

# Communication Standards in Power Control

Andrew C. West B.E., B.Sc., B.A., P.Eng, Grad. I.E., Aust, MIEEE  
Triangle MicroWorks Inc.

## 1. Summary

This paper was presented at the 1999 Electricity Supply Association of Australia Residential School in Electric Power Engineering, conducted at the University of Queensland in February, 1999.

It reviews the evolution of communication protocols used in Supervisory Control and Data Acquisition (SCADA) for power system control. It considers the features of the two communication protocol standards that are presently dominant in power system SCADA: IEC 60870-5-101 and DNP V3.00. Current development directions in power control communications standards are briefly considered.

## 2. Introduction

Electric power transmission utilities were among the first industrial entities to embrace data telemetry and telecontrol on a wide scale. Remote monitoring and control systems were first implemented in the early 1940's, and have progressively grown and evolved since then. Early SCADA systems provided very rudimentary monitoring, logging of digital changes (e.g.: circuit breaker tripping or closure) and periodic sampling of analog data. These systems predated the development of high-integration-density electronics, and were based on what, in hindsight, seem quite simple mechanisms for data acquisition and data communication.

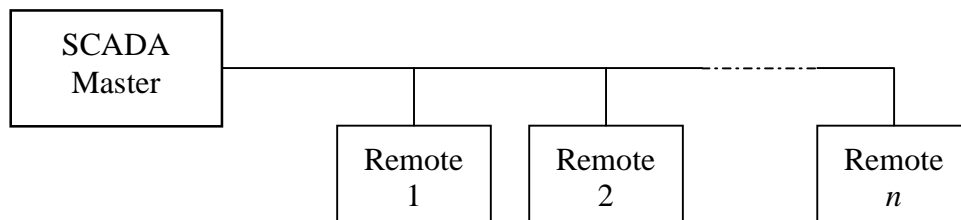
The diversity of equipment and manufacturers lead to a proliferation of proprietary protocols for data communication among power system control equipment. During this period control equipment was undergoing rapid change as new microelectronic technologies were applied to power system control for the first time. Suppliers endeavoured to establish a technical or commercial advantage through evolution of their products. Some companies established a considerable installed user base of their proprietary equipment. In the prevailing economic conditions of the time, it was believed that technical superiority; proprietary equipment and an installed customer base would lead to continued future sales.

Utilities and system integrators were confronted with a difficult challenge whenever equipment from different vendors was integrated into a single system. The different control protocols, parameters and operational philosophies often meant that it was difficult and sometimes impossible to make the disparate components operate sensibly in a single system. The expenditure of engineering resources to overcome these hurdles rarely resulted in systems with significantly superior capabilities, merely ones with unique combinations of equipment. Indeed, even when several utilities had similar combinations of equipment, their differing operational regimes and priorities sometimes prevented useful cost cutting through sharing of design or integration information.

In light of these difficulties, utilities and system integrators (many of whom were also system vendors) perceived the need for standardisation of interfaces between control equipment, so as to reduce the cost and complexity of control system integration and testing. Where appropriate, standards were incorporated from related industries such as computing and telecommunications.

### 3. Power System Control Requirements

Power system SCADA requires a high level of availability (control system outages must be infrequent and brief), a fairly high level of measurement accuracy (most analog measurements made within 0.25% of full-scale range), and high security (validation of received data and prevention of inadvertent or incorrect control operation). Most power system SCADA requires an efficient means of gathering small quantities of data from a large number of remote sites. Most SCADA systems are based on a multi-drop communications topology, as shown in Figure 1.



**Figure 1—Typical multi-drop communication topology**

All modern SCADA systems convert sampled analogue field quantities to digital values and use digital data transmission. Data collected from a typical substation will consist of a number of digital indications (e.g.: status of circuit breaker position, alarm signals, mode indications) and analogue quantities (e.g.: feeder current, bus voltage, transformer tap position). The quantity of data may vary from a few bits to many hundreds of bits. Most SCADA systems for power transmission will contain many substations requiring approximately 100 bytes per site to transmit a complete snapshot of their current status. Most SCADA systems used in distribution networks will collect data from a much larger number of smaller devices (e.g.: pole-top reclosers). These might only report ten bytes of data or less. In both cases, the amount of data to be transmitted is significantly less than the thousands to millions of bytes that are typically transferred between computers on typical corporate data networks.

Power system SCADA security and reliability requirements have often forced utilities to provide and maintain their own communications infrastructure. Some utilities require permanent connection, and the projected lifetime cost of hiring the telecomms carrier's leased lines from the control centre to each remote site offsets the cost of establishing and maintaining such a network. Few telecom carriers are able to guarantee the availability that some utilities require. For other utilities (especially distribution utilities), data radios are chosen as the appropriate solution to meet the system's requirements. For some extremely remote sites, satellite communications can become economically viable. Each system's physical, operation and economic requirements need careful evaluation to determine the appropriate communications network type to adopt.

Digital data communication is evolving rapidly, and a succession of standards have emerged for digital data transfer, and the physical interfaces to the systems that

provide these services. SCADA systems have typically taken advantage of these standards and conformed to them.

One particular historic deviation does, however, deserve mention: The V.23 standard specifies frequency shift keying (FSK) modulation of tones on a voice-grade (300Hz–3kHz) channel, providing full-duplex transmission at 1200 bit per second (bps) in one direction and 75 bps in the other. It was designed for use with user display terminals where information download could occur quickly while the user typed commands.

V.23 has been used for many SCADA systems because it provides a high data rate, and (unlike many more-recent data modulation standards) it is relative immune from phase and amplitude distortion due to line characteristics. Hence it does not require a lengthy “line training” arbitration to be performed when devices first establish communication. This allows short message establishment times: typical receiving devices detect and synchronize to the data carrier in less than 20ms. This permits multiple devices to be connected to a single communication system and allow rapid polling of data from successive devices. The significant deviation from the V.23 standard that is employed by most SCADA systems is to use the high data rate (1200 bps) in both the send and receive directions. This requires half-duplex operation on a 2-wire system or a 4-wire system for full duplex operation. As many early systems were “poll-respond” systems, half-duplex operation was satisfactory.

Many recent modem standards allow quite high data rates (many times greater than the 1200 bps allowed by V.23). These systems are typically intended for point-to-point use (i.e.: between two devices, not on a multi-drop link), and require a period of “line training” at connection to determine the characteristics of the line. This training period may be several seconds, added to the beginning of any message establishment. This is not suitable for the multi-drop topology, as this line-training interval would be applied to the beginning of transmission to each remote. The duration of a typical transaction of a few to a few hundred bytes is significantly less than the line training time to establish the connection.

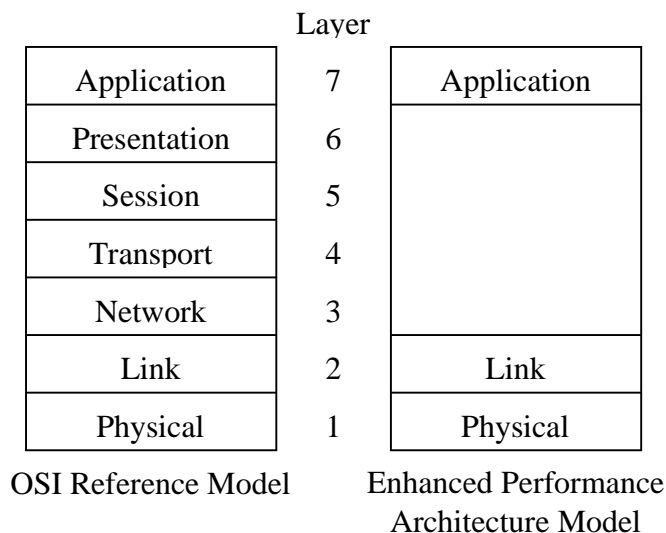
Computer-to-computer data communication standards have been developed over the past few decades. One of the well-known models for this is the seven-layer OSI reference model (see Figure 2). This provides for the encapsulation of the relevant data (the “application data”) within packets that provide the services necessary to transport the application data to its final destination. The lower layers manage establishing the connection, data validation and retry, physical interfacing, etc.

The seven-layer model provides for good isolation of the application program from the underlying system and communications media, but adds a significant overhead in processing power and bandwidth utilisation. Thus, it is generally not a good match for typical SCADA systems. In recognition of this, a working group was established by the International Electrotechnical Commission’s Technical Committee 57 (IEC TC57) to consider the development of an international standard for power system communications for SCADA and related purposes. This working group, WG03, has produced the IEC 60870 series of standards that describe a framework and methodology for designing protocols, and a “worked example” SCADA protocol: IEC 60870-5-101. Other IEC working groups have used IEC 60870 as the basis of

communication protocols for metering (IEC 60870-5-102) and protection functions (IEC 60870-5-103).

Note: The IEC is harmonizing its standard numbering system with the ISO (International Standards Organisation), so that all standards will be assigned a unique five-digit number. Any IEC standard that has a number less than 10000 will have 60000 added to its number on next release. Hence IEC 870 has become IEC 60870.

The IEC 60870 series of standards have been developed and released over a period from the mid-1980's until the present. The first four parts consider general principles, environmental conditions and performance requirements. Part 5 describes the components of communications protocols. It defines a reduced three-layer model, the "Enhanced Performance Architecture" model (EPA), that is intended to reduce the overhead of the seven-layer model in a manner appropriate for SCADA purposes. Figure 2 shows these three layers and their correspondence to approximately equivalent layers of the OSI reference model.



**Figure 2—Reference Models**

In establishing the EPA, the IEC moved a component of the application functionality into the link layer. This provides the ability to enhance system performance by sending a link-layer-only message as a proxy for an application-layer message. In this regard the EPA is not as "pure" as the OSI model.

#### 4. Application Layers

The description of the data link framing formats (IEC 60870-5-1) was published in 1990, and the procedures (commands and formats) for link transmission (IEC 60870-5-2) were published in 1992. Many SCADA system suppliers quickly adopted these into their existing products, leading to the emergence of a new wave of protocols that offered essentially interoperable data link framing, but having proprietary application layers. This permitted these suppliers to truthfully state compliance to the standards. However, most of these protocols remained proprietary, and did not gain wide market acceptance. One notable exception was the Distributed Network Protocol version 3.00 (DNP V3.00) produced by Westronic (now GE-Harris) and placed in the

public domain. By taking this unusual step at a time when the IEC standard for the application layer was still far in the future, DNP became an accepted de-facto standard by many equipment vendors in North America. It was not until the release of IEC 60870-5-101 in November 1995 that there was an official international standard application layer for electric power SCADA. DNP is maintained by a consortium of DNP users and vendors, known as the DNP User Group. The DNP User Group has a technical committee that is responsible for further development of the protocol.

During the 1990's a consortium of North American utilities worked on a research project considering the future of substation communications and control. This work has been coordinated by the Electric Power Research Institute (EPRI), and is nearing completion. The outcome is the Utilities Communication Architecture: UCA2 (UCA was an interim trial). UCA2 is not simply a communications protocol, but an architecture for coordinating the operation and interaction of devices within and between substations. Communication between the devices uses the Manufacturing Messaging Specification (MMS), but any other protocol could be used to transport UCA2 information. The significant work of UCA2 is to identify how equipment should interoperate, and how devices publish and subscribe to each other's information. This development is outside the scope of this paper, but warrants attention as it may prove to be the direction of future electric power control system development, especially for electricity distribution systems.

The IEEE's Power Engineering Society has taken an interest in the developments of SCADA protocols and substation automation systems. The IEEE has published a trial use recommended practice for substation data communication (IEEE P1379) that recommends both DNP and IEC 60870-5 protocols as suitable for use.

The IEC and the DNP User Group Technical Committee (DNP UG TC) are considering the means to transport SCADA data over local and wide area networks (LANs and WANs). The IEC has issued a draft international standard specifying the transport of IEC 60870-5-101 data (with extensions) over TCP/IP. If accepted this will become IEC 60870-5-104. The DNP UG TC is expected to publish a technical bulletin specifying the use of TCP/IP for transporting DNP over WANs, and UDP/IP for transporting DNP over LANs.

## **5. Comparison of DNP and IEC 60870-5-101**

This section lists the similarities and differences between the DNP V3.00 and IEC 60870-5-101 protocols.

### **5.1 General**

The protocols have many similarities in their functionality. Each permits:

- Collection of binary (digital) data
- Collection of analogue data
- Collection, freezing and clearing of counters
- Single pass or two-pass control of binary (digital) outputs
- Single pass or two-pass control of analog outputs
- Reporting of binary and analog events (report by exception)
- Time synchronization

- Time-stamping events
- Grouping data objects
- File Transfer

Both protocols permit polling for all data (this is normally done at startup to collect the initial state of the slave), and subsets of data. Both normally operate by only collecting events (changes) from the field.

## 5.2 Differences

- DNP is based on a paradigm of securely transporting generic SCADA data in a manner that uses bandwidth as efficiently as possible while generally conforming to the rules and procedures established by the IEC. The IEC data model creates compound objects (e.g.: tap position indicator), that may consist of several binary or analogue values.
- DNP does not conform exactly to the frame format specified by the IEC: The DNP frame adds start and stop bits to each octet of the FT3 frame format (using a 16-bit CRC) to allow the use of standard asynchronous data communications equipment. The IEC chose to use the less-secure FT1.2 (which already includes start and stop bits) for 101 so that they would not need to specify a new frame format.
- DNP only uses balanced link services. 101 may use balanced or unbalanced services.
- DNP supports only a single addressing format. 101 allows most of the options specified in 60870-5-2. The DNP addressing format supports peer-to-peer operation, the 101 format does not.
- DNP introduces a pseudo-transport layer (OSI layer 4) to build application data messages larger than a single data link frame. Each 101 message must be contained in a single data link frame.
- DNP permits more than one object type to appear in a message. 101 only permits a single object type in a message.
- DNP requires an application layer message to contain a poll request (or any other command). Polling in 101 can be triggered by a link-layer message containing no application data.
- 101 includes a concept of “Cause of transmission” that is not included in DNP. This permits a 101 device to cause data to become available (pseudo-events) for a larger number of reasons than available to a DNP device.
- DNP groups data into four classes. This may be used to prioritize event reporting. One class is for “static” data: current values of inputs; the other three are for “event” data: reporting changes. All four classes may be requested simultaneously. IEC groups data into two classes, and while not explicitly stated in the 101 standard, one class is intended for “cyclic” data, and the other class is for all other data. Only one class or the other may be requested in a single poll. The device indicates in the link layer which class should be polled for next.
- DNP supports unsolicited reporting using a collision-avoidance mechanism for multi-drop systems. 101 only permits unsolicited reporting on point-to-point links where collision is impossible.

- DNP relies on the data link address to identify the source of the application data. 101 uses the data link address to identify where the frame should be delivered, and includes the data addresses within the application data.
- Because DNP allows more than one data type in a message, it includes more complex data type and identity information in the application data than 101. Hence parsing a DNP message is more complex than parsing a 101 message.
- DNP defines a number of implementation subsets that simplify determining if equipment will interoperate. Each DNP device vendor indicates which DNP objects and functions are supported in a standard-format "Device profile". The intent of this is to maximize the likelihood that devices from different vendors will work together with minimal configuration. 101 includes an interoperability chapter defining how a vendor indicates which objects and options are implemented. There are no defined subsets. This requires careful analysis to ensure that devices will work together or can be configured to work together.
- DNP is maintained by the technical committee of the DNP User Group. This body provides information about the protocol, and clarifies ambiguous areas of the protocol definition. The IEC does not provide information to clarify the interpretation of its standards. Questions are best addressed to a vendor of a product that supports 101.

### 5.3 Difficulties

No SCADA protocol presently offers "plug-and-play" functionality. This is one of the areas where the UCA2 initiative may show promise.

Considerable familiarity with DNP and IEC 60870-5-101 are required to ensure that equipment can be configured to work together in a single system. The services of a consultant or system integrator (perhaps the system supplier) may be required if the utility does not maintain expertise in SCADA communication.

The "not invented here" syndrome is very apparent when reviewing product offerings that support these protocols. Typically a manufacturer has chosen one as a primary offering, and then implemented the other because of marketplace demand. The two protocols have very similar overall functionality, but familiarity with one protocol quickly clouds one's opinion or comprehension of the other.

## 6. Summary

Both DNP V3.00 and IEC 60870-5-101:

- Were specifically designed for transmission of SCADA data for electric power system control.
- Have wide market acceptance and are implemented by major equipment manufacturers.
- Are intended for use in SCADA systems using directly connected serial links: they do not specify how these connections are established or maintained.
- Require similar amounts of communications bandwidth to transmit the same amount of data.
- Are being extended to support LAN or WAN operation.

When first deciding to implement either DNP or IEC 60870-5-101, a factor to select one over the other is the determination of what other systems or equipment are to be incorporated. If it is likely that some existing equipment is to be included that already supports only one of the protocols, then this should be chosen. Otherwise there is little technical merit in specifying either protocol. It is more appropriate to specify desired system functionality and review the submissions from vendors. Typically each vendor will have a preference for one of these protocols. This may be based on the geographic location of their major market (Europe or USA) or their individual experience with these protocols. There may also be a price differential. The user should choose the system that provides the desired performance at an acceptable price, rather than base the decision on protocol selection.

Once a system has one of these protocols installed, this would normally be specified for future equipment to be added to the system. It is possible to introduce protocol converters to allow DNP and 101 to be mixed on the same system, but the engineering effort to configure and maintain this is difficult to justify.

By the year 2005, the directions to be taken by the next generation of SCADA protocols will be clear. DNP and the IEC 60870 family may evolve to provide new functionality or transport options, or UCA2 may prove to provide significant benefits and become a dominant system.

DNP and IEC 60870-5-101 should have a useful system life until at least the second decade of the next century.

## 7. References

### 1. International Standard

Telecontrol equipment and systems — Part 5: Transmission Protocols — Section 101: Companion standard for basic telecontrol tasks,  
International Electrotechnical Commission Publication 870-5-101: 1995.

### 2. DNP V3.00 “Basic 4”: Data Link Layer, Transport Functions, Application Layer and Application Object Library; Subset Definitions, DNP User Group

### 3. IEEE Standard P1379

Trial Use Recommended Practice for Data Communications Between Intelligent Electronic Devices and Remote Terminal Units in a Substation

## 8. Useful Web Sites

DNP User Group	<a href="http://www.dnp.org">http://www.dnp.org</a>
IEC	<a href="http://www.iec.ch">http://www.iec.ch</a>
IEC 870-5 Info	<a href="http://www.TriangleMicroWorks.com">http://www.TriangleMicroWorks.com</a>
SCADA Mail List	<a href="http://www.iinet.net.au/~ianw">http://www.iinet.net.au/~ianw</a>
IEEE	<a href="http://ieee.org">http://ieee.org</a>

## 9. Contact

The author may be contacted by email at: [awest@TriangleMicroWorks.com](mailto:awest@TriangleMicroWorks.com)



# Communications Standards in Power Control

SS101

SCADA Communications  
Protocol Standards for the  
Electricity Industry

Andrew West  
Andrew West



Triangle MicroWorks, Inc.

# Course of Discussion

- A brief history of SCADA protocols
- SCADA protocol attributes
- Directions in electric power SCADA standards

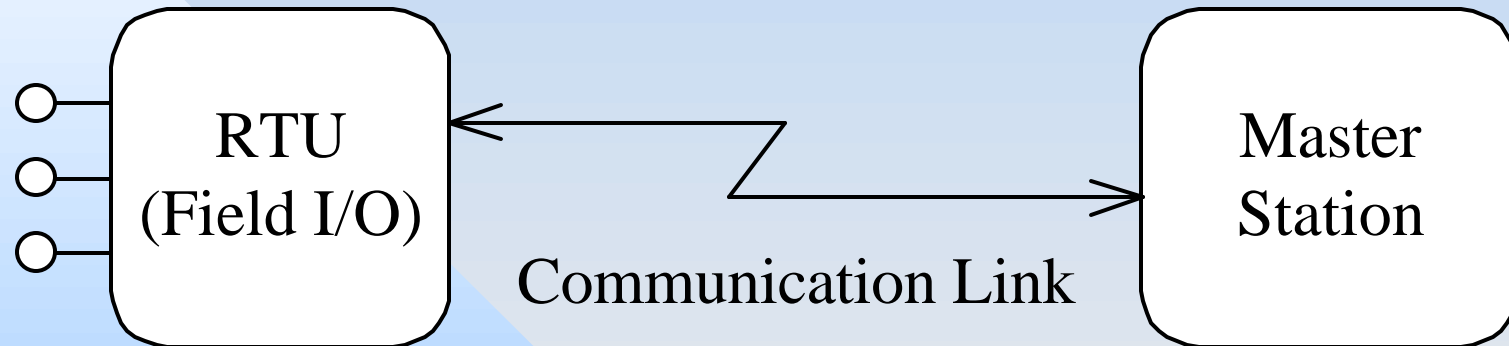
# History of SCADA Protocols

- First electric power remote control systems in 1940's
- Early SCADA systems in 1950's
- Each vendor provided their own solution
  - Multiplicity of proprietary protocols
  - Little or no compatibility between systems

# History of SCADA Protocols...

- Event processing schemes in 1970's
- Unsolicited reporting in 1980's
- Integration of multiple devices
- Impact of data networks
- Push for standardisation

# Typical SCADA Architecture



# Electricity SCADA Requirements

- High Data Reliability
- Control Security
- Small Data Sets
  - Bits to 1,000's bits
- Data Concentrators

# Electricity SCADA Requirements...

- Multi-Drop Network Topologies
- Allow Low Data Speed Communications
- Capture Transitory Events
- Conservative Industry
  - Slow acceptance of influence from other industries

# Data Reliability

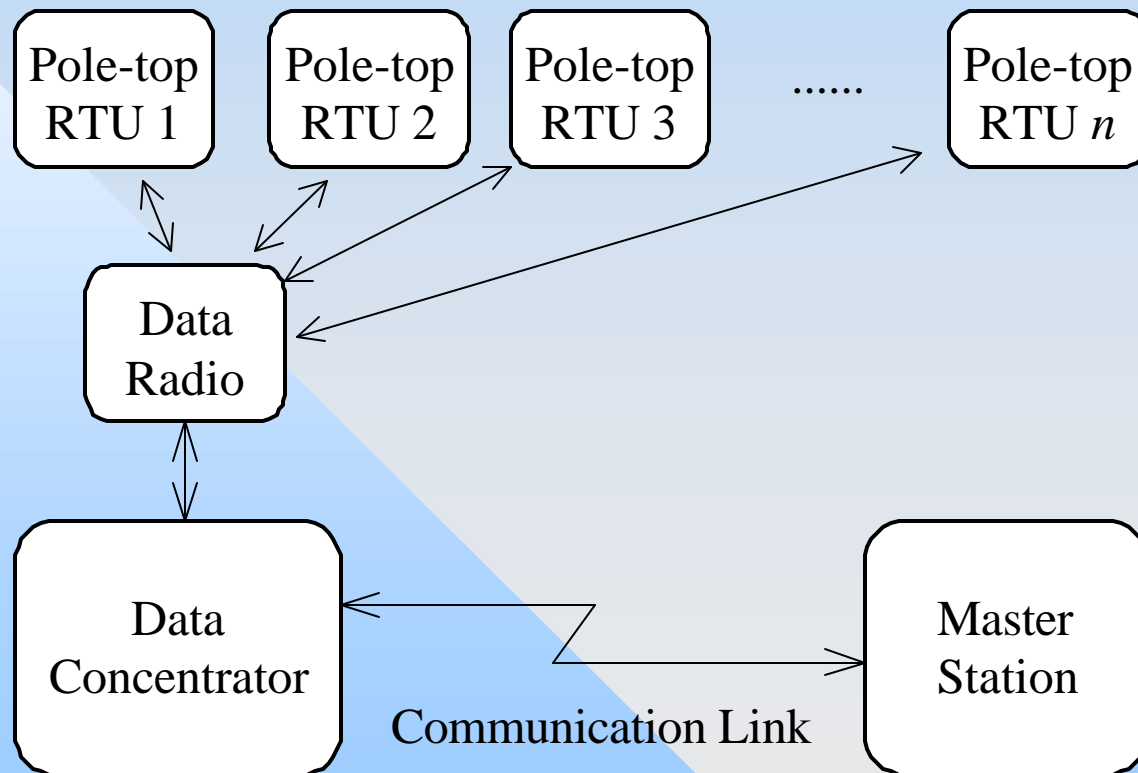
- Message Packet Framing
  - Check codes for error detection
- Data Validation Information
  - Data quality flags
  - Device integrity indicators
- Multi-bit Digital Data



# Control Security

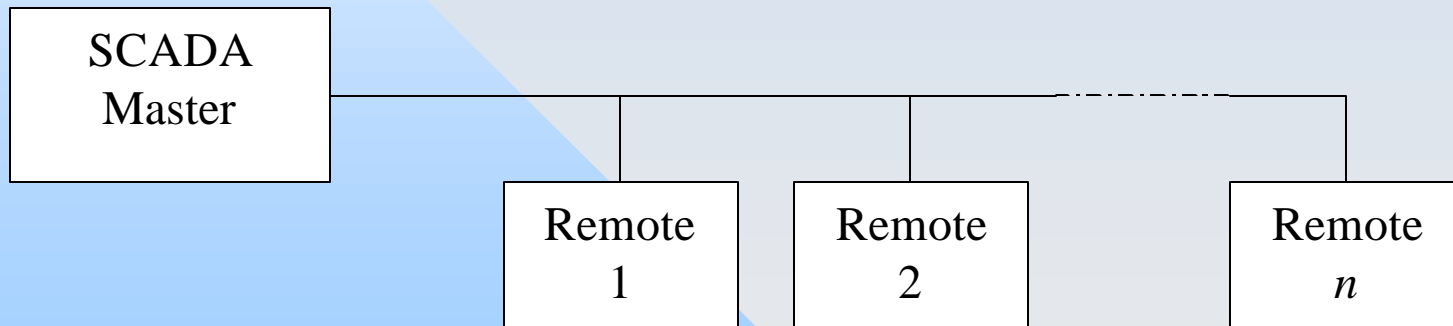
- Frame Integrity
- 2-Pass Control Strategy
- Hardware Verification Before Operation
- Redundancy/Security of Protocol Objects

# Data Concentrator Architecture



# Multi-drop Topology

- Each device ignores messages addressed to other devices



# Capture Transient Events

- Momentary Change Detect (MCD)
  - suitable for use with state-based systems
  - Similar to a R/S Flip-Flop
- Sequence of Event (SOE)
  - Time-stamped event data

# Traditional Approach (1960's)

- Conitel Protocol
  - Synchronous serial stream
  - 32-bit Blocks
    - 4-Bit Address
    - 4-Bit Subaddress/Group ID
    - 4-Bit Function
    - 12-Bit Data Elements
    - BCH Error detection/correction

# Event-Oriented Approach

- Harris 5000
  - Uses an event-reporting model
  - Report either current state or only changes in state
  - Includes some data validity

# Emergence of Standards

- IEC Technical Committee 57 WG 03
  - Produced IEC 60870 Series of Standards
- DNP User Group
  - DNP has been placed in the Public Domain
  - Technical Committee maintains DNP
  - Based on early work of IEC TC57

# Emergence of Standards...

- Electric Power Research Institute (EPRI)
  - Research Project Producing UCA2
  - UCA2 is more concerned with Substation Automation than SCADA communications
- IEEE Power Engineering Society  
Both DNP and IEC 870-5-101 have been specified in IEEE P1379 *Trial Use Recommended Practice for Data Communications Between Intelligent Electronic Devices and Remote Terminal Units*



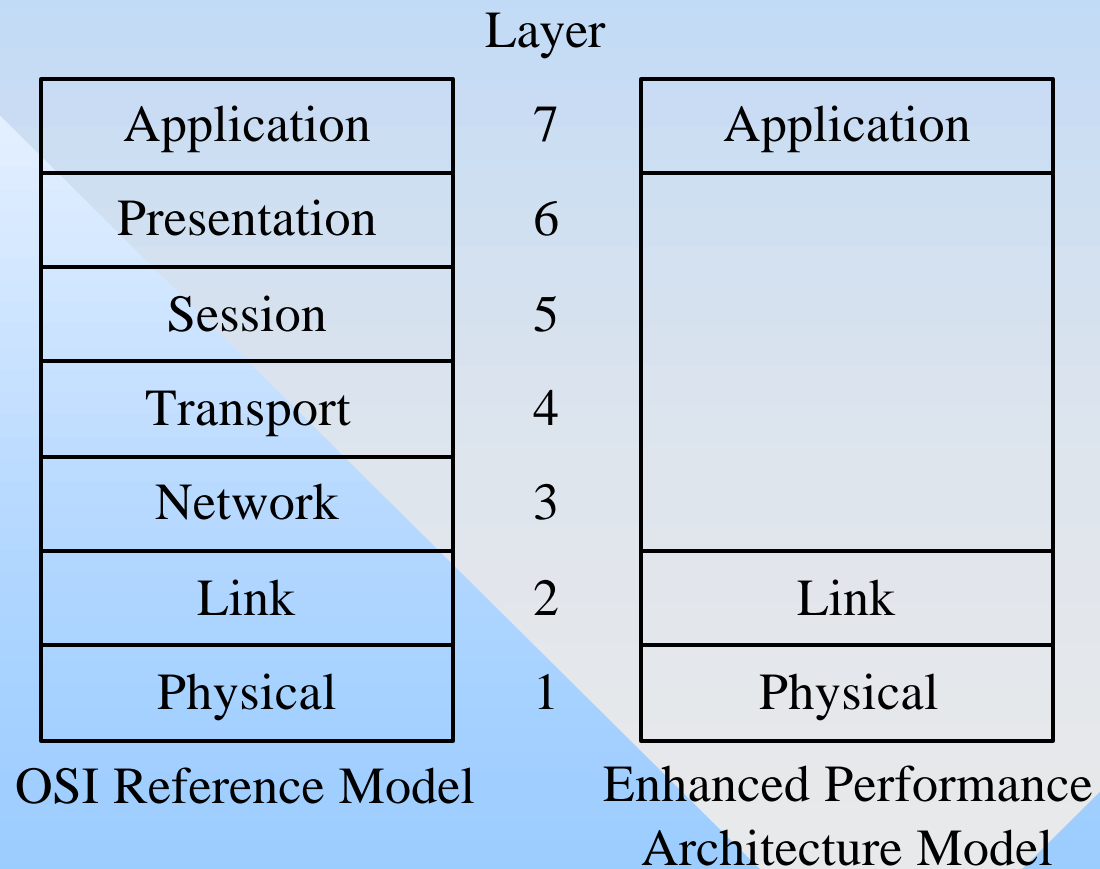
# IEC 60870 Standards

- Work in Progress Since Mid-1980's
- 60870 (870) is a Framework for Specifying SCADA Protocols
- 60870-5-101 (1995) is a Completely Specified Example of a SCADA Protocol
- 60870-5-104 Coming Soon

# Distributed Network Protocol

- Originally produced by Westronic
- Based on early parts of IEC 60870
- Placed in Public Domain early 1993
- Active Protocol Maintenance

# Reference Models



# IEC Frame Formats

Frame Type	Hamming Distance	Security	Max Length
FT1.1	2	Even Parity	128
FT1.2	4	8 bit Checksum	255
FT2	4	8 bit CRC	255
FT3	6	16 bit CRC	255

FT1.1 & 1.2	Isochronous
FT2 & 3	Synchronous

# 60870-5-101 & DNP...

- Collection of binary (digital) data
- Collection of analogue data
- Collection, freezing and clearing of counters
- Grouping data objects

# 60870-5-101 & DNP...

- Single pass or two-pass control of binary (digital) outputs
- Single pass or two-pass control of analog outputs
- Reporting of binary and analog events (report by exception)

# 60870-5-101 & DNP...

- Time synchronization
- Time-stamping events
- File Transfer
- Unsolicited Event Reporting
- Messages Include Identifying Information

# 101 & DNP Differences

Attribute	101	DNP
Frame Type	FT1.2	Pseudo-FT3
Reference Model	3-Layer EPA	EPA Plus Pseudo-Transport
Data Link Procedures	Unbalanced or Balanced	Balanced
Function	Inferred from Link Layer	Specified in Application Layer
Application Objects	Power System Specific	Generic



# Paradigm Differences

- DNP allows multiple object types in one message
  - better data packing
  - more complex message analysis
- DNP uses simple object types
- DNP has a better defined set of implementation options

# Paradigm Differences...

- 101 includes a "Cause of Transmission"
- 101 allows application commands in data link messages
- DNP transport functions allow larger data objects
- DNP defines functionality to a greater extent

# Paradigm Differences...

- DNP prioritizes data into Classes by point assignment
- 101 prioritizes data according to how it came to exist: Class 2 is for "Cyclic" data
- Understanding one paradigm does not aid understanding the other

# SCADA on the Web

- Email discussion groups:
  - [scada@gospel.iinet.com.au](mailto:scada@gospel.iinet.com.au)
  - IEC 60870-5: enroll from <http://www.TriangleMicroWorks.com>
- Web sites
  - DNP information: <http://www.dnp.org>
  - IEC information: <http://www.iec.ch>

# Things to Remember

- Both DNP & IEC 60870-5-101 were designed for electric power SCADA, and have wide market acceptance
- Are intended for permanent serial links
- Importance of standardisation

## Note

Communications can be the most important part of a SCADA system.

# Questions?

- Contact:  
[awest@TriangleMicroWorks.com](mailto:awest@TriangleMicroWorks.com)

