
SUBNET™
SOLUTIONS INC.
ANY GRID PROJECT.
ONE INTEGRATION
SOLUTION.

DNP3: SCADA, Clear and Simple

Andrew West, Regional Technical Director, SUBNET Solutions
Chair, DNP Technical Committee

Agenda

- Introductions
- DNP3 philosophy & terminology
- Lesser-known features
- Current developments

Introductions

Contact Details

Andrew West

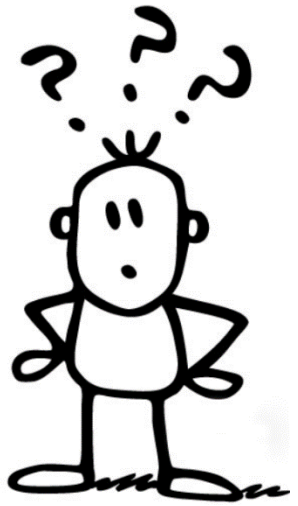
Regional Technical Director, Asia-Pacific

SUBNET Solutions Pty Ltd

Andrew.West@SUBNET.com

Introductions

Who are you?
What do you do?
Why are you here?



DNP3 philosophy & terminology

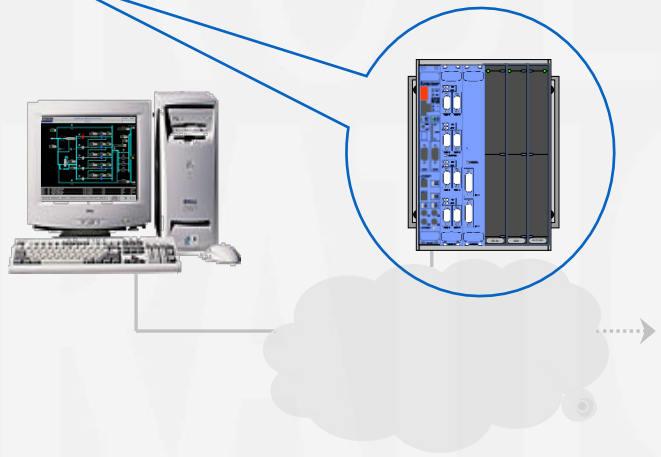
Programmers beware!

- DNP3 terminology uses terms differently from their meanings in common object-oriented programming languages
- Also: Different protocols use terms differently
  - Familiarity with one protocol can lead to confusion when looking at others
- Confusion often occurs with:
  - Objects
  - Types
  - Classes

Terminology: Master Station

- Master (DNP3)
- Master Terminal Unit (MTU)
- Human Machine Interface (HMI)
  - (previously MMI: Man Machine Interface)
- Controlling Station
- Control Centre Equipment
- Front-End Processor
  - Typically the communications interface
- SCADA Client

Terminology: Field Equipment



- Remote Terminal Unit (RTU)
- Remote
- Slave
- Controlled Station
- Outstation
- Data Concentrator (DCIU)
- SCADA Server
- IED: Intelligent Electronic Device
- PLC: Programmable Logic Controller

DNP3

DNP3 Device identification

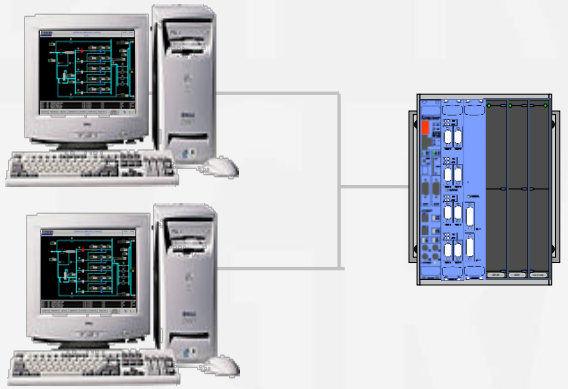
- Each DNP3 device (master or outstation) has a DNP3 address
  - DNP3 addresses are 2-octets or 16-bits in size (range 0 to 65,535 or 0x0000 to 0xFFFF)
  - Each device is assigned an address in the range 0–65,519 (0x0000-0xFFEF)
  - Addresses 65,520–65,535 (0xFFF0-0xFFFF) are reserved for broadcast and special functions
    - No device may be assigned one of these addresses
  - DNP3 addresses appear as “source” and “destination” address fields in the DNP3 data link frame of every message
- There is no implicit meaning to any address other than the reserved addresses: any master or outstation has any address 0–65,519

DNP3 Device identification

- DNP3 addresses are unique on a serial link
  - A single physical device may respond to multiple DNP3 addresses, each appearing to be a separate “logical” device
- DNP3 addresses are unique to each logical device that is accessed through a single IP address
  - Terminal servers may connect multiple serial devices “behind” a single IP address
  - A device with a single IP address may contain multiple DNP3 devices, each of which is considered a separate logical device

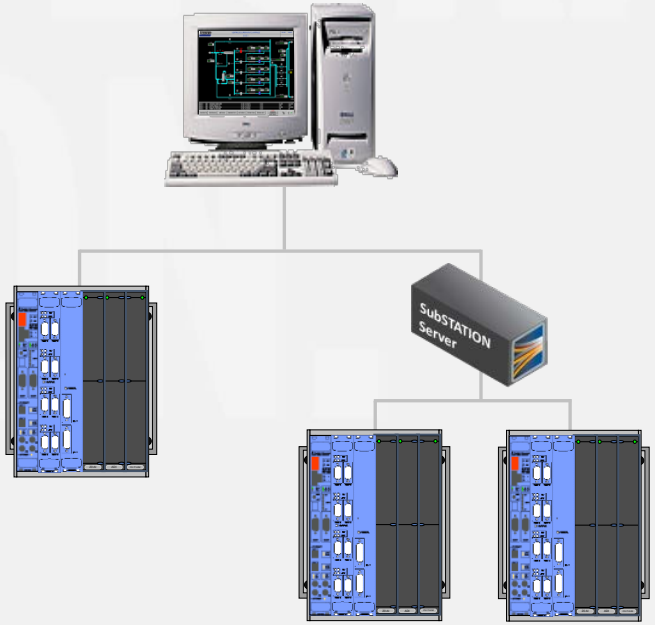
Supported Topologies

One to One



Muti-master

Multidrop



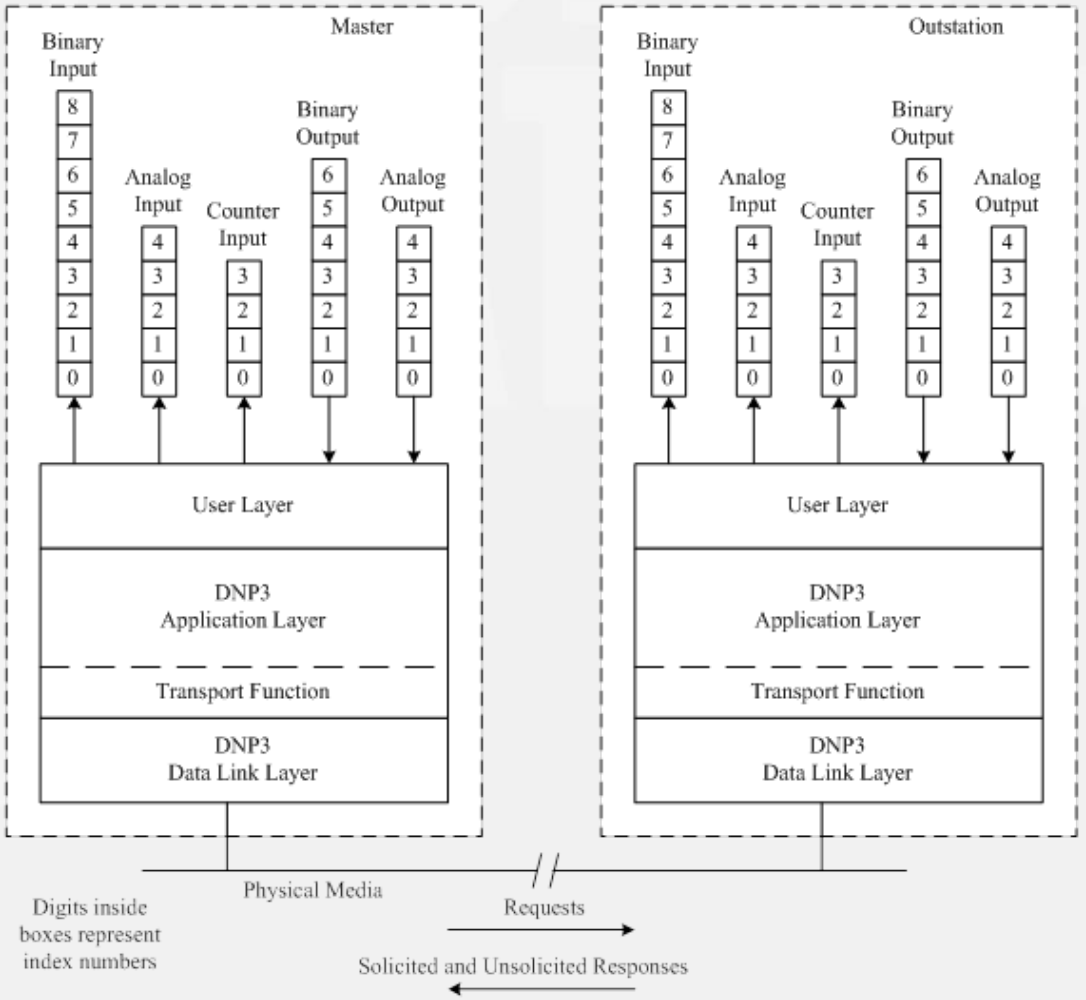
Heirarchical /
Data Concentrator

DNP3 Device identification

- Devices can be uniquely identified by:
  - Combination of DNP3 address and serial channel
  - Combination of DNP3 address and IP address
- From the master's viewpoint, each different outstation address on a single serial link or "behind" a single IP address is a different device
- An "Association" is the combination of a master and an outstation with which it communicates
  - Each association requires separate "housekeeping"
    - Initialization status
    - Message sequence numbers
    - Secure authentication management

DNP3 Data Model & Data Types

- DNP3 models data in terms of one-dimensional arrays of data per outstation:
  - Binary inputs & outputs
  - Analog inputs & outputs
  - Counter inputs (running & frozen)
  - Blob (“string”) objects
  - Data sets (structures of data)
- Data identified by
  - Outstation, data type & index



Data Identification

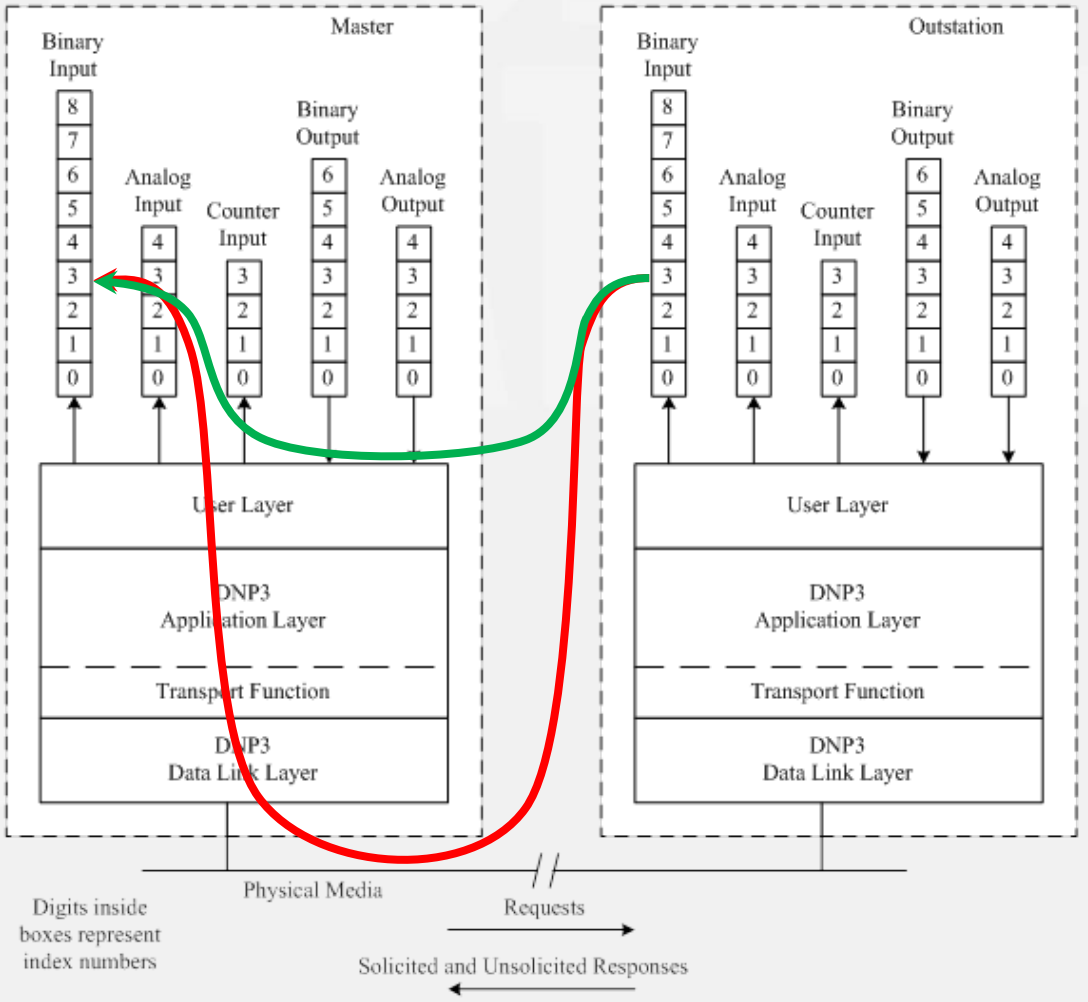
- Each data object (e.g. an individual binary input) is called a “Point”
- Data for a point has a value, quality and time of measurement
- For each data type (binary input, analog input, etc.)
  - “Static” data reports the current state of the point
    - Static does not mean “unchanging”, it just refers to the current “state” of the point
  - “Event” data reports a change or an update of the state of the point
    - Events might or might not indicate a change of state
    - Events are sent for any reason the outstation determines is worth reporting
      - Change of value
      - Change of quality
      - Periodic update
      - Etc…

Data Identification

- Static and event data in DNP3 messages are reported using different “Object Groups”
- Each Object Group has an identifying object group number
  - E.g. Binary Input static data is Object Group 1 & binary input event data is Object Group 2
- Object Groups indicate how to report data for each data type
- The associated static and event object groups for a specific index of any data type update the value of the same point

DNP3 Object Groups

- For example:
  - Binary input static data for index 3 reports the current value of the 4th binary input (indices start at 0)
  - Binary input event data for the same index updates the value of that same binary input
- Event data is stored in and reported from an event buffer
  - When a timestamp is reported, it is the time of data update



DNP3 Object Groups

Obj	Description	Type
0	Device Attributes	Attribute
1	Binary Input	Static
2	Binary Input Change	Event
3	Double Binary Input	Static
4	Double Binary Input Change	Event
10	Binary Output Status	Static
11	Binary Output Event	Event
12	Control Block (Binary Output)	Command
13	Binary Output Command Event	Event
20	Binary Counter	Static
21	Frozen Counter	Static
22	Counter Change Event	Event
23	Frozen Counter Event	Event
30	Analog Input	Static
31	Frozen Analog Input	Static
32	Analog Change Event	Event
33	Frozen Analog Event	Event
34	Analog Input Reporting Deadband	Static R/W
40	Analog Output Status	Static
41	Analog Output Block	Command
42	Analog Ouptut Event	Event
43	Analog Output Command Event	Event

Obj	Description	Type
50	Time and Date - All Variations	Info R/W
51	Time and Date CTO - All Variations	(Event)
52	Time Delay - All Variations	Info
60	Class Data	Command
70	File Transfer	Info R/W
80	Internal Indications	Static R/W
81	Storage Object	Info
82	Device Profile	Info
83	Private Registration Object	Info/Any
85	Data Set Prototype	Info
86	Data Set Descriptor	Info
87	Data Set Present Value	Static
88	Data Set Snapsot	Event
90	Application Identifier	Info
100	Floating Point (obsolete)	Static
101	Packed Binary-Coded Decimal	Static
102	Unsigned 8-bit Integer	Static
110	Octet String	Static
111	Octet String Event	Event
112	Virtual Terminal	Write
113	Virtual Terminal Event	Event
120	Authentication	Info

DNP3 Data Object Structure

- For point data:
  - An Object Group can report data in various formats
    - Analog inputs can be 16-bit integer, 32-bit integer or 32-bit or 64-bit floating point
    - Counters can be reported as 16-bit or 32-bit values
  - The different formats are known as “Variations” (identified by a number)
  - Any point can theoretically be reported in any variation
    - A specific analog input could be reported as a 16-bit or 32-bit integer or as a float: The same value would be reported in whichever variation is used (subject to scaling, overflow, rounding, etc.)
    - Each point has a default variation (which may be configurable)
  - A master may request the variation it wants reported
  - Variation 0 is specified in read requests to mean “any variation” (use default)

DNP3 Data Object Structure

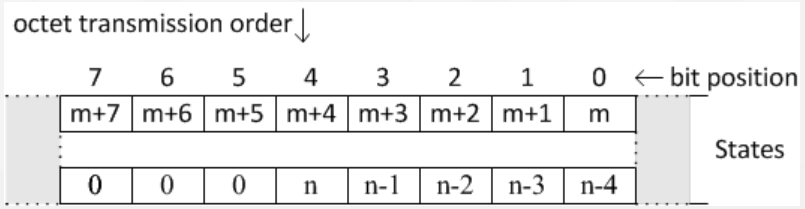
- Point data objects typically consist of:
  - Value
  - Qualifier flags
  - Timestamp (optional: events & frozen objects only)
- For Static data:
  - Some variations include qualifier flags, some don't
    - When qualifier flags are not reported, this means exactly the same as a variation with flags indicating "On-Line with no errors"
- In all cases, the Variation number indicates the format of the data object in the message

DNP3 Data Object Structure

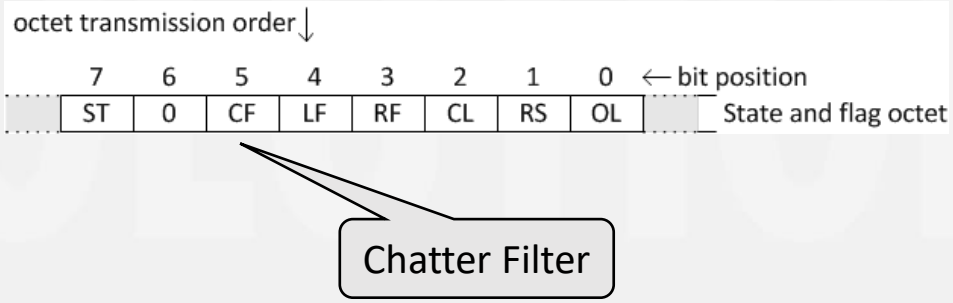
- 5 common flags: Normal Status (used in all data types)
  - On Line 1
  - Restart 0
  - Communication Lost 0
  - Remote Forced 0
  - Local Forced 0
- Additional type-specific flags (all normally 0):
  - Binary: Chatter Filter
  - Analog: Overrange & reference error
  - Counter: Discontinuity & rollover (rollover is deprecated)

Binary Input Variations

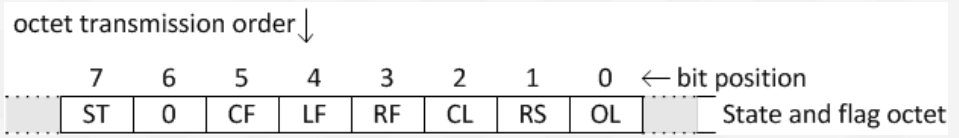
- Static (Object Group 1)
  - Variation 1: Packed (index m–n)



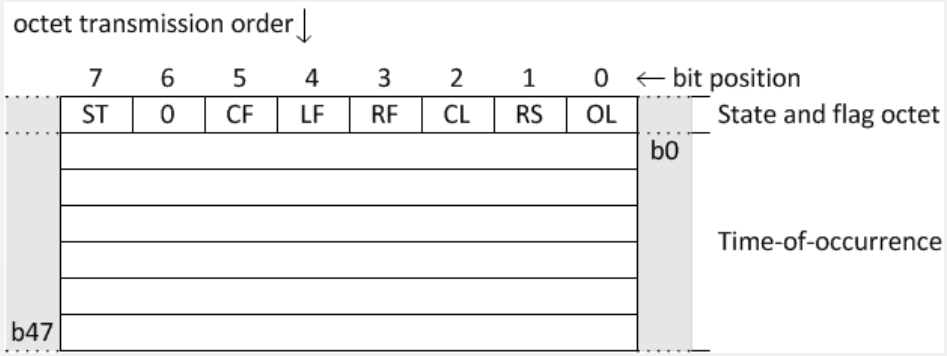
  - Variation 2: With Flags (per index)



- Event (Object Group 2)
  - Variation 1: Without time



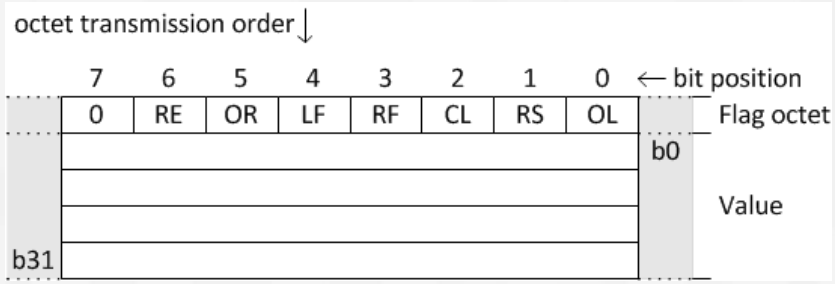
  - Variation 2: With time



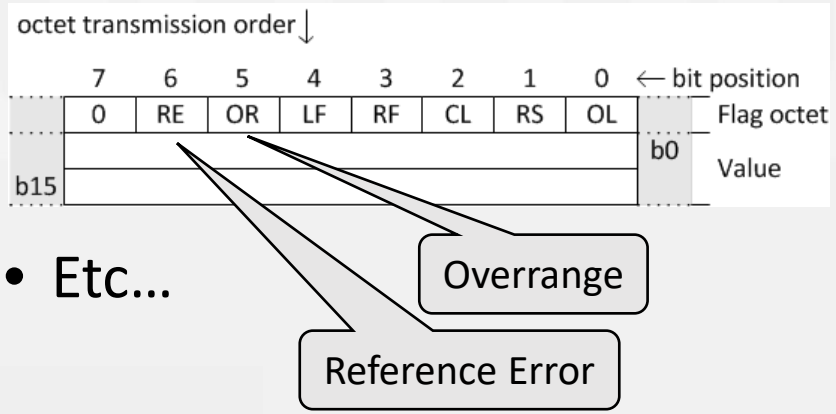
  - Etc…

Analog Input Variations

- Static (Object Group 30)
  - Variation 1: 32-bit with Flags

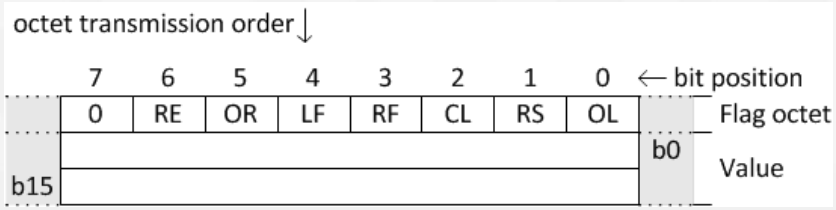


  - Variation 2: 16-bit with Flags

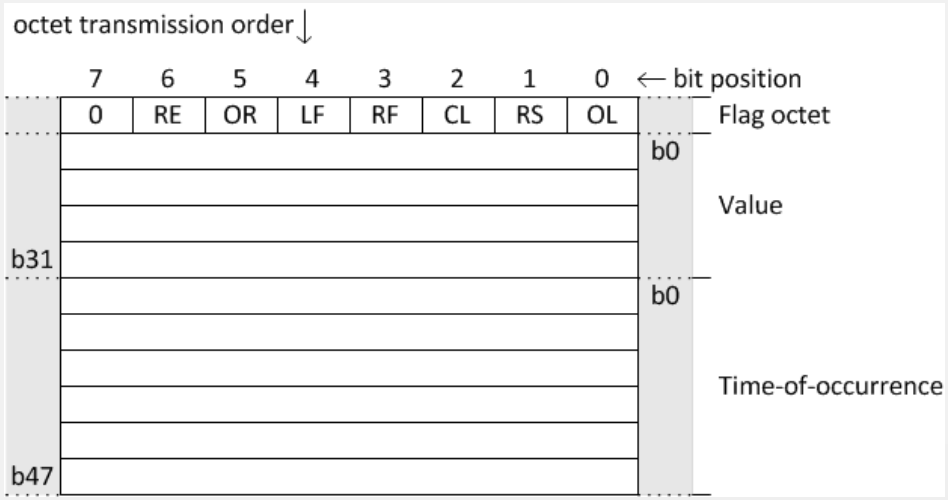


  - Etc…

- Event (Object Group 32)
  - Variation 2: 16-bit without time

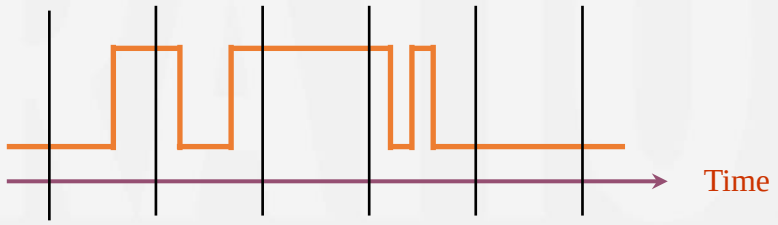


  - Variation 7: Short float with time



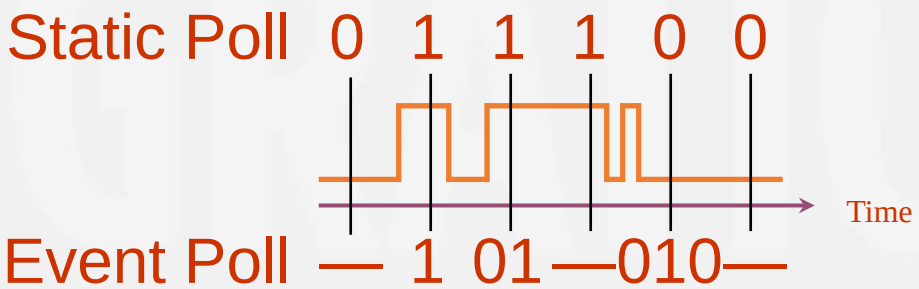
Polling

- Polling is typically a periodic process
  - Requests are issued by the master station
  - The outstation returns the data that is requested
- DNP3 supports polling by a master or “unsolicited reporting” from an outstation (or a mixture)
  - An outstation may spontaneously reports changes to the master, instead of being polled



Polling for Events

- Systems may:
  - Ignore values occurring between polls, return value at time of scan
  - Report changes, including those that occur between polls (Event Reporting or RBE)
    - after collecting the initial 0
- Analogs & counters
  - Events may indicate a significant change, a periodic update or whatever the outstation decides



(0 1 1 1 0 0)

(— 1 01 —010—)

RBE Reporting Model

- All changes reported as events (with or without timestamps)
- Current value need only be collected at start up or after data loss
- Use events for all SCADA data processes
  - Update database
  - Alarm processing
  - History

Data Handling

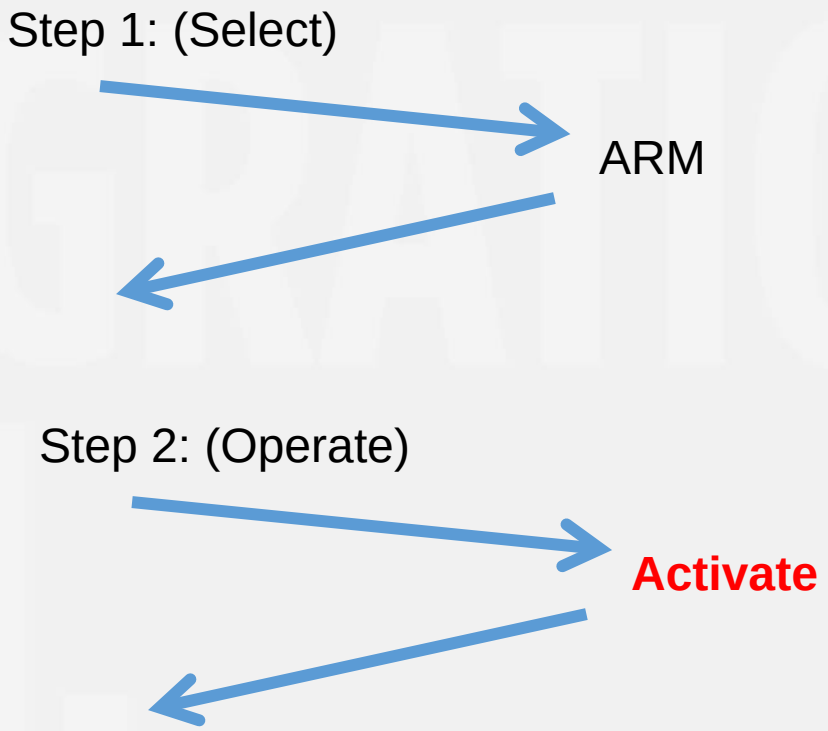
- Modern SCADA protocols use RBE
- Data reported is: {Value, Quality, Timestamp}
- Consecutive samples for each data object (point) is reported in the same order it is read
  - Master updates the database with data in the sequence received: the final value is the most recent value
- Event buffer overflow requires re-initialization by reading all current values

Control Commands

- Single Pass Command
  - Control command issued and immediately activated
  - Subject to incorrect commands due to communications errors

Control Commands

- Two Pass Command
  - "Select Before Operate" (SBO) or "Select Execute"
    - The first command, Select, "arms" an output and the outstation responds
    - The master receives response and checks it
    - If it is correct, the Operate or "activate" command is issued
    - The outstation verifies that the "Operate" matches the "Select"
  - Provides very high integrity against incorrect commands due to communications errors



All high integrity SCADA protocols support 2-pass controls

Structures and Paradigms

- DNP3 is based on a set of paradigms:
  - Report-By-Exception (RBE)
    - An initial image of field data is reported
    - Thereafter only “changes” are reported
    - Uses communications bandwidth efficiently
    - Requires data identification in messages
  - Uses a layered structure
  - Data for each object is always reported in the same order that it is measured
  - Reporting of event data is confirmed

DNP3 Classes

- In DNP3, Classes are used to collect together various kinds of data
- Each class may be polled with a different period
- A single class, Class 0, is the set of all kinds of static data
  - Class 0 may be considered to be identical to the set of static data for each kind of data point in a device:
    - Reading Class 0 is equivalent to reading all binary input static data and all analog input static data and all counter input static data, etc.
    - Some devices also include output point static data in Class 0
- Note for programmers: Classes in DNP3 are not “data structures”
  - DNP3 Object Groups and their Variations are “data structures” in messages

DNP3 Classes

- Three classes, Classes 1, 2 and 3 are sets of event data
  - The three classes may be considered as separate collections of points
  - Each event class may be polled at a different period or at the same period
    - Polling different classes at different periods assigns a different priority or maximum data latency to the class
    - There is no inherent ordering of priority of the event classes, the priority or periodicity of reporting depends on the system configuration
  - If events are to be reported for a point, its static value must be reported as part of the Class 0 data for the device
- Event data is buffered

DNP3 Classes

- Except for very small outstations, all DNP3 devices support event reporting
  - Small outstations are permitted to operate by only reporting static data
    - If the largest possible response to a poll for Class 0 data fits in one DNP3 Data Link Frame (no more than 249 bytes of Application Layer data), then the outstation is not required to support event reporting
- Normal DNP3 operation is by Class Polling
  - A combined poll for Classes 1, 2, 3 & 0 is an integrity poll (synch database)
    - Required at startup or after buffer overflow, may be requested occasionally
  - Events are periodically collected by requesting Classes 1, 2 and 3 periodically
    - May be polled together or independently

DNP3 Classes

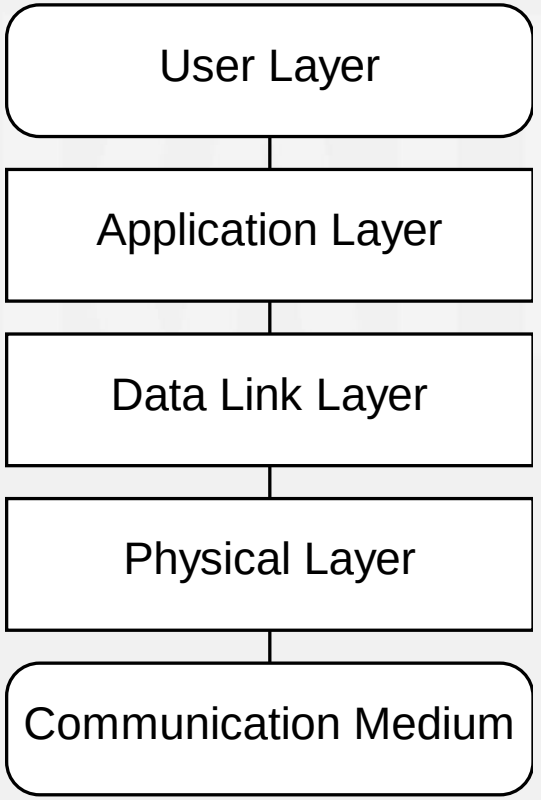
- Classes are “shorthand” descriptions for groups of other objects
  - Class 0 is a shorthand reference meaning the same thing as specifying all the static data types
  - Classes 1, 2 & 3 are groups of event objects
    - Specifying a class is a shorthand way of specifying the set of objects that report events in that class
    - Allows selection of three different reporting priorities
- The master can read objects or classes

DNP3 Classes

- The purpose of Class 0 is to collect all device data at startup: To capture an “initial database image”
  - Called “Integrity Poll”: Also collect events: Classes 1,2,3 & 0!
- All Static data is included in Class 0
- Event Classes allow grouping or prioritization in whatever manner the user chooses
- There is no implied priority of Event Classes
- It is possible to request a limited number of events in an event class poll

DNP3 Layers (EPA Model)

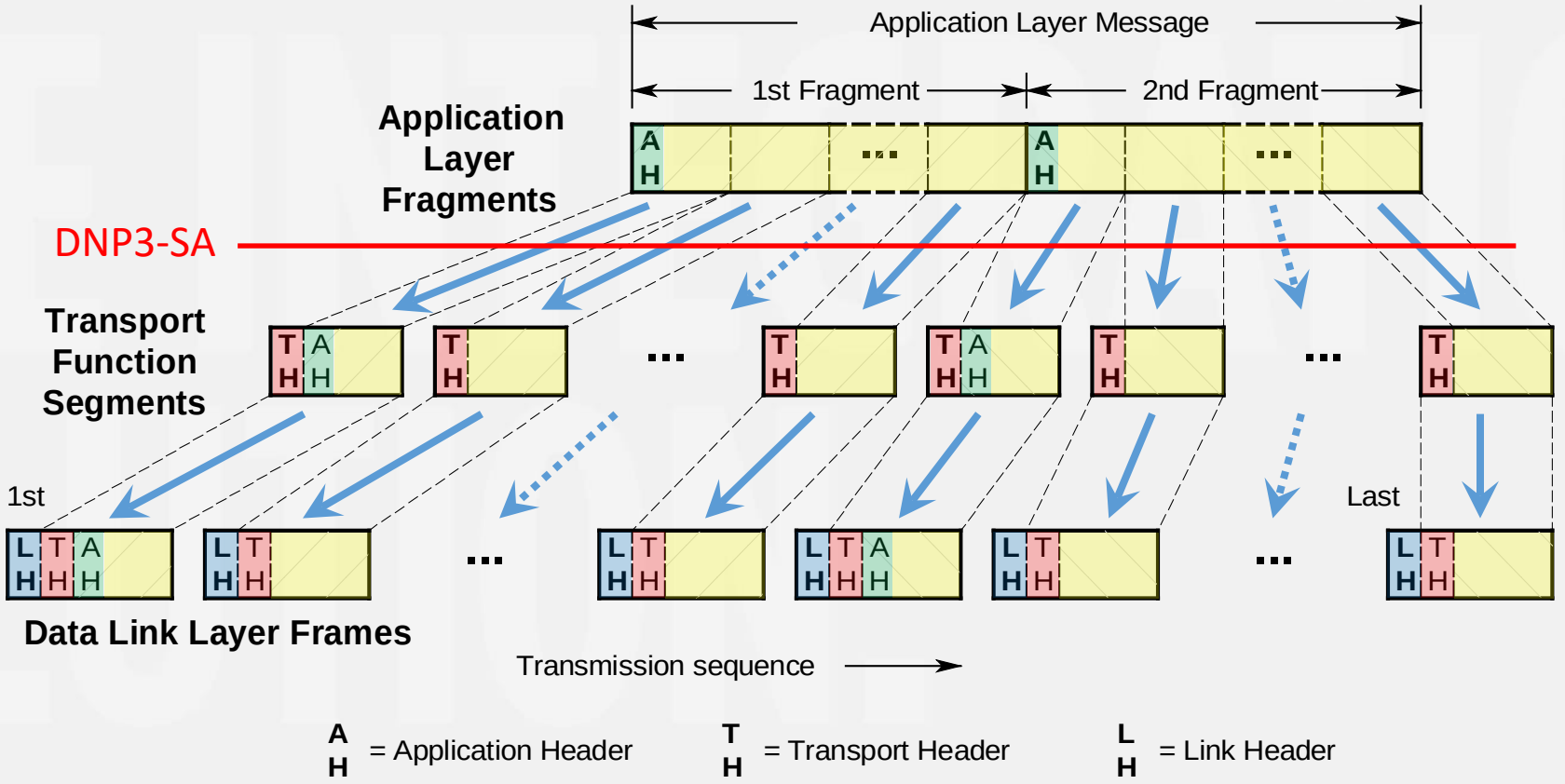
- Physical
  - Media and network interfaces
- Data Link
  - Handles link control, frame checks, addressing
- Transport (function or pseudo-layer)
  - Assembles application message fragments
- Application Layer
  - Defines DNP data objects and services



DNP3 Layer Terminology

- Data Link FRAME
  - A complete data link message
- Transport SEGMENT
  - A Data Link Frame with Transport Header
  - Between DNP3 Application Layer and Data Link Layer
- Security (starting from SAv6): SPDU
- Application FRAGMENT
  - A complete, parseable collection of Segments
- Application MESSAGE
  - A complete message (one or multiple Fragments)

DNP3 Message Components



DNP3 Link Layer Usage

- For almost all applications:
  - Only Unconfirmed User Data Service is used
    - No need for any secondary messages
    - No need to perform Reset Link States command
    - Traffic is minimized
- Only use data link confirmation if required for flow control
  - Usually only for devices that are unable to buffer a complete Application Fragment

DNP3 Application Confirmation

- When reporting events, outstations request application confirm
  - When the master confirms receipt of data, the reported events are cleared form the event buffer
    - If not confirmed, the data remains buffered and is reported in a subsequent response
- When reporting a non-final fragment, outstations request app conf
  - Receipt of the confirm indicates to the outstation that it is to transmit the next fragment
  - The final fragment will request confirm if it contains events

DNP3 Command Summary

- Data are collected by READ commands
- Data can also be reported in Unsolicited messages
- Output objects can be read
  - Not usually required by all systems
- Time can be written
- Internal Indication “Device Restart” flag is cleared by writing it to zero
- Outputs are NOT issued by Write commands

DNP3 Subset Levels

- Subset Levels provide a way for DNP3 to identify commonly used sets of objects and functions
- Subset Level 1 permits Class polls, commands
- Subset Level 2 permits Data Type polls and supports frozen counters
- Subset Level 3 permits individual object polling and adds some advanced features
- Subset Level 4 includes all basic data types

Normal DNP3 Operation uses Subset Level 1 functions

DNP3 Output Commands

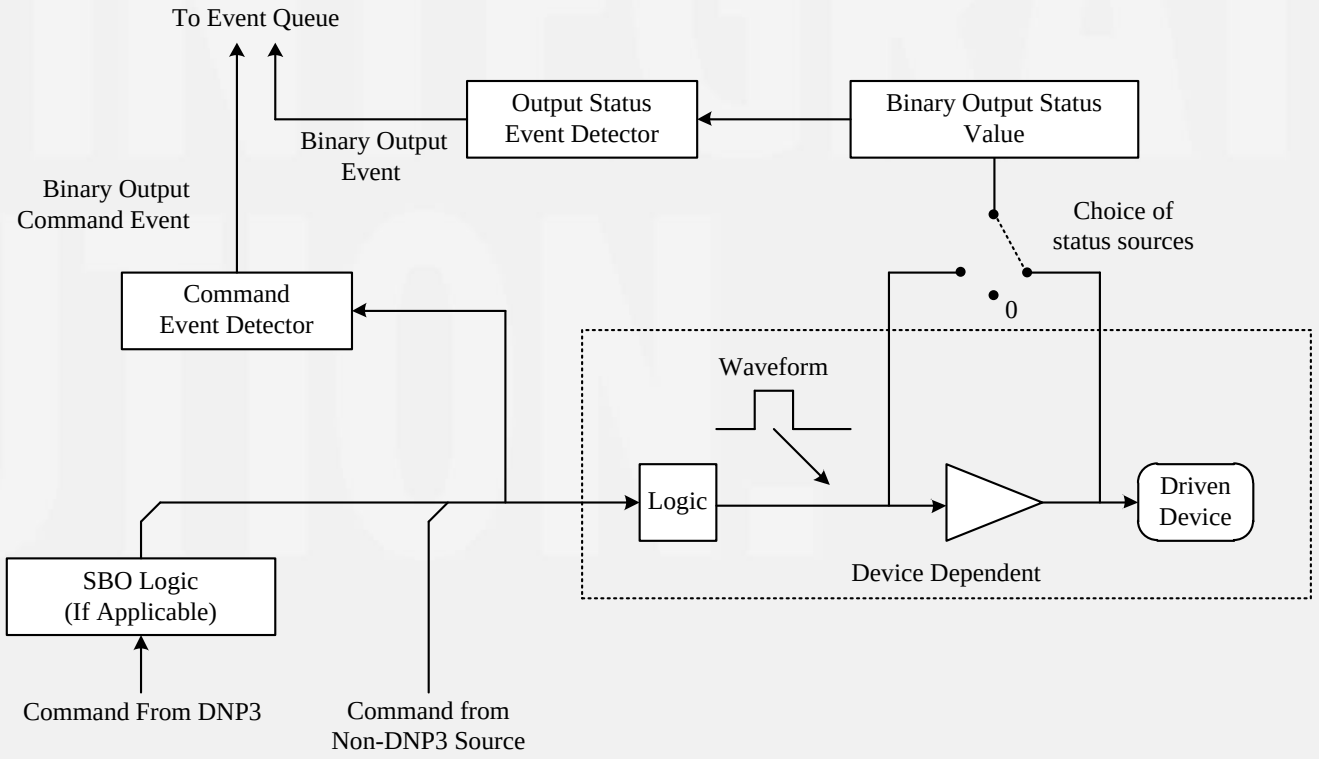
- DNP3 Supports direct execute or Select-Before-Operate (1-pass and 2-pass) commands on both binary outputs and analog outputs
- Binary outputs are controlled through the CROB (Object Group 12, Variation 1)
- Analog outputs are controlled through the analog output block (Object Group 41)
- It is permissible (but unusual) to issue multiple control commands in one message

DNP3 Binary Outputs

- The CROB can accept many parameters
- The basic implementation permits:
  - Trip/Close
  - Latch On/Latch Off
  - Pulsed contact closure
- Paired commands may be issued to one index or to a pair of indices
- The master is required to be configurable to match the outstation's requirements

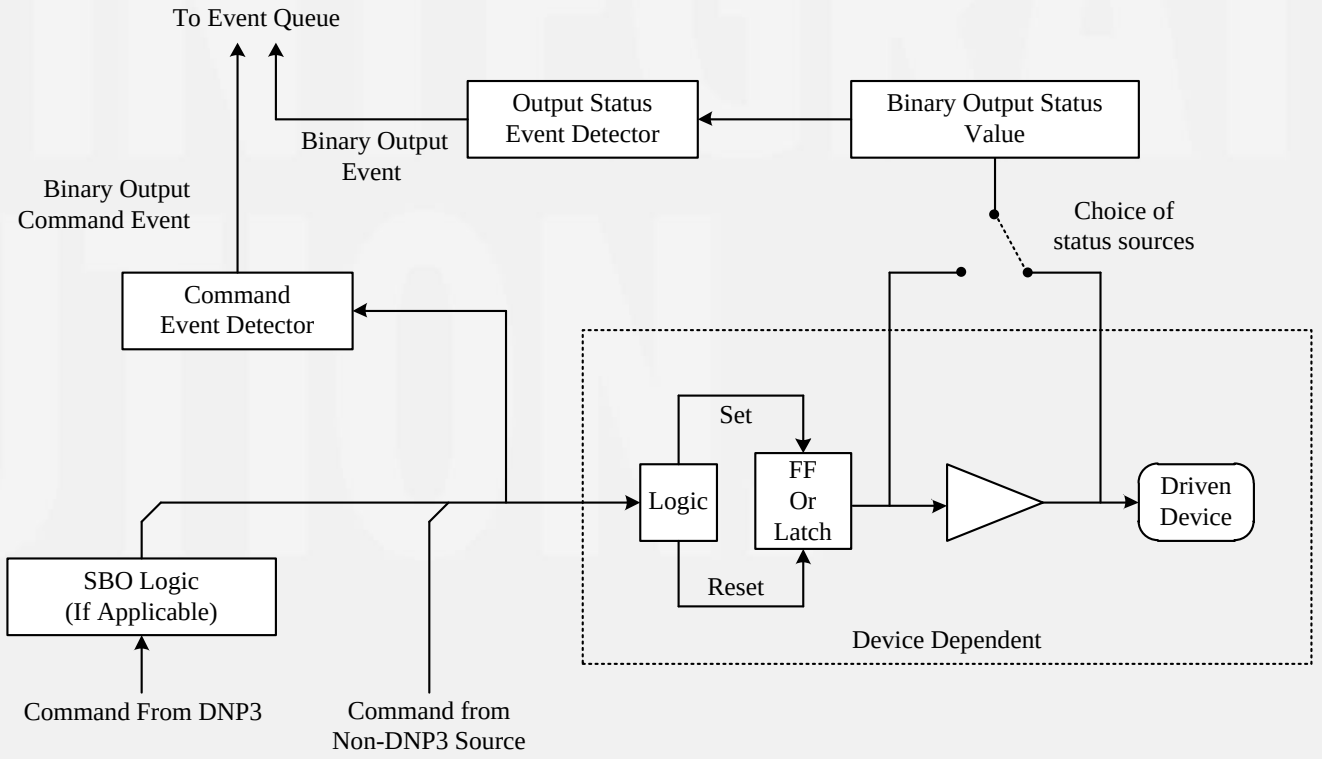
Binary Output Models

- Activation model
  - Control commands initiate an action



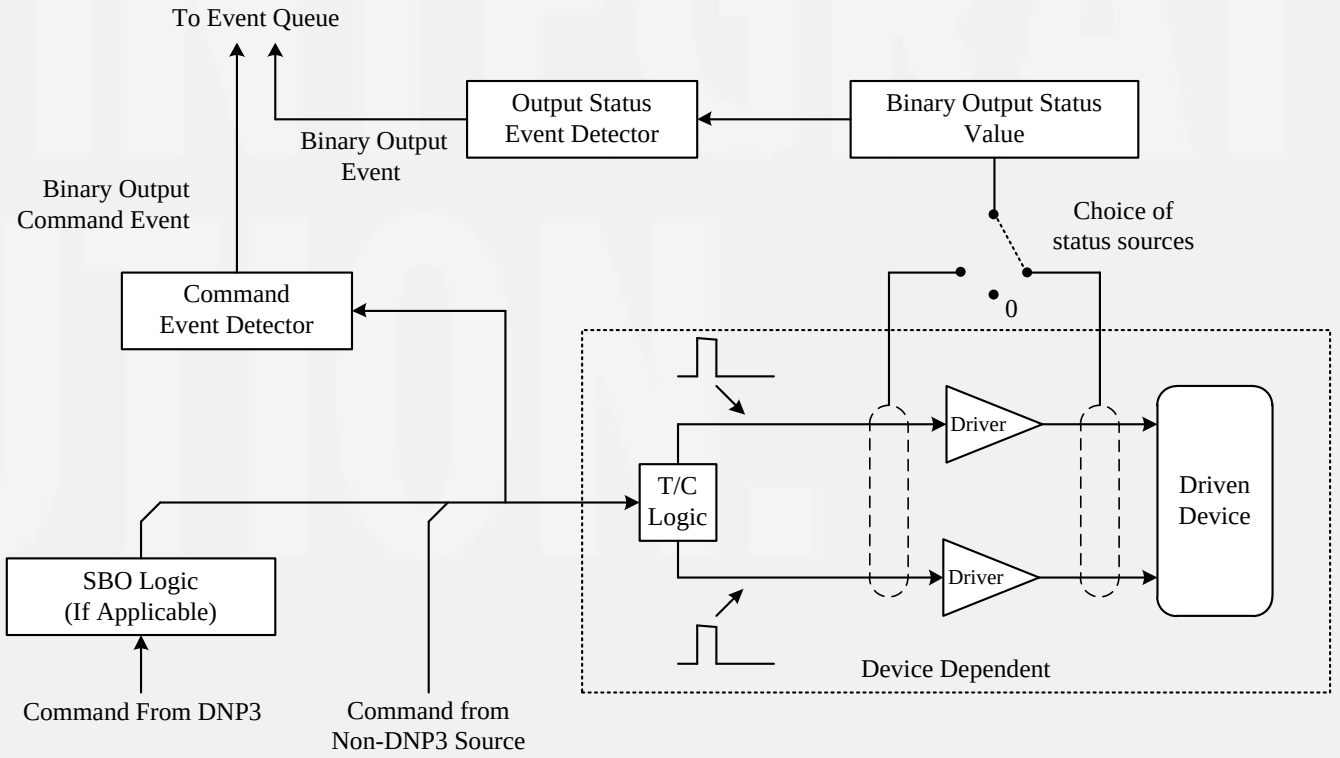
Binary Output Models

- Complementary Latch model
  - Control commands operate to two states



Binary Output Models

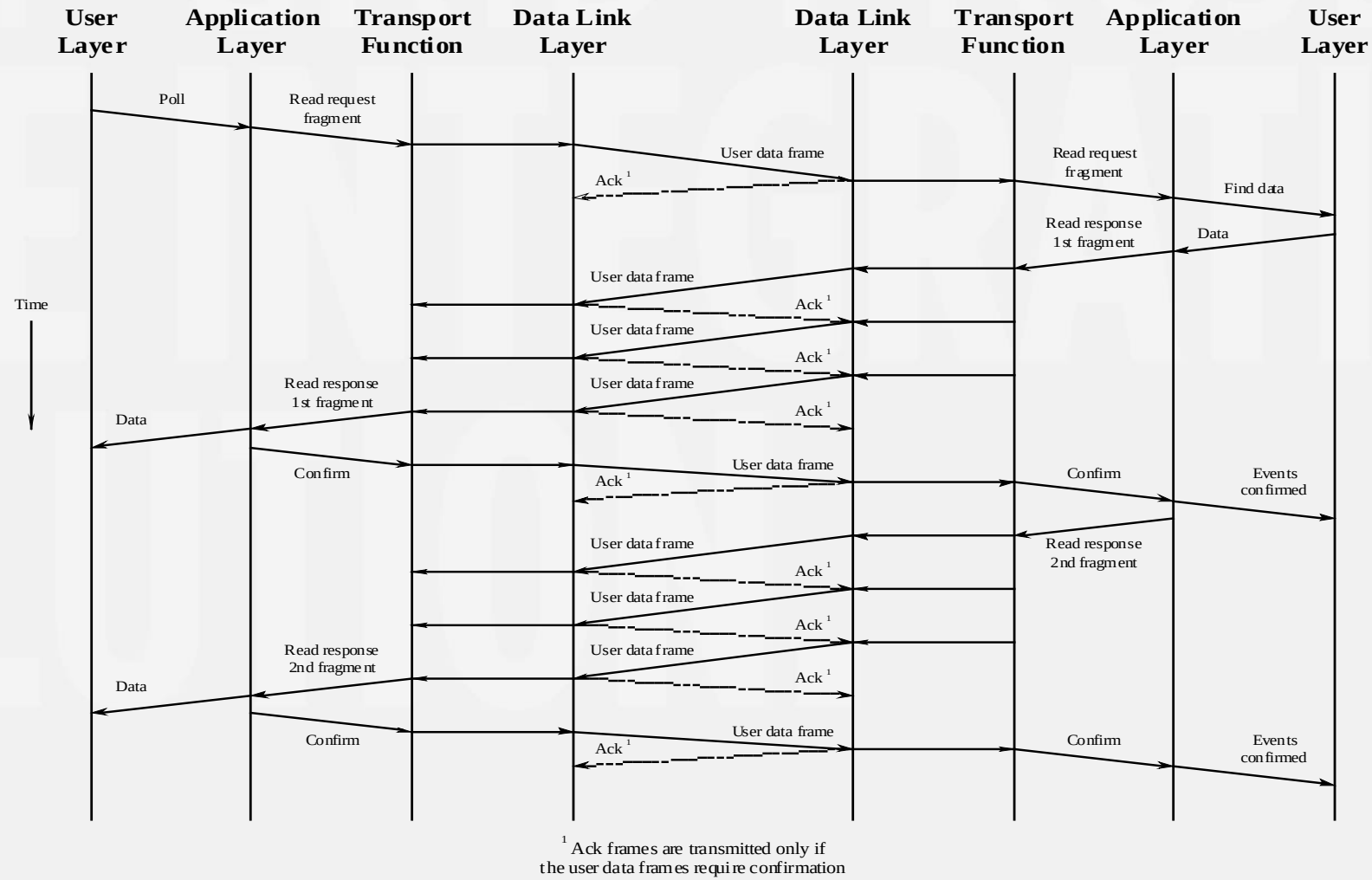
- Complementary Two-Output model
  - Control commands operate to two states



DNP3 Unsolicited Reporting

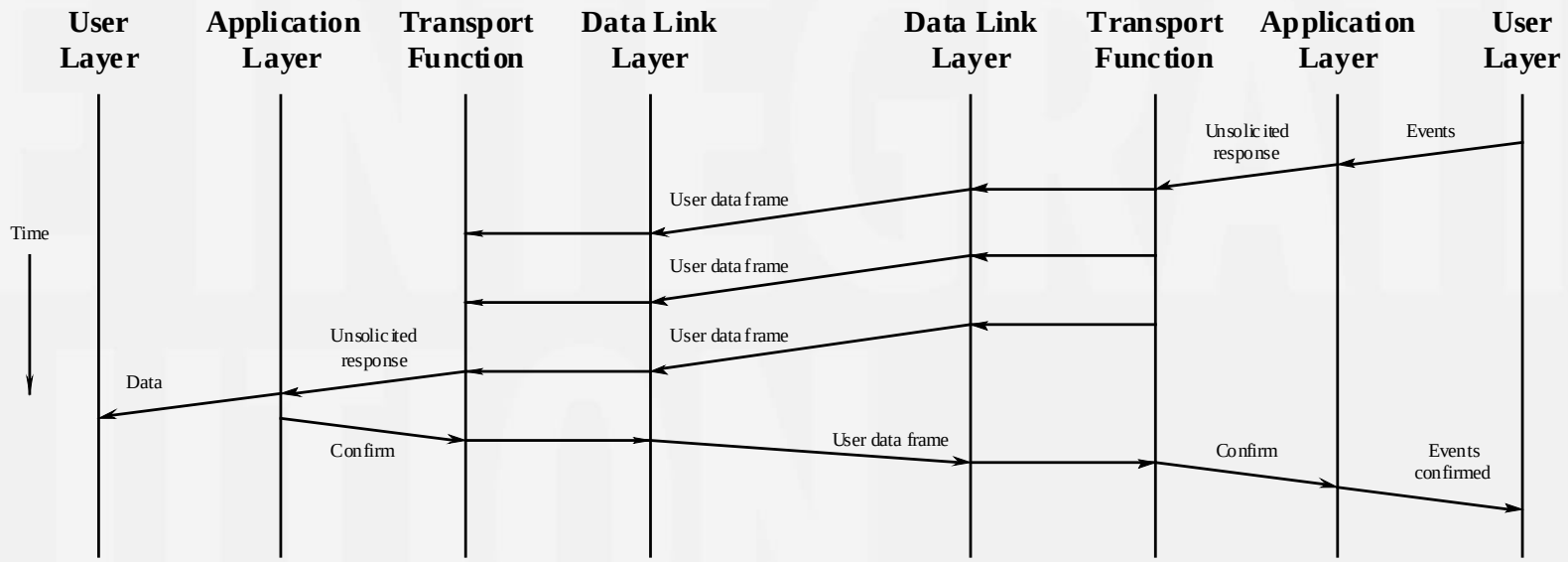
- Outstation is permitted to spontaneously report events (and requests master to issue confirm)
- Startup behavior changed in DNP3-1999:
  - Outstation sends empty “restarted” message
  - Master issues “enable unsolicited” command
  - Prior behavior did not require “enable unsolicited”
- Collision avoidance and backoff
  - Configure sensible backoff times!

DNP3 Poll Transaction Sequence



[1] Ack frames are transmitted only if the user data frames require confirmation

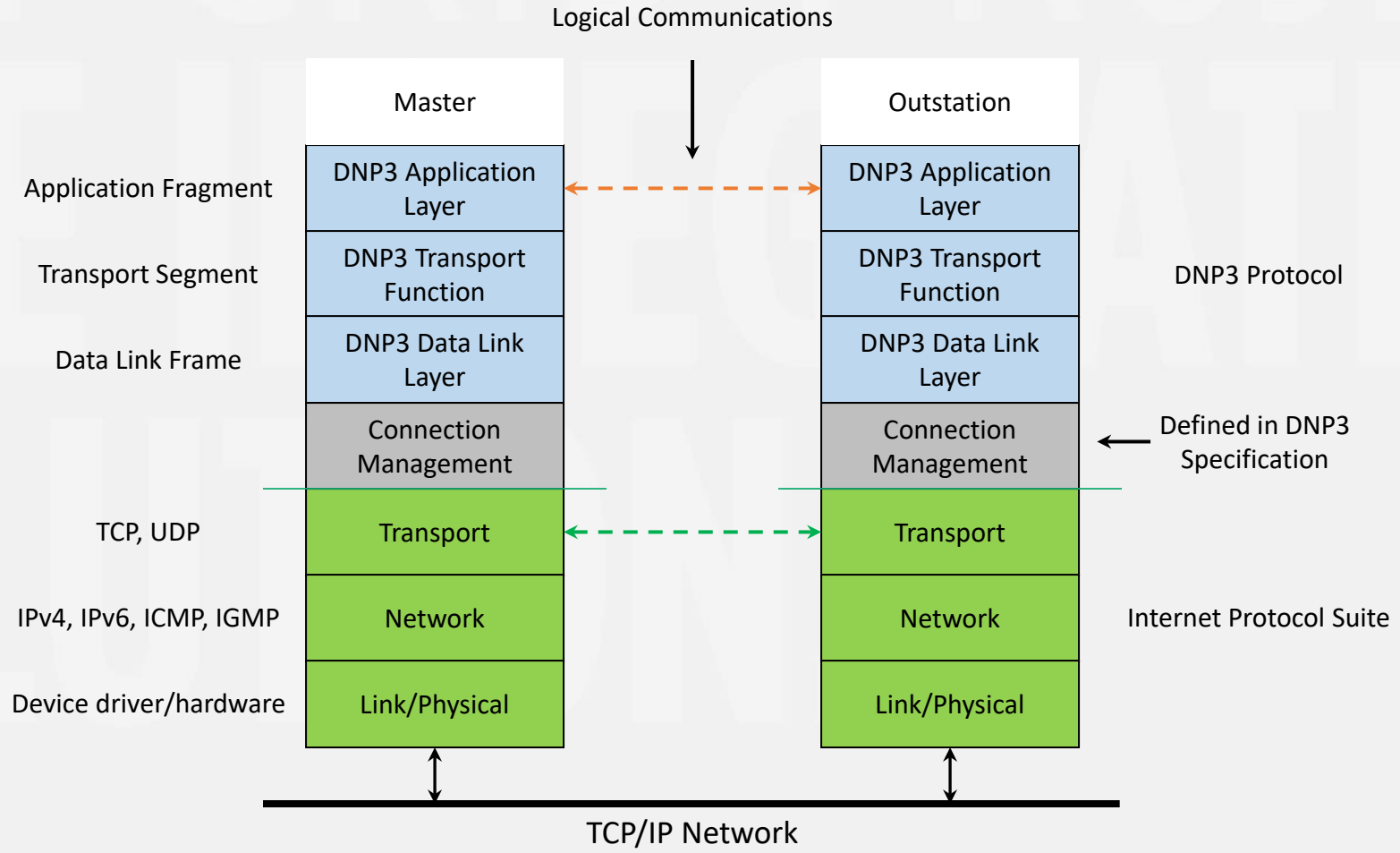
DNP3 Unsolicited “Response”



DNP3 LAN/WAN Usage

- DNP3 on LAN/WAN specification
  - First published December 1998
  - Specifies UDP/IP for single-segment LANs
  - Specifies TCP/IP for WANs and multi-segment LANs
  - Assigned TCP/UDP port number 20000
  - Adds time sync function for single-segment LANs
- Encapsulates “serial” DNP3 in an IP packet
- Adds 56-byte packet overhead in TCP/IP

DNP3 Operation over IP



DNP3 The Easy Way

- At startup, clear the Device Restart flag & Issue a combined Class 1, 2, 3 & 0 (integrity) poll
- Periodically issue a combined Class 1, 2, 3 poll (or individually at different rates)
- When the device requests time synch, issue a write time request
- Messages containing events request confirmation

Lesser-known features

IEEE 1815 (DNP3)

- DNP3 is actively managed by the DNP Users Group
- DNP Technical Committee and IEEE Power & Energy Society combine to work on IEEE 1815
- DNP TC announces proposed revisions through Technical Bulletins
  - Technical Bulletins and other updates are merged into revisions of IEEE 1815
- Application Notes published to address specific applications
- Next edition of IEEE 1815 due 2021/2022

DNP3 Engineering

- DNP3-XML Device Profile published in 2006
  - Defines capabilities
  - Can optionally describe device configuration
    - Import configuration into other devices
      - Auto-configure master connected to fixed-function IED
      - Halve the configuration effort for mapable devices
  - Part of IEEE 1815.1 configuration automation

Cybersecurity

- DNP3 Secure Authentication (DNP3-SA)
  - First published (Version 1) February 2007
    - Pre-shared keys
  - SAv2 included in IEEE 1815-2010
  - Updated and extended
    - SAv5 released in IEEE 1815-2012
    - Added remote key change
  - Provides cryptographically-strong authentication of DNP3 devices and verification of message integrity
  - Adopted as a required functionality in UK Water Industry

IEEE 1815.1: Mapping DNP3 ↔ IEC 61850

- Published December 2016
  - May be adopted as IEC 61850-80-2
- Purpose
  - To support the adoption of IEC 61850 substation automation into systems that use DNP3 for SCADA
  - To allow integration of DNP3 IEDs into IEC 61850 Substation Automation
  - The mapping is to be automatic as far as possible
- Builds on IEC 61850 SCL and DNP3-XML

IEEE 1815.1 Use Cases

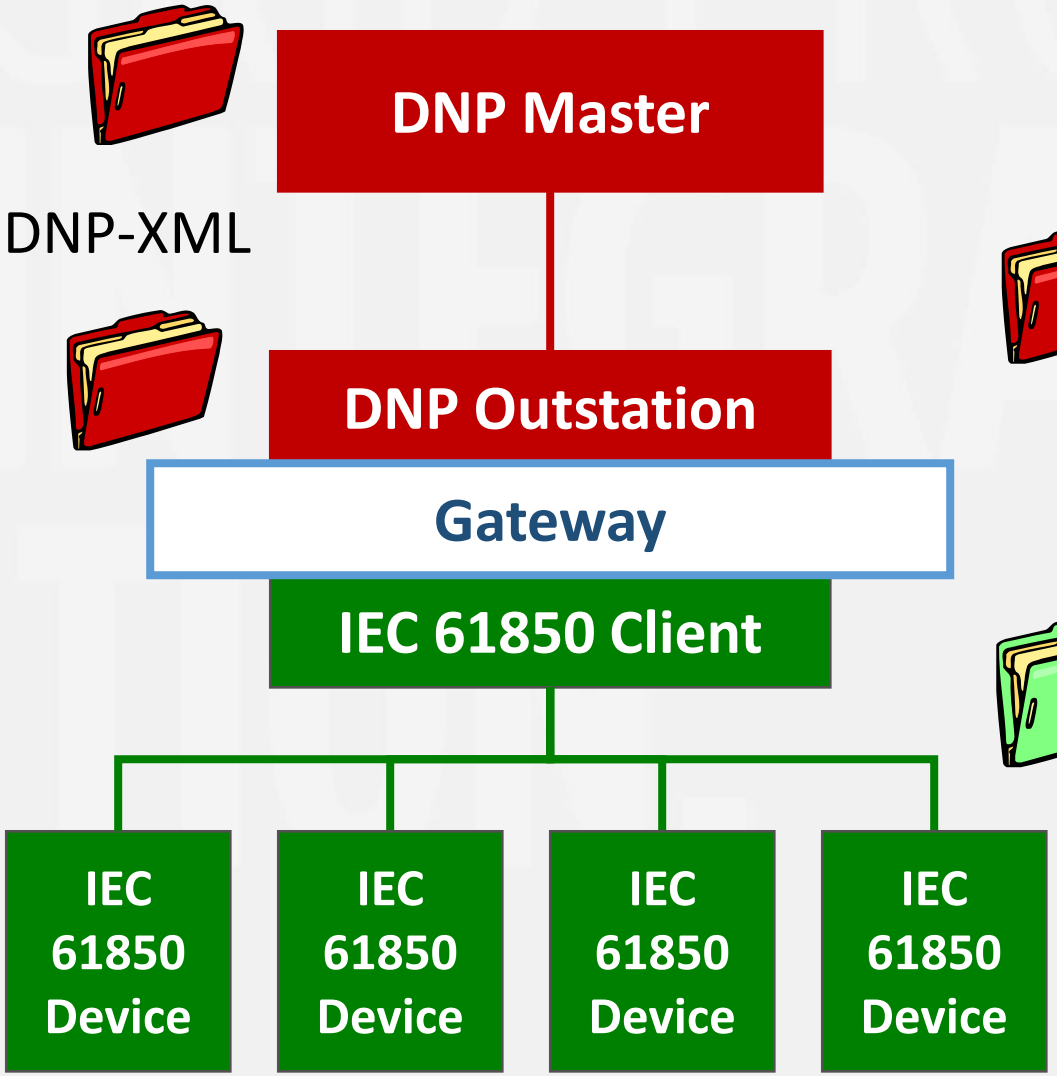
- Two basic use cases:
  - (a) Mapping from IEC 61850 to DNP3
  - (b) Mapping from DNP3 to IEC 61850
- Use case (a) sub-cases
  - (a1) Greenfield:
    - Free data selection
  - (a2) Retrofit:
    - The DNP3 point list is already defined

IEEE 1815.1

INPUT
Capabilities Files

DNP-XML

IEC 61850 ICDs

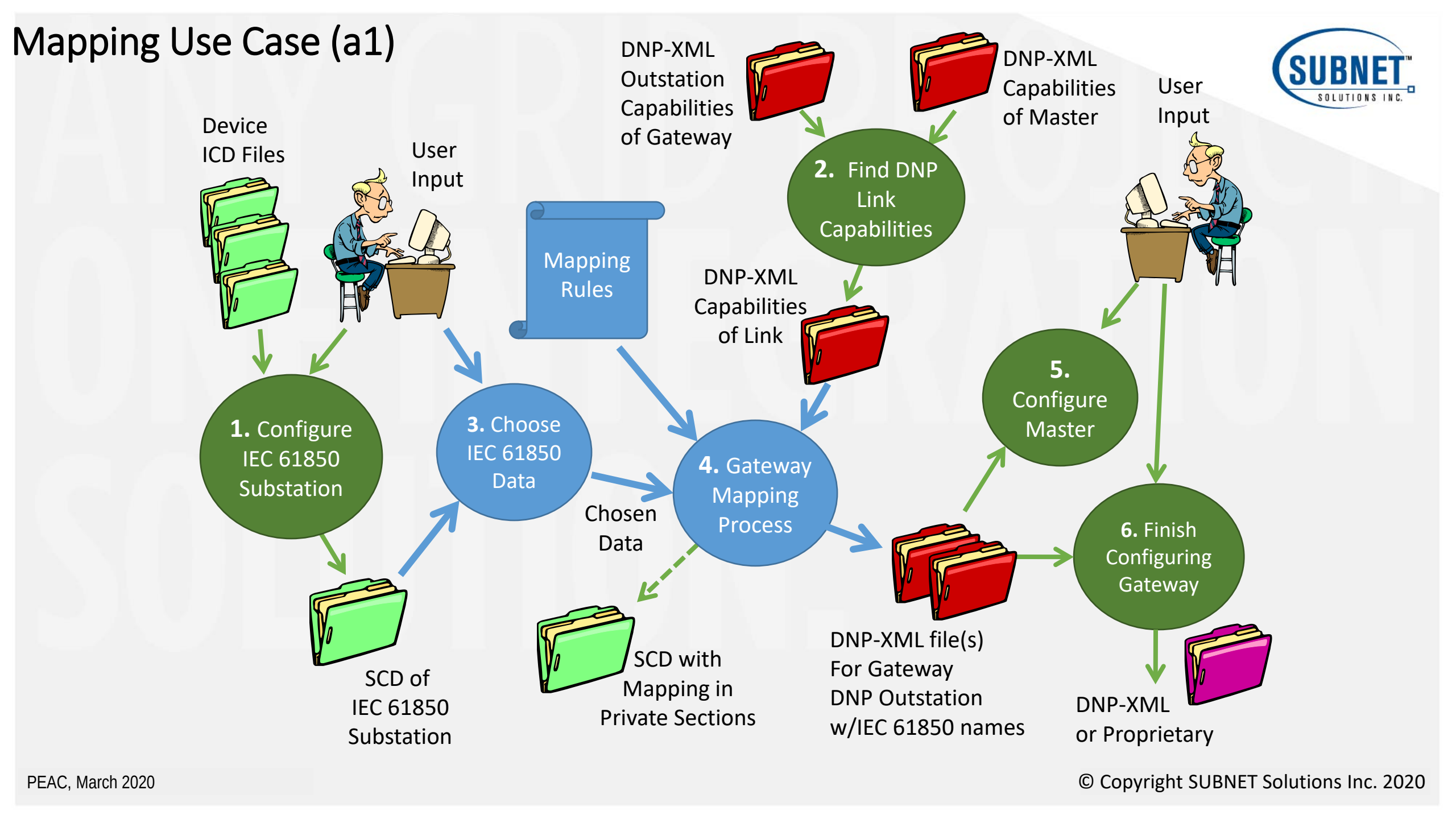


OUTPUT
System Files

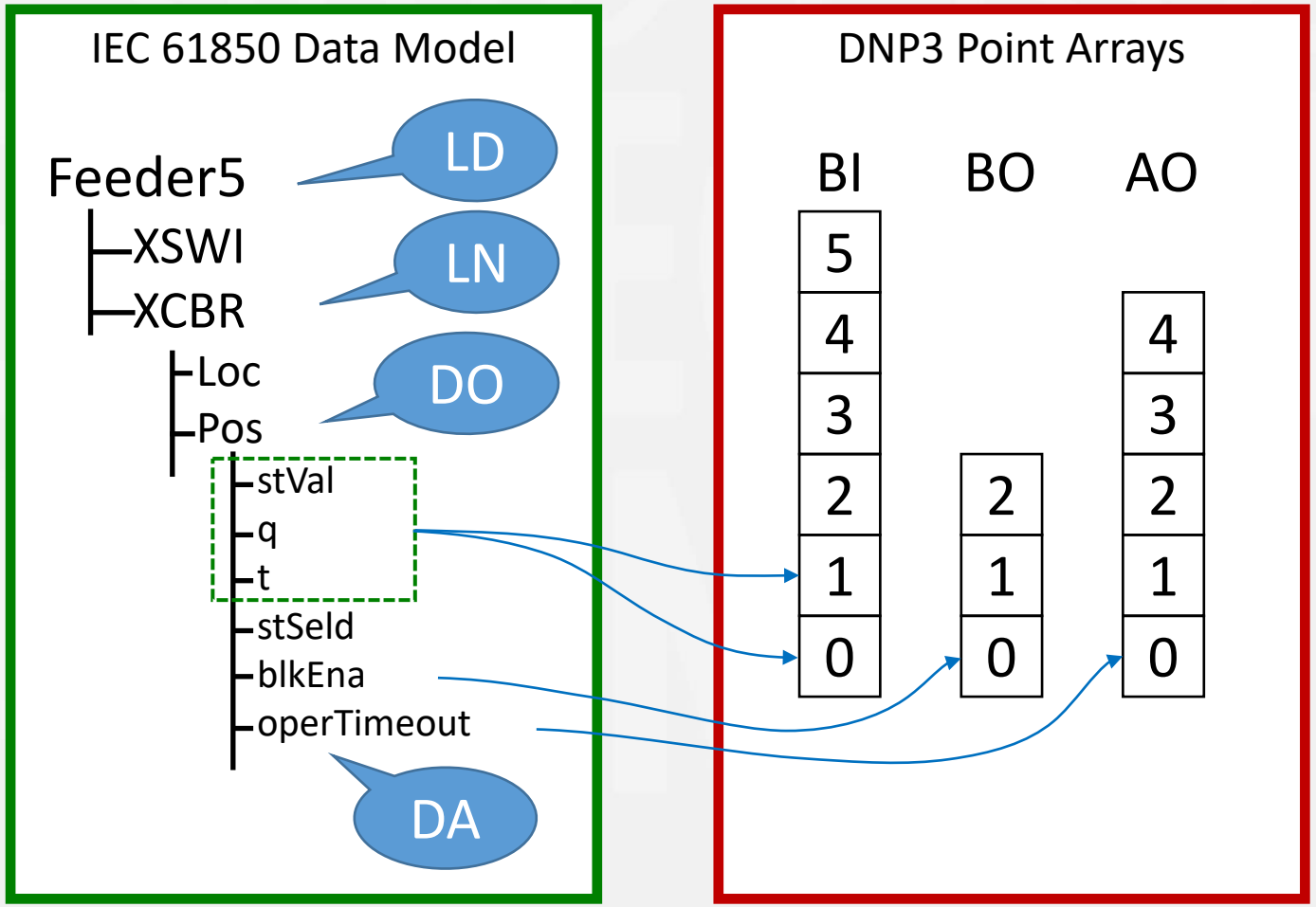
DNP XML with IEC 61850 names

IEC 61850 SCD with private DNP info

Mapping Use Case (a1)



Attribute to data point mapping



DNP3 IED Test Procedure

- Conformance test procedures for DNP3 first published 1999
  - Separate test documents for Subset Levels 1 & 2
  - Devices tested for conformance to a single Subset Level
- Significantly improved interoperability
- Many devices support functions beyond the basic subset definitions

DNP3 Conformance Test Procedure

- A new verification of DNP3 Conformance Test Results has been implemented
- Requires review & validation of test results prior to listing a device as being conformance tested
  - More rigorous than previous procedure
- Many previously-listed conformant devices no longer listed
  - Manufacturers unable to provide satisfactory test result documentation
- Depends on utilities specifying tested devices

DER Communication

DER Communication

- DNP3 Application Note AN2018-001
- Collaborative effort between EPRI, Sunspec, MESA and DNP Users Group
  - Defines a standard mapping for management of Distributed Energy Resources (Solar, battery, wind, electric vehicles) using DNP3 mapping of IEC 60870-7-420 DER data models
- Implements IEEE 1547-2018 functionality requirements
- Work has commenced to ratify this as IEEE Standard 1815.2

Current developments

DNP3 Master Station Test Procedures

- Testing outstations is traditionally straightforward: When sent a stimulus message, they respond to that stimulus
- Testing masters is traditionally more difficult: They do whatever they do in whatever way they do it and this might or might or might not be triggered on demand
- Previous attempts to create tests for DNP3 masters ran into issues of deciding what a master “should” do and how to verify that it does
- The new process checks for the master to perform a set of functions that it claims to implement

DNP3 Master Station Test Procedures

- There is a three-part definition process for the tests
  - A list of functions available for testing
    - The master vendor indicates which of these functions the master implements, and these are then checked
    - Already published on www.dnp.org
  - An outline of how that function is to be verified
    - Due for publication mid-2020
  - The specific test steps that must be implemented
    - In development, due late 2020 / early 2021

MSTP Part 1

General area			Master station requests		Always	Opt	Never
Data Link and General			Send messages with Data Link Confirm				
			Supports DNP3 serial				
			Supports DNP3 LAN/WAN (UDP, TCP)	General			
				UDP listening			
				TCP dual end point			
Poll	All Data	Class Data	Only class 0		2		
			Classes 1, 2, 3, and 0				
			Class 1, 2, and/or 3				2
	Binary	Static data	Variation 0	All qualifier (06)			
				Start/stop Qualifier (00,01)			
			Explicit variation				
		Event data	Variation 0				
			Explicit variation		3		
			Processes time stamps in messages				
	Counter	Static data	Variation 0	All qualifier (06)			
				Start/stop qualifier (00,01)			
			Explicit variation				
		Event data	Variation 0		4		
			Explicit variation 1 or 2		4		
	Frozen Counter	Static data	Variation 0				
			Explicit variation without time				
			Explicit variation with time				
		Event data	Variation 0				
			Explicit variation without time				

Not Level 1, 2+ OK

Not Level 1 or 2, 3+ OK

Not Level 1, 2 or 3

See numbered note

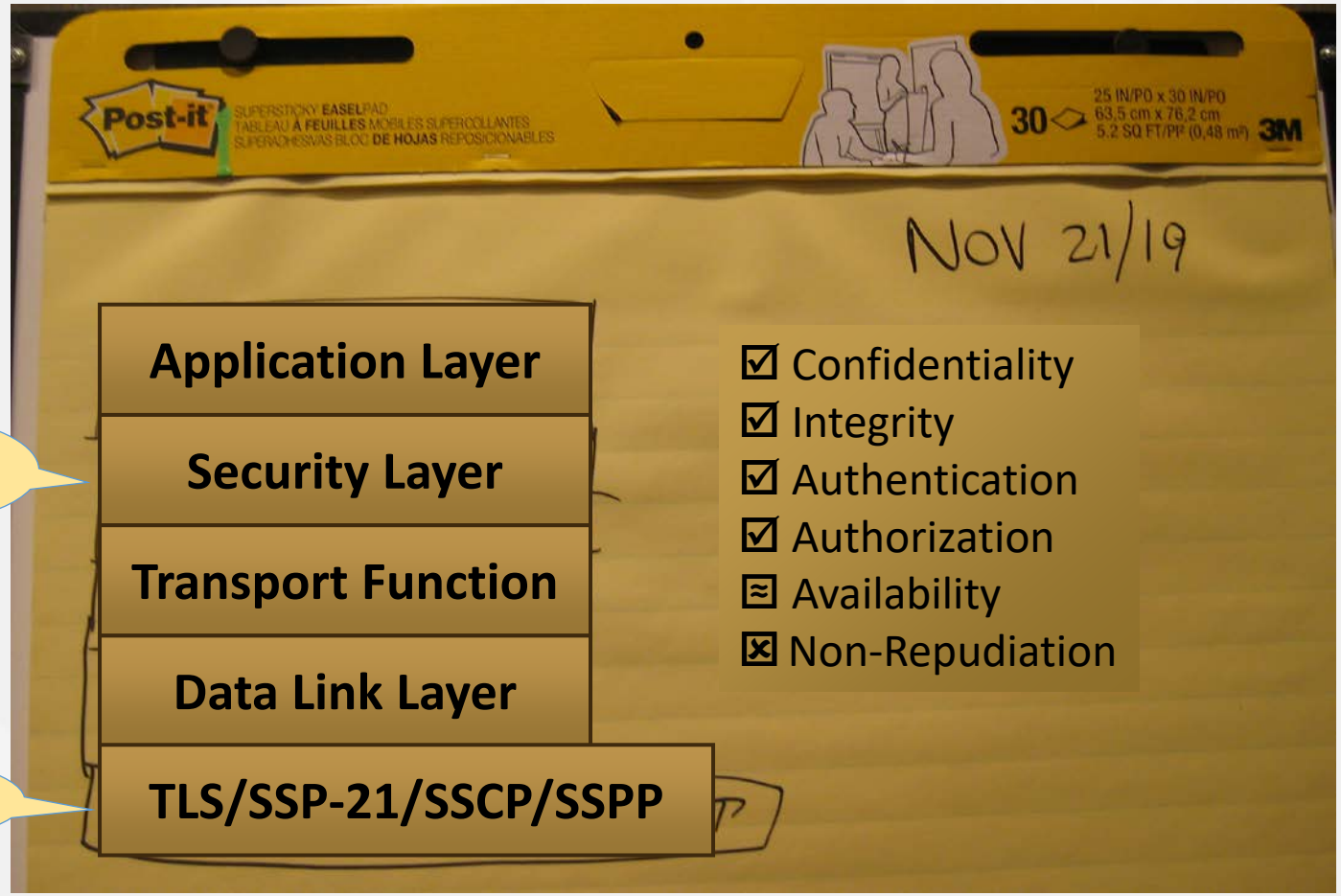
Updated IED Test Procedure

- Verifies conformance to Subset Level 1, 2 or 3
- Tests for correct implementation of functions from higher levels
- Technical Committee review of initial draft commencing Q2 2020

Secure Authentication Revision

- Significant improvements in procedure to manage security credentials
  - New device enrolment process
  - No human handles or knows the cryptographic keys
- Separates security to a layer between transport function and application layer
  - Simplifies specification and design
    - Should lead to “better” and “more secure” implementations
  - Reference implementation available on github
- Still permits mixing secured and non-secured devices on a link
- Adds new option for encryption when data needs to be kept secret

The SAv6 CI(AA)A “Triad”



New

Compatible

Important!!

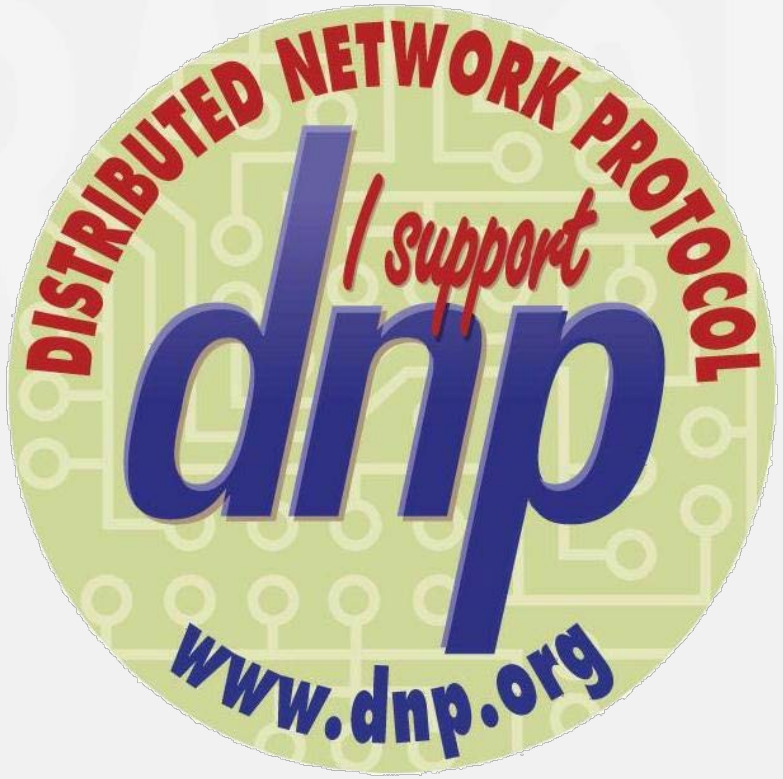
- DNP3-SAv6 is expected to be easier to use than SAv5, BUT:
  - It will probably not be widely available until ~2023
  - If considering DNP3-SA, do not wait for SAv6. Implement SAv5 NOW!
    - For SAv5, follow guidance in technical bulletins for correct implementation
    - Use fixed, pre-shared keys for initial deployment
    - Plan to upgrade to SAv6 when it is available
- Security can be complicated: Get expert advice if you need it

Revision of IEEE 1815

- A major review of IEEE 1815-2012
- Incorporates all Technical Bulletins since 2012
- Introduces clarifications identified in association with development of new master test procedures and Subset Level 3 IEC test procedures
- Clarifies operation of devices that have no clock
- Clarifies / simplifies definition of various parts of the specification
- Incorporates DNP3-SAv6
- Anticipated publication late 2021 / early 2022

Summary

- DNP3 is still actively being enhanced to support utility industry goals
- DNP3 documentation is available free to DNP3 Users Group members
  - Anyone implementing or using DNP3 should be a member!
- More information at www.dnp.org



감사합니다

Danke

谢谢

Gracias

Merci

Thank You

ありがとう

Спасибо

Obrigado