



This presentation was originally prepared for the January 1997 meeting of the DNP Users Group.

It has been revised to clarify ambiguous items; in response to comments received from industry experts; and to reflect recent changes in the respective protocols descriptions and items under review by the IEC and DNP Technical Committees.

Andrew West

15th September, 1999



Comparison of DNP and IEC 870-5-101

Jim Coats
President, Triangle MicroWorks Inc.
Vice President, DNP User's Group

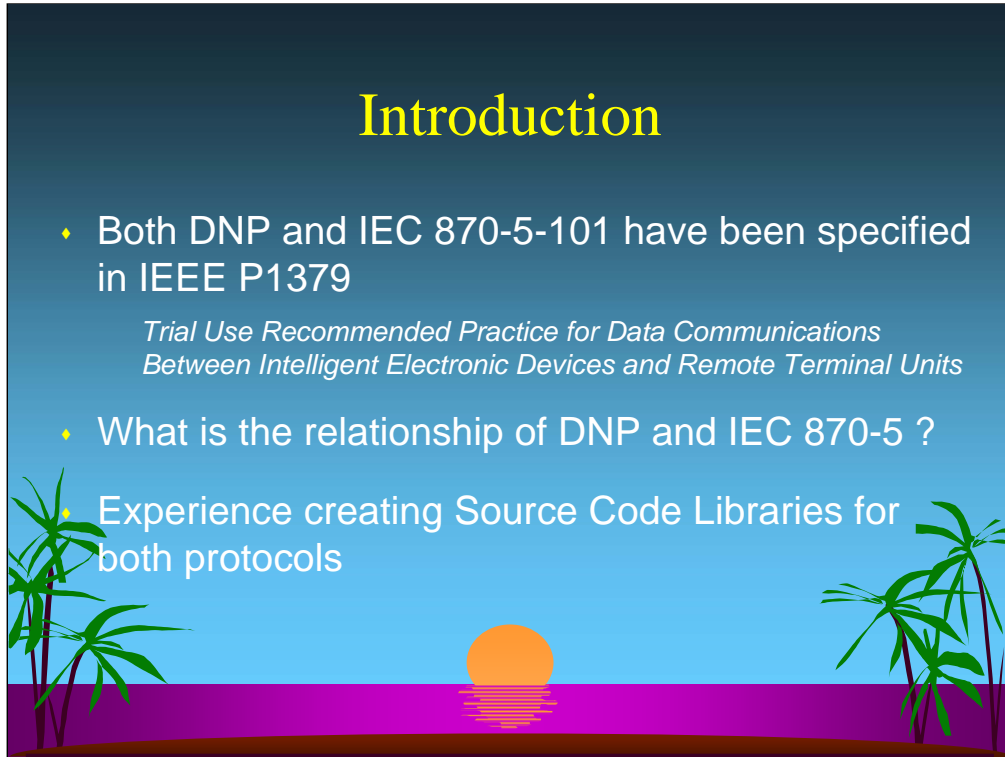
Revised September 1999

Introduction

- 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*

- What is the relationship of DNP and IEC 870-5 ?
- Experience creating Source Code Libraries for both protocols



Is DNP Based on IEC 870-5?

DNP's framing is based on (but not identical to) a framing format specified in 870-5-2. The application layer is not based on any of the 870 standards. DNP was specified soon after 870-5-2 was published, before the 870-5-4, -5 and -101 application standards were published.

Is DNP IEC 870-5 compliant?

No.

Introduction

- ♦ Objective is to compare protocols, not to conclude one is better
- ♦ Both are used world-wide, but selection is often based on location
 - DNP => Dominant in North America & industrialized Southern Hemisphere countries
 - IEC 870-5 => Dominant in Europe & Middle East

Both protocols provide similar application functionality.

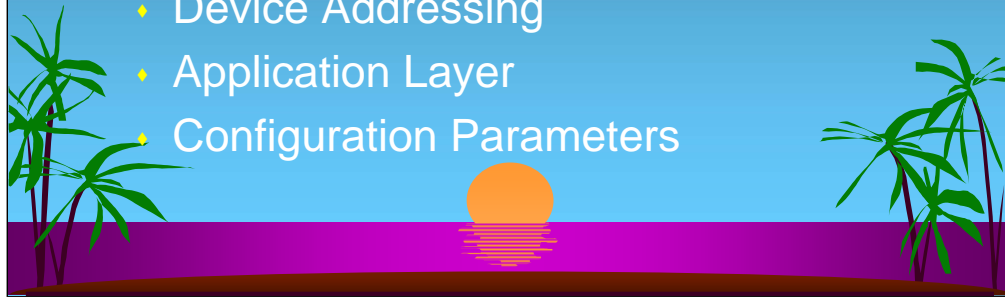
They were primarily designed for point-to-point or multi-drop serial link architectures, but can work over radio, LAN, etc.

Both protocols are used worldwide for electric power SCADA. DNP is dominant in North America, Australia, South Africa. IEC is required by legislation in some European countries. It is also common in the Middle East. In most of Asia and South America both are used almost equally.

DNP has gained wide acceptance in non-electric power applications, where IEC is little used.

Agenda

- ♦ Background Information
- ♦ Protocol Specifications
- ♦ Data Link
 - Balanced
 - Unbalanced
- ♦ Device Addressing
- ♦ Application Layer
- ♦ Configuration Parameters



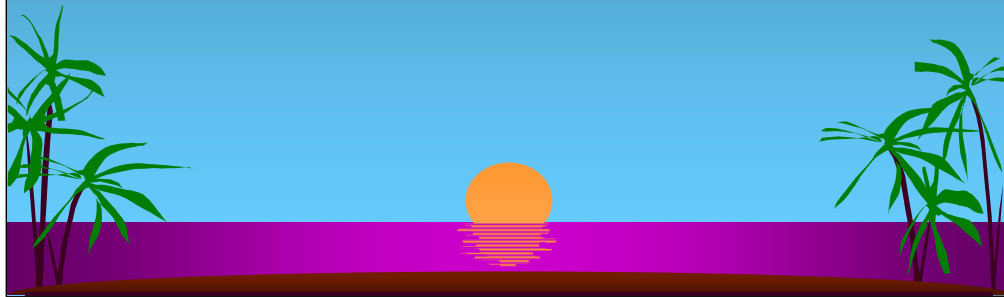
Background Information

- DNP
 - Developed by GE Harris
 - Based on early parts of IEC 870-5
 - Turned over to Users Group in 1993
- IEC 870-5-101
 - Technical Committee 57 Working Group 03 Chartered to develop the standard
 - Documentation finalized June 1995

- DNP continues to be expanded by the addition of new objects, under the guidance of the DNP Technical Committee.
- IEC 870-5-101 has been expanded with new objects to transport more-complete time tags. Further amendments are in production by the IEC Working Group.

Core Specification Documents

- ♦ DNP V3.0 Basic 4 Document Set
 - DNP V3.0 Data Link Layer
 - DNP V3.0 Transport Functions
 - DNP V3.0 Application Layer Specification
 - DNP V3.0 Data Object Library



The DNP Basic 4 document set is augmented by a Subset Definition document, a number of Technical Bulletins and Conformance Test Procedures. All of these documents are available for download by DNP User Group members from the DNP web site.

Core Specification Documents

- ♦ IEC 870-5 Standard Documents
 - IEC 870-5-1 Transmission Frame Formats
 - IEC 870-5-2 Link Transmission Procedures
 - IEC 870-5-3 General Structure of Application Data
 - IEC 870-5-4 Definition and Coding of Application Information Elements
 - IEC 870-5-5 Basic Application Functions



The IEC standards may be purchased directly from the IEC in Switzerland, or from the national standards bodies in most countries. The documents can be downloaded from the IEC web site.

Implementation Agreements

- DNP V3.0 Subset Definitions Document (Level 1, 2, & 3)
- IEC 870-5-101: Basic telecontrol tasks (Communication with RTU's)
- IEC 870-5-102: Transmission of integrated totals
- IEC 870-5-103: "Informative interface" of protection equipment
- IEC 870-5-104: Network access for IEC 870-5-101

IEC 870-5-101: published November 1995

IEC 870-5-102: published June 96

IEC 870-5-103: published December 1997

IEC 870-5-104: CDV February 1999

104: The ASDU's from IEC 870-5-101 are used, but the lower layers are based on standard transport profiles

101: Addendum adding new time-tag formats for event objects (RVC November 1998), addendum with supplementary definitions in preparation.

The 101, 102 and 103 profiles are essentially separate application protocols that have common design elements.

An interoperability checklist is used in 101 to identify the protocol subset supported by a device.

DNP specifies Subset Levels and a device profile document to identify interoperability between devices.

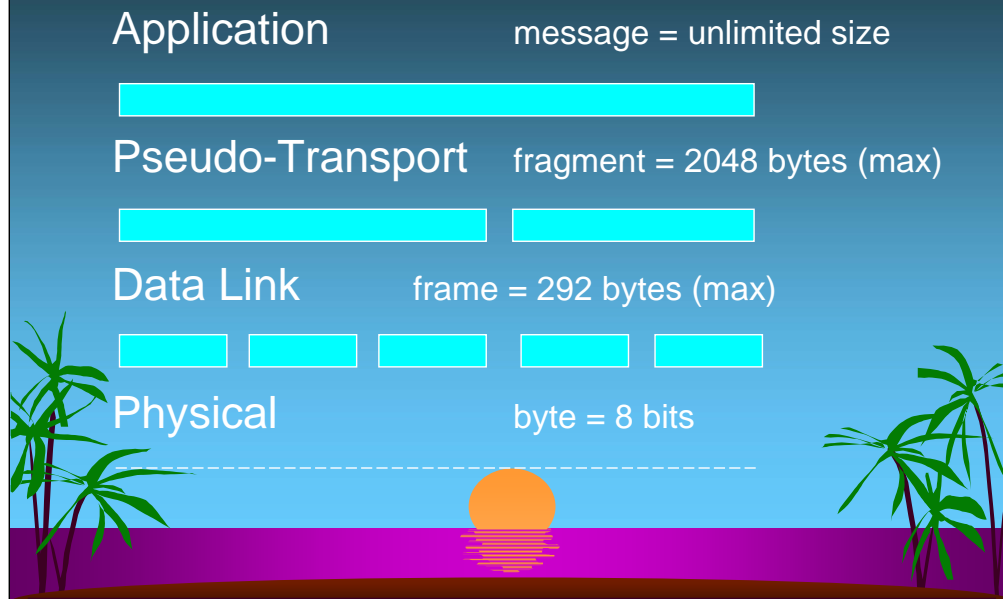
OSI 7-Layer Model Compliance

- ♦ Both protocols use a simplified 3 layer version of the OSI 7 Layer model called EPA (Enhanced Performance Architecture)
- ♦ DNP adds a Transport layer to permit single-function messages larger than a data link frame
- ♦ Every 101 Profile single-function message is sent as a single data link frame

In DNP all application layer functions are implemented as application layer messages encapsulated in data link frames.

101 supports a mechanism to specify a set of application functions (e.g. poll requests) in a data link layer message containing no application data. This improves efficiency, but blurs the separation of application and data link functionality.

DNP Message Buildup



- Receive goes up the stack, transmit goes down the stack.
- Size of data transmitted/received may fit into one data link frame. So do not require multi-frame fragments or multi-fragment messages.
- A single DNP application function is usually sent as a single application layer message, which can consist of many data link frames.
- IEC 870-5 has no transport layer. Each data link frame containing application data is a complete application message. A single application function (e.g.: interrogation) may require that several messages are sent to complete the function.

Data Link

- ♦ IEC 870-5 Defines 4 different frame types
 - FT1.1, FT1.2, FT2, FT3
- ♦ IEC profiles 101, 102 and 103 specify FT1.2
- ♦ Hamming distance and residual error probability provide a measure of the reliability of the communications link



Major differences between frame formats

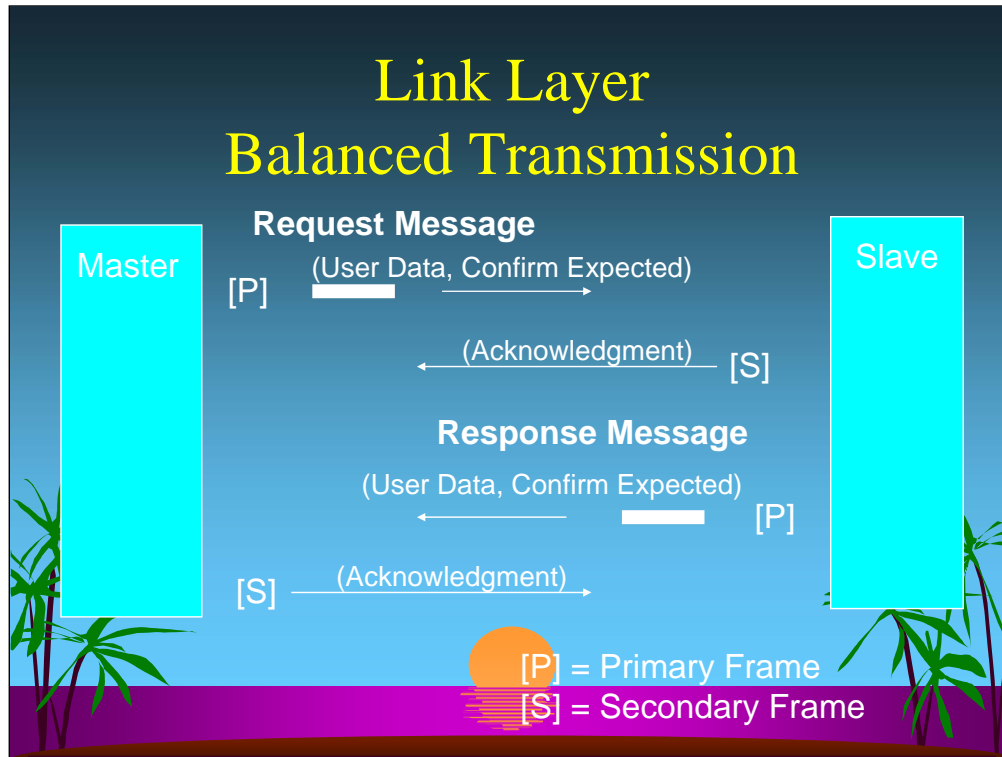
Address size and format for source and destination are specified in DNP, a single address size is selected from several options in 101.

DNP only uses variable-length frames. IEC 870-5-101 uses single character ACK, fixed-length frames and variable-length frames.

Hamming distance is the number of single bit errors which must occur for a corrupted message to be mistaken for a valid message

IEC 870-5 Frame Type Comparison

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

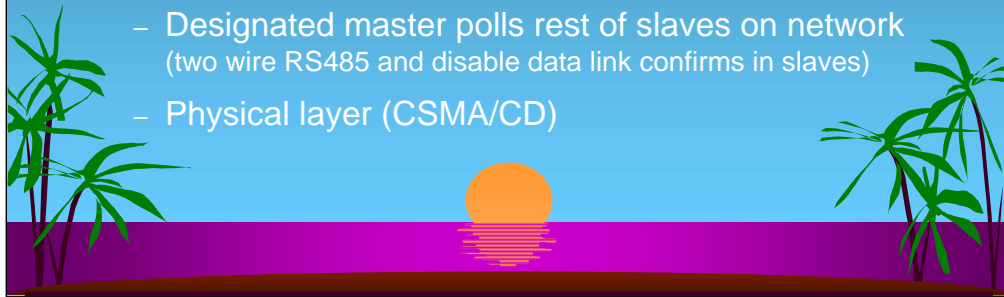


DNP only uses balanced transmission

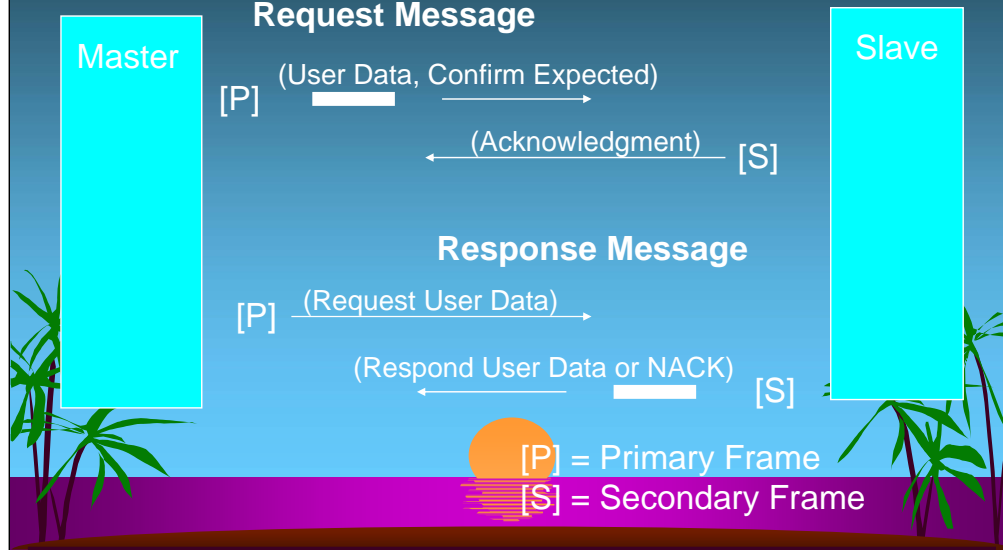
IEC profiles permit either balanced or unbalanced transmission

Link Layer Balanced Transmission

- ♦ At the link layer, all devices are equal
- ♦ Collision avoidance by one of the following:
 - Full duplex point to point connection (RS232 or four wire RS485)
 - Designated master polls rest of slaves on network (two wire RS485 and disable data link confirms in slaves)
 - Physical layer (CSMA/CD)



Link Layer Unbalanced Transmission



Not supported in DNP

Link Layer

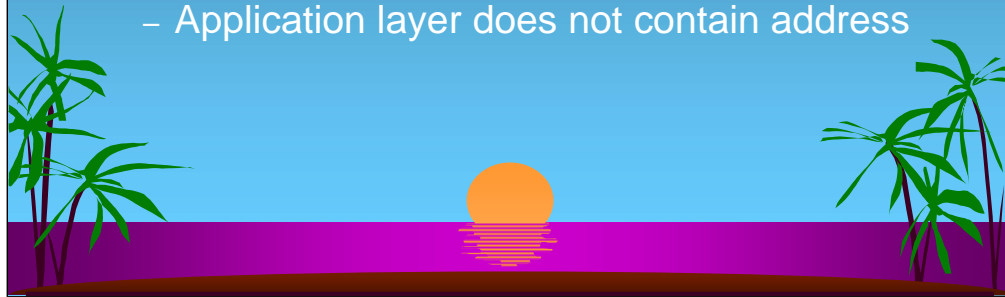
Unbalanced Transmission

- Only Master device can transmit primary frames
- Collision avoidance is not necessary since slave device cannot initiate exchange, or retry failed messages
- If the slave device responds with *NACK: requested data not available* the master will try again until it gets data, or a response time-out occurs



Device Addressing

- ♦ DNP
 - Link contains both Source and Destination address
 - Both are always 16 bits
 - Application layer does not contain address



The provision of a source and destination address simplifies message routing in certain network topologies.

A DNP link address is a device's logical address. A single physical device is permitted to respond to multiple addresses (contain multiple logical devices). Each device will appear to the master as a completely separate device.

Device Addressing

- ♦ IEC 870-5-101
 - Link address can be 0, 1, or 2 bytes
 - Unbalanced link always contains the slave address (destination of primary messages, source of secondary messages)
 - Balanced link is point to point only, so link address is optional (but may be included for security). The application layer address identifies data.
 - Link addressing prevents peer to peer network of more than 2 devices

The DNP concept of “peer-to-peer” operation where pairs of devices may swap “master” and “slave” roles does not appear to have a parallel in the IEC profiles.

Device Addressing

- ♦ IEC 870-5-101 (continued)
 - Application layer *sector address* (common address of ASDU) can be unrelated to link address of device
 - Can have multiple *sector addresses* per device
 - Application layer may contain an optional Source Address



IEC 870-5-101 Application Layer

- ♦ Review DNP Application Layer Diagram
- ♦ Show ASDU diagram

Type ID - Identifies the object format

Qualifier

Quantity of points
indexed or sequence of points

Cause of Transmission - optional originator address
e.g.: cyclic; spontaneous; activation; activation
termination

ASDU Address - 8 or 16 bits fixed

Information Object Address - 8, 16, or 24 bits fixed

Point number - repeated if qualifier is indexed

Data - repeated *quantity* times

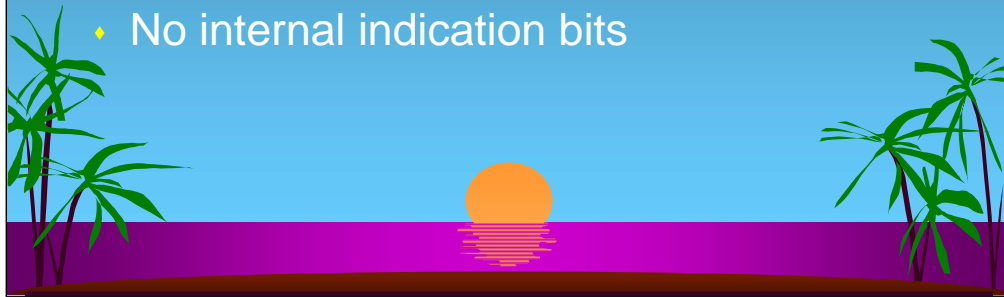
Application Layer Both Protocols Provide:

- Time Synchronization
- Time-stamped events
- Freeze/Clear Counters
- Select before operate
- Polled report by exception
- Unsolicited Responses
- Data groups/classes

End result of application layer is very similar
Different means to accomplish same task

IEC 870-5-101 Application Layer

- ♦ Limited to single data type per message
- ♦ Can only control one point per message
- ♦ No application layer confirms for events
- ♦ No internal indication bits



DNP permits multiple data types in one message. 101 requires one data type per message.

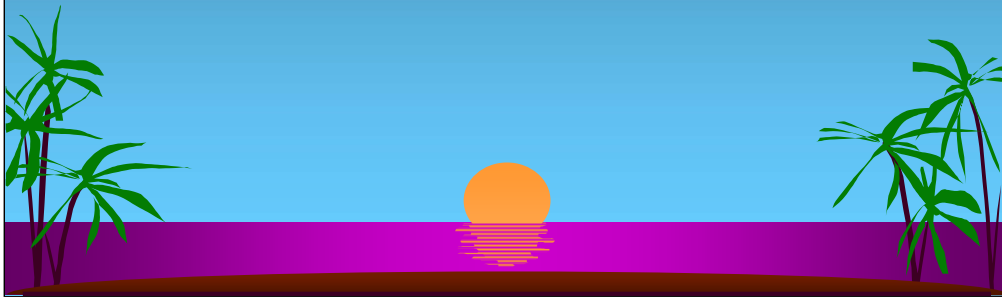
DNP permits multiple points to be controlled in one message transaction sequence (e.g. select/execute). 101 requires a separate transaction sequence for each control point.

DNP relies on an application layer confirm to guarantee the master has received events before clearing them from an event buffer. 101 relies on the security features of the data link layer.

DNP defines specific indications. 101 relies on configuring of particular process variables as indications to provide any necessary functions.

Configuration Parameters Required for Basic Communication

- ♦ DNP
 - Baud Rate
 - Device Address
 - Fragment Size



Configuration Parameters Required for Basic Communication

- ♦ IEC 870-5-101
 - Baud Rate
 - Device Address
 - Balanced/Unbalanced
 - Frame Length
 - Size of Link Address
 - Size of ASDU Address
 - Size/structure of Point number
 - Size of Cause of Transmission

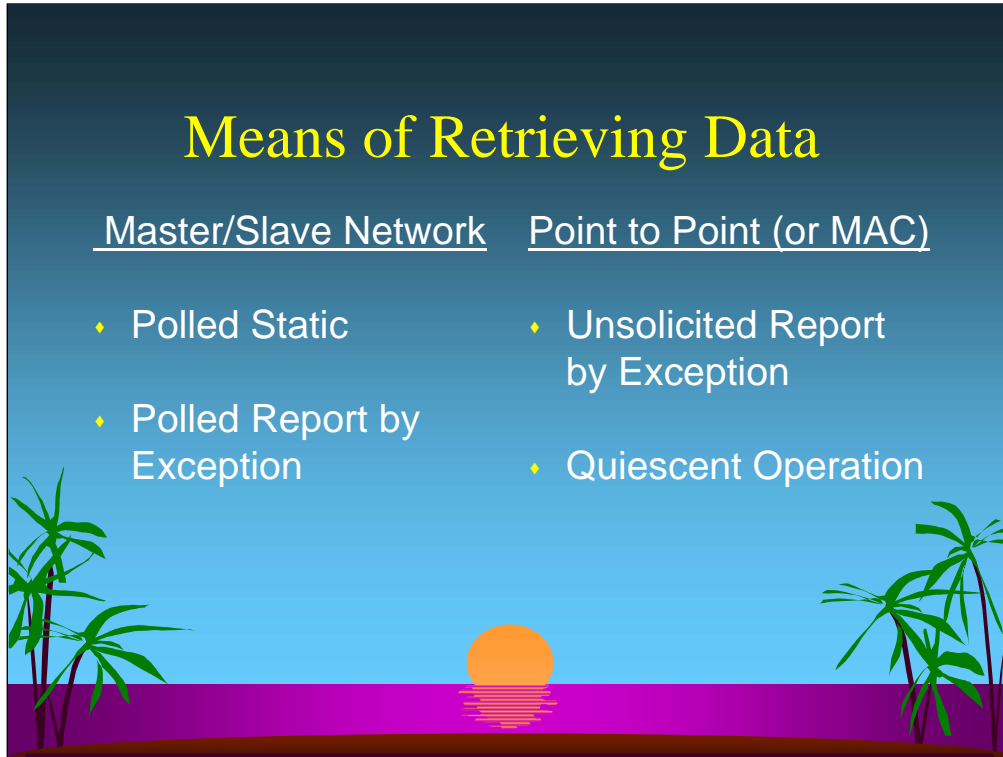
Means of Retrieving Data

Master/Slave Network

- Polled Static
- Polled Report by Exception

Point to Point (or MAC)

- Unsolicited Report by Exception
- Quiescent Operation



Master/Slave Network - Slaves do not speak unless spoken to

MAC = Media Access Control - CSMA/CD

Polled Static - Class 0 or specific data request message sent to each device

Polled Report by Exception - Class 1, 2, 3 request message sent to each device with occasional integrity (class 0) data poll.

Unsolicited Report by Exception - most communication is unsolicited, but the Master occasionally sends integrity polls for class 0 Data to verify its' database.

Quiescent Operation - master never polls slave

Last two modes are useful when communication medium is dial-up modem.

Additional IEC 870-5 Data Acquisition Methods

- ♦ Cyclic Data Transmission
 - Eliminates static data poll message from master
 - Balanced or unbalanced link layer
 - Interrupted by event-triggered communication requests



Conclusions

- Combining DNP function code and data format into the *Type ID* field reduces confusion, but limits message to one data format
- IEC 870-5-101 has a simpler qualifier code
- The above items replace the implementation tables in a DNP Device Profile Document with check boxes

Because DNP permits multiple object types per message, it also requires a more complex object header format.

IEC uses a combination of Cause of Transmission and qualifier codes embedded in data objects (Type ID) in a similar manner to DNP's use of application function codes. DNP function code applies to all object types in the message.

Conclusions

- ♦ IEC 870-5-101 and DNP provide similar application functionality in similar ways
- ♦ To perform some functions, IEC 870-5-101 sends many small messages where DNP will send a smaller number of larger messages
- ♦ The larger number of low-level configuration options in IEC 870-5-101 tends to require greater knowledge on the part of a system integrator to successfully commission devices

More options in IEC typically means either more configuration options and support program code or else unsupported options so some IEC 870-5-101 devices do not communicate with other devices.

But: familiarity with one protocol makes the other look more complex, no matter which protocol is more familiar! Each has features that are elegant and simple, and features that are complex.

More Information on DNP & IEC 870-5

- ♦ DNP - www.dnp.org
- ♦ IEC - www.iec.ch
- ♦ IEEE P1379 - www.ieee.org
- ♦ IEC 870-5 Mail list - join at
www.TriangleMicroWorks.com/iec870-5/
- ♦ Australian based SCADA Mailing List - join at
www.iinet.net.au/~ianw
- ♦ Contact me, Jim Coats at:
jcoats@TriangleMicroWorks.com
www.TriangleMicroWorks.com
[+1 \(919\) 870-6615](tel:+19198706615)

No technical support provided directly by IEC: questions are usually handled by consultants, vendors or volunteers who may contribute to the mail lists.

DNP technical support is provided by the DNP Technical Committee. DNP User Group members are automatically enrolled on a DNP mail list forum. Technical questions can be submitted to this list.