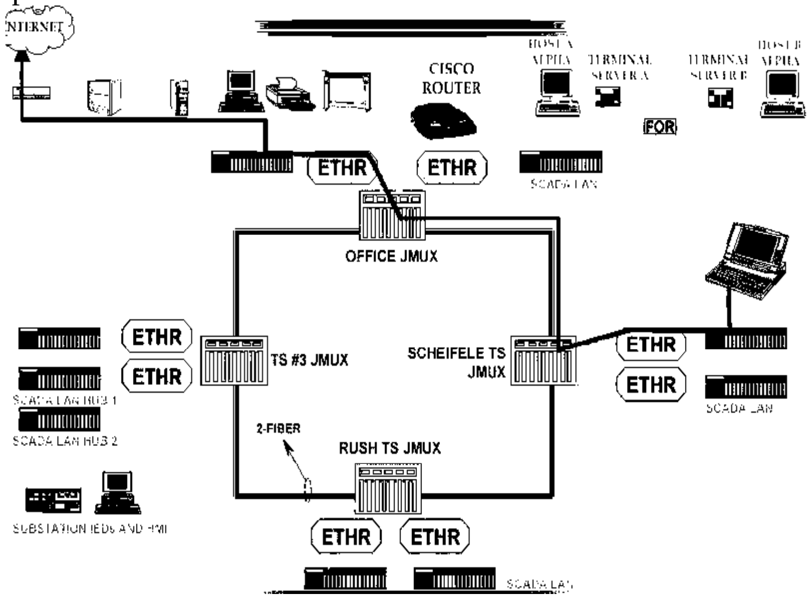




COMMUNICATIONS NETWORK

Waterloo Hydro Automation project;

- Peer to peer communication; less wiring
- Accessibility to each IED or HMI from ANY location
- Improved response time
- Easier access to backup facilities
- Disaster recovery; Web client access to HMI
- Capability of operating station over LAN/ WAN/ dial-in RAS
- Backup Control Room

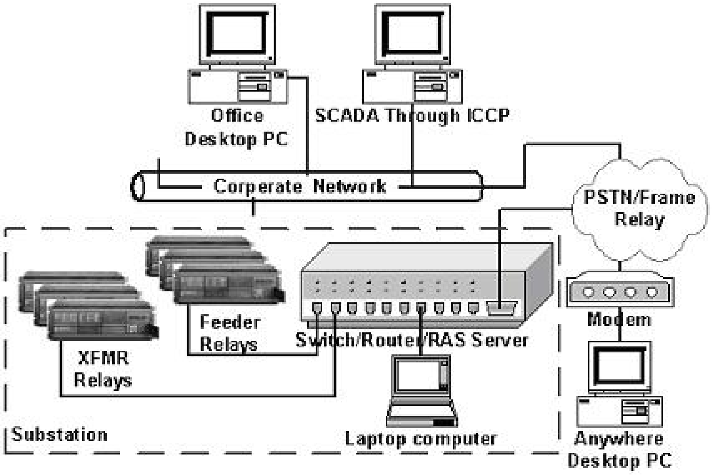


CINERGY Distribution Automation Project;
Background and Goals;

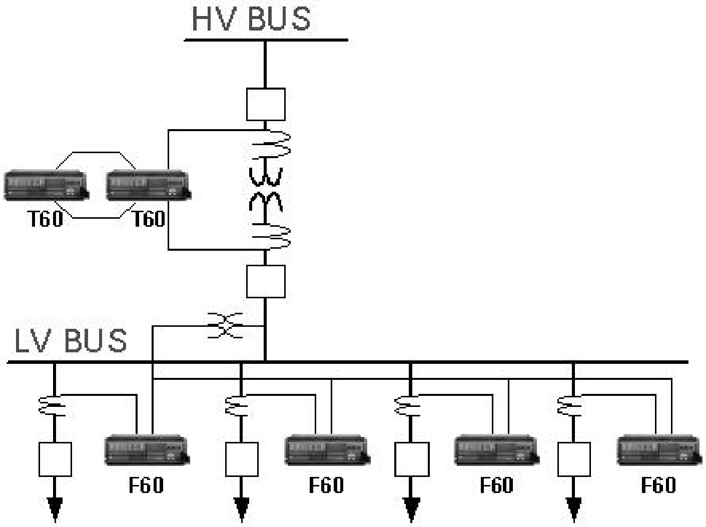
The choice to implement UCA2 crosses many departmental boundaries in an effort to reduce installation and maintenance costs. Departments would traditionally install redundant systems to access information specific to their department. These redundant systems introduce cost on an ongoing basis. Implementing UCA2 with smart protective devices makes information available at a departmental level without introducing redundant systems.

Another goal of this project was to reduce/eliminate interconnections between devices. This is accomplished by taking advantage of ‘virtual wiring’ via the GOOSE message and sharing information between devices over a substation network.

Conceptual Architecture;



Substation Layout;



- Reduce ongoing O&M costs
- Reduce installation time/cost
- Corporate-wide access to data
- No hardwired interconnections between devices
- Information shared between devices via ‘virtual wiring’ (i.e. GOOSE message)
    - From FDR to XFMR
        - Breaker failure
        - Lockout function
        - Virtual bus protection
    - From XFMR to FDR
        - XFMR trips
        - Lockout function
        - Virtual bus protection

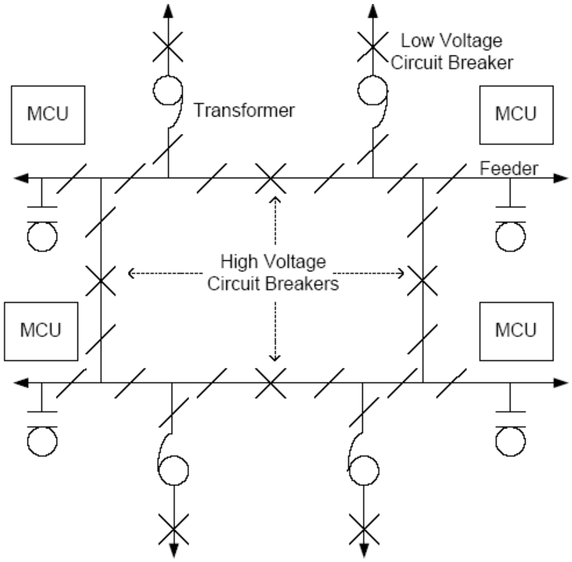
AREVA T&D EAI GOOSE Applications

AREVA is currently implementing UCA2 in several ranges of products – distribution and transmission protection relays, monitoring and recording IEDs, substation computers (PLC/RTU type devices) and substation automation systems.
GOOSE messages are starting to find their way as the preferred choice for interaction between multiple protection IEDS in distributed protection and control schemes. At this time the UCA2 protocol is being implemented for a delayed auto-reclose (DAR) scheme on the transmission system in the UK. The Mesh-corner (ring bus) plant topology requires coordinated control logic and DAR. Using the high-speed peer-to-peer communications GOOSE messages of UCA2 it is possible to satisfy the demanding time constraints for passing the control information between relays via the substation Ethernet LAN. The relay provides the full control logic and input-output (I/O) required for auto-isolation and DAR of a single corner of the mesh. Combining several of these devices and communicating over an Ethernet link, it is possible to control systems ranging from a single switch (circuit breaker) to a six-switch mesh corner scheme.

A mesh busbar arrangement is commonly used within the UK EHV transmission network. The aim of the arrangement is to reduce the number of high voltage circuit breakers required to protect several items of plant. A typical four circuit breaker mesh corner single line diagram is shown in the Figure below with the distribution of the Mesh Corner Units (MCU) indicated.

As shown in the diagram eight items of plant, four transformers and four lines can be protected using four EHV circuit breakers. In the case of a fault on any of the plant items, or busbar, all circuit breakers adjacent to the fault operate to isolate fault. Depending on the nature of the fault either a direct reclose of all circuit breakers will be made, or the faulted plant will be isolated from the system using the plant isolators prior to reclosure. The mesh corner auto-reclose system is required to perform the EHV breaker reclosure, auto-isolation of the plant and switching to suppress a ferroresonance condition occurring between the line and transformer.
To perform these operations and interfacing to all the plant status and controls requires significant digital I/O.

A decision was made to utilize the peer-peer communication defined in the UCA2 standard. The GOOSE services of this architecture allow digital status to be communicated between multiple IEDs.

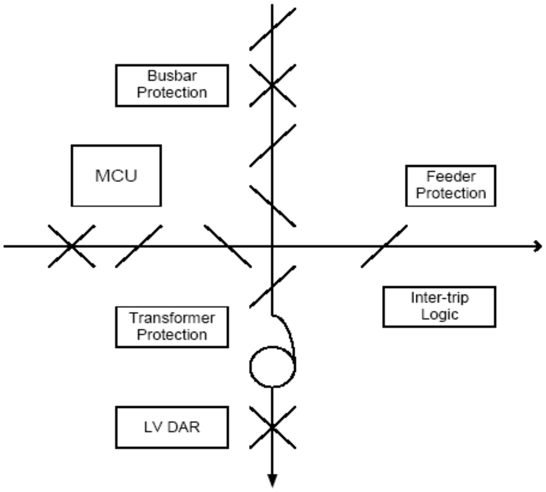


Mesh (Ring-Bus) Topology

The design of the mesh corner unit (MCU) is to provide the functional blocks to cover the switching requirements for a single corner. This includes the logic for the auto-isolation of up to three transformers, two lines and DAR for two circuit breakers. The relay also provides logic to permit ferroresonance suppression by flapping of the transformer disconnector and inter-trip reset logic. These modules are designed to be loosely coupled within the unit; connections between the modules are made using the Programmable Scheme Logic (PSL). This method provides the flexibility to couple modules within the same unit, via a hardwired connection or over the GOOSE communications. It is then possible to add additional MCUs to meet the switching requirements of different mesh corner topologies. This flexibility has been demonstrated by the application of the relay to an assortment of different mesh configurations up to a six-switch mesh corner.

The Mesh-corner plant topology requires coordinated control logic and DAR. Using the GOOSE element of UCA2 it is possible to satisfy the demanding time constraints for passing the control information between relays via Ethernet. The relay provides the full control logic and input-output (I/O) required for auto-isolation and DAR of a single corner of the mesh. Combining several of these devices, communicating over an Ethernet link, it is possible to control systems ranging from a single switch (circuit breaker) to a six-switch mesh corner scheme.

To allow the control logic functions inside the relay to link between the MCUs it is necessary to provide an interface to the GOOSE processing. As GOOSE is transmitted as a fixed size message it is necessary to map any information required by other devices into the message. Within the relay all logic signals to interface between the hardware and protection/control modules are stored on a Digital Data Bus (DDB). The relay provides the facility for any of the signals on the DDB to be mapped into the GOOSE message. As part of this mapping it is necessary to convert the single Boolean value to the bit pair that is used by the GOOSE messaging. If more complex mapping is required then it is possible to use the relay PSL to create the signal prior to mapping into the GOOSE message.



MCU Interfaces

To allow the GOOSE interfaces to be configured an additional PC based support tool was created. This is used in conjunction with the Programmable Logic Editor to define the system interconnectivity. These tools allow the output and input mappings to be created for each relay on the system. It also allows the communication failure states to be defined, i.e. what the receiving relay will assume if no valid message is received from an enrolled device.

Thus far the MCU scheme based on the GOOSE messaging has been installed at seven sites. Some sites have been a new installation of all protection and control equipment where the MCUS are separated between different cubicles. In other cases only the auto-reclose scheme has been replaced in which case all units have been installed in one cubicle.

To ensure reliable operation of the Ethernet communications a rail switch was used. In this configuration the rail switches are connected via 100MHz fiber optic cable in a ring connection. The use of fiber to make the connection between cubicles ensures immunity to EMC. The ring topology allows the scheme to continue to operate if one of the fibers is damaged. Within the cubicle all devices requiring communicating over the LAN are connected in a ‘star’ connection using an electrical link to the rail switch.

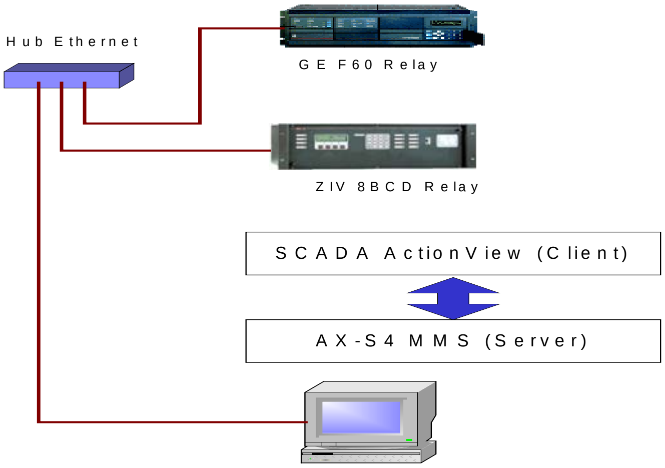
CTEEP and São Paulo University Research Project

CTEEP (Companhia de Transmissão de Energia Elétrica Paulista) is a Brazilian Utility that is sponsoring a research project performed by GAGTD (Grupo de Automação da Geração, Transmissão e Distribuição de Energia Eletrica - Automation of Electric Energy Generation, Transmission and Distribution Group) of São Paulo University, in order to evaluate the applicability of UCA architecture in its automation system.

CTEEP is a transmission utility that has 99 substations and a capacity of 36,424 MVA. The CTEEP's automation system is composed of devices of different manufacturers with different protocols. Thus, the present work intends to verify in a practical way the interoperability, integration and performance offered by UCA architecture.

To achieve the objectives of this project, it is being implemented as a test platform that include products of different manufacturers connected in a LAN. The products that constitute the test platform are:

- 8BCD relay (ZIV)
- F60 relay (GE)
- MMS Server (Sisco)
- ActionView SCADA program



Chapter 12: References

References

Substation Integrated Protection, Control and Data Acquisition Requirements Specification, EPRI Project RP-3599 Preliminary Report 1.1, November 7, 1997

ISO 9646-1: OSI Conformance Testing Methodology and Framework Part 1: General Concepts

ISO 9506-1: Industrial automation systems – Manufacturing Message Specification (MMS) – Part 1: Service Definition

ISO 9506-2: Industrial automation systems – Manufacturing Message Specification – Part 2: Protocol Specification

NIST Special Publication 500-206: Stable Implementation Agreements for Open Systems Interconnection Protocols Version 6 Edition 1, December 1992: Part 20 – MMS

IEC 61850, Communication Requirements for Substation Systems, Final Draft International Standard, 2003

IEEE Technical Report 1550, UCA™ Services, Models and Profiles, November, 1999 (Key portions of this document are being incorporated into IEC 61850)

IEEE C37.115-2003, Standard Test Method for Use in Evaluation of Message Communications between Intelligent Electronic Devices in an Integrated Substation Protection, Control, and Data Acquisition System – Report

IEEE 1613-2003, Standard Environmental Testing Requirements for Communications Networking Devices in Electronic Power Stations

Generic Object Models for Substation and Feeder Equipment (GOMSFE), Version 9.2, May, 2001 (Being incorporated into IEC 61850)

UCA™-2 Test Plan Scope Document, DRAFT Revision 0.7, May, 2001

Substation LAN Application Management, User Test and Monitoring Requirements for Substation LAN Systems, (Jim Whatley) HydroOne, (Mark Simon) ComEd, September 11, 1998

UCA™ Substation Product List, September 15, 2000

Initial Testing Capability Report, September 28, 2000 by KC Associates

UCA™ Demonstration at AEP Inez, October 1999, Presentation by John Burger

Laboratory Demonstration of UCA™ Substation Performance at HydroOne, September 2000, Presentation by Jim Whatley

IEEE Conference Paper **"LAN Congestion Scenario and Performance Analysis"**

by Mark Simon, Charles Sufana and John Tengdin

UCA™ Substation Workshop Proceeding, KC Associates, September, 2000

IEEE Std 100-2000 The Authoritative Dictionary of IEEE Standards Terms 7th Edition

Webopedia (an online dictionary for words, phrases and abbreviations that are related to computer and Internet technology): The URL is http://www.webopedia.com/

Chapter 13: Dictionary- GLOSSARY/ACRONYMS

access
Specific interaction between a subject and an object that is intended to result in the flow of information from one to the other.

Access Control
Means of restricting access to objects based on sensitivity (as represented by a label) of the information contained in the object and formal authorization of subjects to access information of such sensitivity.

accumulator
An integer value that counts the number of pulses or transitions of a binary input.

ACSI
Abstract Communications Service Interface

adaptive relaying
Protection system in which lower-level setpoints, relay logic, and relay action setpoints are adjusted based on data either locally acquired, or provided by the neighboring device on the same level locally or remotely, or sent down from a higher level.

addressing
Means to identify the source and sink (recipients) of all information transfers.

adjacent substation protection
Protection of power system equipment at one substation based on data measured at others. Examples are line differential protection and teleprotection schemes.

ADLC
Asynchronous Data Link Control

agent
Servers that are designed to work with compatible client stubs known as user agents which share the same server protocol. Agents are responsible for picking up and delivering messages between senders and receivers.

alarm processing Alarm analysis procedures to improve presentation of alarm data. It ranges from updating alarm lists and producing group alarms up to more intelligent evaluations.

Application layer OSI Layer 7 (the highest), this layer supports application and end-user processes.

attribute Represents a property or facility of an object (something that an object knows). It reflects both the problem domain and the system's responsibilities as some data (state information) for which each object in a class has its own value.

automatic reclosing Automated closing of breakers after the trip by a relay fulfilling some local and/or remote boundary conditions like synchrocheck reclose if applicable.

automatic switching sequences Automatic sequential operation of groups of power system devices to reduce operator workload and/or switching time and to avoid unsuccessful or unnecessary switching attempts.

availability of data State in which data are where the user needs them, when the user needs them, and how the user needs them. (see also multiple → transparent data access).

BFI Breaker Failure Initiate.

breaker Device that connects and disconnects energized power circuits, with fault interrupting capability under normal operational conditions (nominal values for current and voltage) and that is capable of interrupting short circuits (synonymous with circuit breaker).

breaker (health) monitoring Automated procedure to measure breaker operating times and accumulated interrupting duty for maintenance scheduling or maintenance on request.

breaker failure protection Backup protection scheme to trip all connected breakers if a breaker fails to trip on a detected fault.

broadcast Simultaneous transmission of data to all destinations on a network.

busbar fault isolation Minimizing propagation of bus and feeder faults. Subset of the general term → fault isolation (transformer fault, etc.).

busbar protection Scheme to detect busbar faults and trip all breakers attached to the faulted busbar.

busbar restoration Formal procedures for service restoration after busbar trips, very often according to fixed or load dependent priorities (see also → load shedding).

busbar voltage control

a) Automatics to maintain scheduled busbar voltage by any means (tap change, VAr control, etc.)

b) Network analysis to determine optimal settings of power system devices to maintain bus voltage.

calibrate function

Process of adjusting internal parameters of a measurement unit to reduce errors in its measured values.

capacitor bank

Group of capacitors used to adjust power circuit impedance.

CASM

Common Application Service Model

CCITT

Comité Consultatif International Téléphonique et Télégraphique, now part of the ITU (International Telecommunication Union)

CHAP

Challenge Handshake Authentication Protocol

circuit breaker

Device that connects and disconnects energized power circuits under normal operational conditions (nominal values for current and voltage) and is capable of interrupting short circuits (synonymous with breaker).

Client

An IED object that requests information from another (i.e., from the server).

Client/Server architecture

An application architecture where one end system (the client) requests another end system (the server) to perform operations and to give back results.

Client/Server concept

Communication management scheme in which multiple objects (i.e., the client(s)) can request specified information from one or more other objects (i.e., from the server(s)). Only Clients may issue unsolicited data. Usually data flows primarily from the server to the clients.

Client/Server operation

Complete transaction consisting of a request followed by an information delivery of requested information.

cold load pickup

Automated procedure to change feeder relay settings to pick up load after an extended outage (special case of adaptive relaying).

Cold-Load Pickup Control

Detection of the possibility of cold-load pickup (according to the cold-load pickup time delay) before closing the feeder Breaker refers to the need to either inhibit the instantaneous setting of the Overcurrent Protection, or to raise the Overcurrent settings for a certain period of time when the circuit is energized. By doing so, the protection settings can take into account transient current increases on circuit energization, and the normal fault settings can be adjusted closer to the load profile.

communication interface

Serial interface of a device that allows exchange of (physical and logical) information among devices of the same or different functional levels in a hierarchical system. An interface specifies the connection of a communication link, with regard to the mechanical connection as well as to the signal's physical and functional characteristics. A well known example of an interface is CCITT V.24/V.28 whose American counterpart is EIA RS-232C.

configuration data exchange

a) Power system topology exchanges with other, usually neighbor, utilities.

b) Exchange of any kind of configurations from power system topology to device setups (parameters, terminals).

Critical (synonymous with integrity)

Three levels of data (delivery) criticality are required:

High, where delivery is essential to operation of the power system (e.g., delivery of a SCADA control command). Examples are settings, commands switchgear states or positions, blocking, releases, trips, synchrocheck detection, and total energy.

Medium, where later repetition by application of a failed data transfer is acceptable (e.g., delivery of a stored data file) Examples are measured values (measurands) and disturbance recorder data.

Non-critical, where the recipient can tolerate occasional transfer failures (e.g., delivery of periodically updated data to a data monitoring or averaging process) Examples are repeated continuously polled data and display values.

CSOM

Client-Server Object Model.

CT

Current Transformer.

DAIS

Database Access Integration Services

data

Information with specific physical representation.

Data Acquisition Unit (DAU)

General purpose data collector, often used for sensors.

data confidentiality
Security service that provides for the protection of data from unauthorized disclosure.

data integrity
Security service used to determine if data has been altered or destroyed in transit.

Data Link layer
OSI Layer 2, At this layer, data packets are encoded and decoded into bits. It furnishes transmission protocol knowledge and management and handles errors in the physical layer, flow control and frame synchronization.

Data Object
A Data Object is an abstract element of a real device which is capable of providing (when read) or accepting (when written) or both, a typed data value. A Data Object may represent a single data element (i.e., one measurement point) or a data structure (i.e., a complex set of data elements). The mapping of a Data Object to a real, physical entity in the device is defined by the model of the device being represented, and is outside the scope of this document.

data transparency
Data transmission in which there are no restrictions on the bit patterns that user data may have.

DataSet
A DataSet is an ordered list of references to Data Objects associated with a specific DataSet Name. A DataSet is a means of grouping data together that is frequently accessed as a group.

DDE
Dynamic Data Exchange

deadband
The amount by which an analog input must change from the last reported value to be spontaneously reported.

Definite Time OvercurrentProtection
The Definite Time Overcurrent Protection corresponds to the definition of IEEE Device Number 62. If there is no intentional time delay, then the Overcurrent Protective Device corresponds to the definition of the IEEE Instantaneous Overcurrent Device Number 50 and 50N.

denial of service
Accidental or intentional actions by a communication network node that disable normal operation of any part of the network and can result in denial of (communication) service to other network users.

dependability
Measure of the certainty that a relay will operate correctly for all of the faults for which it has been designed to operate.

device
Physical entity connected to the communication network composed of at least one communication element (the network element) which may have a control element and/or a monitoring element (transducer, actuator, etc.).

DeviceIdentity

The DeviceIdentity, DI, contains the nameplate information of a device such as make, model, and serial number.

Digital Fault Recorder (DFR)

Device that samples and stores analog and related binary sensor data during power system transients for later replay and analysis.

Directional Overcurrent

Directional overcurrent relaying is necessary for the protection of multiple-source feeders, when it is essential to limit the tripping of faults in only one direction. Fault directional control is possible for faults on each phase, as well as the neutral. Directional current sensing and control requires a voltage, current, or a dual polarizing signal for selective detection of the direction or phase of the fault current. If directional overcurrent control is enabled, the overcurrent protection is inhibited for faults in the non-trip direction.

directory

Collection of open systems which cooperate to hold a logical data base of information about a set of objects in the real world (e.g., OSI users and network resources). The directory also provides services for users (people and application processes) to access the information contained in the repository.

DLCI

Data Link Connection Identifier

DNA

Dynamic Network Announcement

DSL

Digital Subscriber Line

EDC

Embedded Device Controller.

EIA

Electronic Industries Alliance

EPRI

Electric Power Research Institute.

Ethernet

Local area network architecture developed by Xerox Corp. with DEC and Intel cooperation.

equipment clock synchronization

Automated procedure to maintain consistent time data throughout the substation or power system, e.g., for time tagging or synchronized sampling.

equipment diagnostics

Procedures that monitor the on-line operation of power system devices, perform off-line tests, and provide early warning of potential failures (see also breaker health monitoring). The goal is optimized maintenance scheduling (maintenance on request).

expandability

The capability of a system to be increased in capacity or provided with additional functions.

extensibility

The ease with which a system or component can be modified to increase its storage or functional capacity.

Event Report

Event Report is the report generated in the Server by the action of a Transfer Set to be sent to the Client.

Fast ethernet

A newer version of Ethernet, called 100Base-T (or Fast Ethernet), supports data transfer rates of 100 Mbps.

Fault Identification and Location

This is logic that determines the type of fault, e.g., phase-to-phase, etc., the distance to the fault, and the impedance of the fault.

fault isolating

Minimizing the impact of a fault on a power network device (transformer, busbar, Switchgear, etc.).

fault recording

Procedures for collection, storage, and analysis of power system fault data.

feeder fault isolation

Automated procedure to operate feeder sectionalizing switches (isolators) to bypass a faulted feeder section.

feeder fault location estimation

Procedure to locate feeder faults to minimize service restoration time.

feeder monitoring

Display of feeder breaker and connectivity status.

feeder switching

Automated procedure to manage feeder connectivity changes (see also automatic switching sequences).

freeze

To copy the current value of an accumulator to another memory location.

functional block

An autonomous function, such as auto-reclosing, operational units, breaker failure protection, disturbance recording, etc., which might be implemented in separate hardware.

gateway

Processor providing communication protocol conversion services to permit communications between dissimilar data systems.

generator protection

Schemes to protect generators from fault conditions such as loss-of-field, motoring, and from all other potentially damaging conditions.

Global Positioning System (GPS) Receiver

Device that acquires precision time and position data from the U.S. Department of Defense system of a constellation of low-orbit satellites for position determination world-wide. For substations it is used as time receiver for equipment clock synchronization.

GMT

Greenwich Mean Time, now called UTC.

Hash function

An algorithm that allows messages to be sent in a secure manner.

High Impedance Fault (HiZ) Detection

HiZ detection reports possible high impedance arcing fault conditions on the feeder. A high impedance fault is characterized as having an impedance sufficiently high that it is not detected by conventional OvercurrentProtection. To date, this has been commercially applied to distribution feeder ProtectiveDevices, and is mostly used in the monitoring and alarm mode.

HMI

Human machine interface

IDS

Intrusion Detection System

IEC

International Electrotechnical Commission.

IEC TC 57

International Electrotechnical Commission Technical Committee 57.

IED

Intelligent Electronic Device

instance of (when instantiated)

Phrase used to denote that an abstraction (class-object) takes on a real-world form and behavior of a person, place or thing that it represents. An instance of is usually denoted by an attribute identifier that it inherits from the parent or is an attribute of the class-object instantiated.

integrity

Immunity requirements to the network of data transfer errors due to accidental or intentional interference. Three levels are defined (see also “critical”):

High, where a vanishingly small probability of undetected error must be achieved.

Medium, where inherent data redundancy provides adequate error immunity.

Low, where errors are merely a nuisance to the data recipient.

Intelligent Electronic Device (IED)

Programmable monitoring, control, protection, or data processing device with at least one serial communication interface.

interchangeability

Two IEDs are interchangeable when one can replace the other without changing external functionality or performances.

interoperability

Two IEDs are interoperable when able to exchange information needed for their on-line operation. This is normally achieved by using only published standard data and object definitions, standard commands and standard protocols at all relevant layers of the OSI Reference Model.

Inverse Time Overcurrent

This device determines whether a fault exists in its associated power apparatus by comparing a current (Ampere) measurement against a threshold (trip setting) value. However, the trip setting is determined (characterized) by a settings curve (time versus measured current). The curves are characterized by varying degrees of the inverse relationships of current to time duration. If the measured current exceeds the trip setting (“pickup” current) for the corresponding time on the settings curve, a fault is indicated.
The Inverse Time Overcurrent Protection corresponds to the definition of the IEEE Inverse Time Overcurrent Device Number 51 and 51N.

ISDN

Integrated Services Digital Network

ISO

International Organization for Standardization.

isolator

Device that connects and disconnects de-energized power circuits.

journaling

Means to maintain an audit trail of all control activities.

kb

Kilobytes.

LAN

Local area network

line fault location

Procedure to locate line faults to minimize service restoration time.

line load monitoring

Automated supervision procedure to support line operation close to limits.

line protection

Scheme to detect line faults and trip all breakers attached to the faulted line.

load flow control

Procedure to manage transmission or distribution line loading.

load tap changer (LTC)

A power switch integral to a LTC transformer or step-voltage regulator that accommodates adjustment of the voltage ratio while operating under load.

Load tap changer (LTC) control

Electronic device which receives scaled system voltage, current or other signals, compares existing operating conditions to that desired and accordingly commands load tap changer action.

Load tap changer controller relay

Device that manages the operation of a load tap changer on a transformer or step-voltage regulator. Synonymous with voltage regulating relay when used for control of the system voltage.

management information base

The set of managed objects in a system, together with their attributes, constitutes that system's management information base. It is a conceptual repository of management information at each system.

management information library

A document containing the specification of all defined managed objects and a complete description of their behavior. Development of this library is currently being proposed by groups such as the NIST OSI Implementers' Workshop Group.

MAS radio

Multiple-Address System radio is a fixed wireless, low capacity point to multipoint system that operates in the 900 MHz region with 3.2 MHz of allowed spectrum. Licensing form 601 is required and most MAS facilities operate under CFR 47, Part 101 of the FCC Code of Federal Regulations.

master

The remote client that requests information or a control operation from an RTU. Usually referred to in the singular, but there may be more than one.

Master/Slave

Communication management scheme called polling in which one IED (the Master) requests a specified one of a group of IEDs (Slaves) to deliver specified information. Only Masters, not Slaves, may issue unsolicited data or commands. Used where data flows primarily between the Slaves and the Master. Quiescent reporting schemes use an implied initial data request solicitation by the Master.

MB

Megabyte.

meter

Device that uses sensor data to calculate real and reactive power and energy.

method

Specific behavior that an object is responsible for exhibiting. The central issue in defining services is to define required behavior classified as follows: 1) on the basis of immediate causation, 2) on similarity or evolutionary history change over time, and 3) on the similarity of function. A service also defines the necessary communication between objects.

MMI

Man-machine interface.

MMS

Manufacturing Message Specification.

modem

Modulator/Demodulator; electronic device that enables digital data to be sent over analog transmission facilities.

ms, msec	millisecond.
multicast	Simultaneous transmission of data to a defined group of destinations on a network.
Negative Sequence Overcurrent Protection	Negative sequence instantaneous and time overcurrent is used to increase sensitivity in the detection of unbalanced load and fault conditions, e.g., in the unbalanced loading of a generator, or unsymmetrical types of faults on a feeder. The negative sequence settings can be set below load current levels since normal, balanced load currents do not generate negative sequence current. This relay monitors the negative sequence current of each phase. Negative Sequence Overcurrent Protection corresponds to the IEEE Device number 46.
Network layer	OSI Layer 3, this layer provides switching and routing technologies, creating logical paths, known as virtual circuits, for transmitting data from node to node.
NIM	Network Interface Module
non-repudiation	Method by which the sender of data is provided with proof of delivery and the recipient is assured of the sender's identity, so that neither can later deny having processed the data.
object	1) Noun defining a person, place, or thing that represents what a system needs to know and do about an actual object) Passive entity that contains or receives information.
OLE	Object Linking and Embedding
OSI	Open Systems Interconnection.
out-of-step protection	Automated detection of potential generator phase slip to avoid generator damage, to manage power network islanding, and to prevent undesired line relay action in the event of a stable power swing.
peer-to-peer	Ability of arbitrary pairs of network nodes to manage communication mutual information in contrast to the master/slave communication.
phase shifter control	Procedure to control the load tap changer of phase shifting transformers to manage phase angles and load flows.

Phasor Measurement Unit (PMU)	Device that extracts line-frequency phase angle and magnitude data from sensor signals.
Physical layer	OSI Layer 1, this layer conveys the bit stream - electrical impulse, light or radio signal -- through the network at the electrical and mechanical level.
pilot channel monitoring	Automated procedure that reports detected failures of protective relaying signaling channels.
PLC	Programmable Logic Controller.
point	Physical input/output hardware, or the data describing that hardware.
power flow control	Automated procedure to manage power transfers through power transmission and distribution networks.
power quality monitoring	Procedures for collection, storage, and analysis of power quality data at subtransmission and distribution load points.
Presentation layer	OSI Layer 6, this layer provides independence from differences in data representation (e.g., encryption) by translating from application to network format, and vice versa.
priority	Ability of the communication network to support several levels of message priority. Higher priority messages are given access to communication resources before lower priority messages.
protection facilities	Manual support of protection system operations.
PT	Potential Transformer; now known as VT.
PVC	Permanent Virtual Circuit
Quality of Service (QOS)	A parameter specifying the level of performance needed for communications, such as transit delay, priority, accuracy, or reliability.
RCB	Report Control Block.
RCL	Relay Control Logic.
reactor/capacitor protection	Scheme for detailed monitoring of reactive devices to detect internal faults and to trip all breakers connected to the faulted reactor/capacitor.

recloser

Special purpose breaker with integral relaying that automatically trips and recloses to minimize service restoration time after temporary faults.

recloser control

Automated procedure to manage the setpoints of reclosers to minimize service restoration time.

regulator

Abbreviated form for step-voltage regulator. Often incorrectly used when load tap changer controller relay is intended.

relay

Device that uses sensor data to protect major power system equipment items.

relay setting control

Procedure to manage the adjustment of setpoints in protective relaying equipment.

relay setting update

Procedures that report existing setpoints of protective relays and support the delivery of revised settings.

relay testing

Procedures that support testing of protective relay equipment.

reliability

Measure of the degree of certainty that a piece of equipment will perform as intended.

Remote Terminal Unit (RTU)

A device that concentrates sensor data for transfer to, and accepts power system device control commands from, an external SCADA system.

Report By Exception (RBE) Criteria

RBE Criteria are the values against which Data Objects in a DataSet will be checked to determine if an “event condition” has occurred. When an “event condition” occurs, then specified Data Objects in the DataSet are collected to be transmitted to the designated Client.

Report Control Block (RCB)

A data structure which describes the criteria for the Server to initiate Unsolicited Data transfers by time and/or event. The data transmitted will either be the complete Data Object or DataSet (no RBE), or it will be only the changed values within a Data Object or DataSet (if RBE is specified).

Report-By-Exception (RBE)

Mode of operation in which an end system (e.g., RTU or IED) only reports information that has changed since data was last transmitted.

response time

Time between the request and the response for a network transaction.

RLC

Reactive Line Component.

router

A device that forwards data packets between networks based on their network address.

RTU
Remote Terminal Unit

SBO
Select Before Operate.

SCADA
Supervisory Control and Data Acquisition.

scale
Multiplier used to convert a value from the measured value to the appropriate units.

Scan group
RTU/SCADA term for a data set

security
Immunity of network resources to accidental or intentional unauthorized access. Three levels are defined:

High, where access is limited to predefined and validated Clients.

Medium, where access is granted to any Client meeting simple criteria.

Low, where access (usually read-only) is granted to any Client.

Measure of the certainty that a relay will not operate incorrectly for any fault.

Select Before Operate (SBO)
Is a sequence of control services consisting of the Select service and the Control/Operate service. The Select service is used to arm an Select Before Operate (SBO device prior to operation. The Control service is used to carry out a control command after a Select has succeeded. This sequence has the effect that a client can lock-out other clients from operating a point for a pre-determined period of time so that it is the only client that can operate the point.

sensor
Sensing device for physical variables such as ac and dc Voltage and Current, Switch Status, Temperature, Humidity, etc.

Sequence of Events (SOE)
Sequence Of Events. An ordered, time-stamped log of the state changes of binary inputs (also known as status inputs). Used to recreate or analyze the behavior of a power system over a period of time.

Sequence of Events (SOE) Recorder
Device that samples and stores all events like contact status changes, trips, limit violations, etc., for later replay and analysis. The events are time-tagged at the source.

Sequence-of-Events Monitoring
Procedure to manage the collection, analysis, and presentation of SOE data.

server

Object that provides information to another (i.e., to the Client). Typical examples of servers are station computers and bay control/protection units. In substation applications servers have real-time requirements and are running with real-time operating systems.

Session layer

OSI Layer 5, this layer establishes, manages and terminates connections between applications.

SNMP

Simple Network Management Protocol

SONET

Synchronous Optical Network, a standard for connecting fiber-optic transmission systems.

SQL

Sequential Query Language.

SS radio

Spread spectrum radio

step-voltage regulator

Device used in the power circuit to regulate the system voltage, usually to within +/-10% of its input voltage level.

supervisory control

Arrangement for operator control and supervision of remotely located apparatus using multiplexing techniques over a relatively small number of interconnecting channels.

switch- electrical

Common denominator for circuit breakers and isolators (i.e., for the switching elements in the power network).

switch- ethernet

A device that passes ethernet packets to other capable devices connected in an Ethernet LAN.

synchro check

Automatic procedure to check if frequency, voltage and phase match when interconnecting energized portions of the power network.

synchronization

Automatic procedure to reach frequency, voltage and phase match when interconnecting energized portions of the power network by active means (excitation, etc.).

syntax

Grammar or structure rules which must be adhered to by a language (e.g., transfer syntax).

TAL

Time-Allowed-to-Live.

Tap changer

In general, may refer to a load tap changer or a deenergized tap changer. Will be used as an abbreviated form for load tap changer in the context of this document.

tap changer controller	Device that manages the operation of load tap changers or voltage regulators for control of voltage level (synonymous with voltage regulation relay in the context of this document).
TASE	Telecontrol Application Service Element
TCP/IP	Transmission Control Protocol/Internet Protocol
tie tripping	Procedures to separate and reconnect the two parts of a split bus to minimize fault propagation through the power network.
time-stamping	Message contains a field that tells the age of the information that it carries.
TOD	Time of Day
Token Ring	Type of computer network in which the computers are arranged schematically in a circle. To send a message, a computer must have the token.
transformer	Device that links power system circuits at different ac voltage levels.
transformer circulating reactive current control	Automated procedure to detect and reduce excessive circulating reactive currents as may result from the parallel operation of non-identical LTC transformers.
transformer protection	Scheme to detect transformer internal faults and to trip all breakers connected to a faulted transformer.
Transport layer	OSI Layer 4, this layer provides transparent transfer of data between end systems, or hosts, and is responsible for end-to-end error recovery and flow control.
UCA	Utility Communications Architecture.
UF	Under Frequency.
UMS	Utility Message Specification.
unit tripping	Automatic disconnection of a faulted generator unit.
unsolicited message	Message transmitted in response to a locally occurring event, rather than an explicit remote request.
UTC	Universal Coordinated Time, formerly known as GMT.
UTP	Unshielded twisted pair cable

VAr controller	Device that manages the operation of banks of capacitors and/or inductors for control of reactive power flow.
virtual device	Class of power system substation devices.
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
volt and VAr control	Procedures to manage bus voltages and VAr flows throughout the transmission or distribution network.
voltage regulating relay	Device that manages the operation of a load tap changer on a transformer or step-voltage regulator when applied for the purpose of controlling system voltage.
voltage regulator	Abbreviated form for step-voltage regulator. Often incorrectly used when load tap changer controller relay is intended.
VT	Voltage transformer.
WAN	Wide Area Network