TOPICS OF THE COURSE:

GETTING FAMILIAR WITH SCADA & METERING SYSTEMS PROTOCOLS

NEDA Industries Cooperation

Designed & Presented By Pouya Ebadollahy

Revision #6

1. **Resources in the Course CD**

1.1. E-Books

1.1.1. 5 Volumes, 3875 Pages

1.1.1.1. TCP/IP Illustrated (Richard Stevens)

1.1.1.2. Unix Network Programming (Richard Stevens)

1.1.1.3. Practical Modern SCADA Protocols: DNP3, 60870-5

1.2. Standards

1.2.1. 40 Volumes, 3308 Pages

1.2.1.1. LAST and Full Version of DLMS Color Books (September 2011)

1.2.1.2. IEC 62056 (Including HDLC)

1.2.1.3. IEC 61850

1.2.1.4. Modbus

1.3. Articles

1.3.1. 25 Articles, 996 Pages

1.4. Conference Papers (IEEE, Cigre, …)

1.4.1. 18 Papers, 193 Pages

1.5. Case Studies

1.5.1. 11 items, 257 Pages

1.5.1.1. Actaris ACE6000 COSEM Implementation

1.6. Training Course Material

1.6.1. 23 items, 915 Pages

1.6.1.1. DLMS/COSEM training course schedule and material by Kalkitech

1.6.1.2. IEC61850 Tutorial By Klaus-Peter Brand (Editor of 61850)

1.7. Software Tools

1.7.1. Serial Port Sniffing Tool for Reverse Engineering

1.7.2. Modbus Poll v3.6 (Full Version for Windows + Cracker)

1.7.3. Modscan32 (Limited Time Edition)

1.7.4. DNP_Config

1.8. Training Course Materials by Subject

1.8.1. TCP/IP: 3763 Pages

1.8.2. DLMS/COSEM: 2240 Pages

1.8.3. IEC 61850: 1986 Pages

1.8.4. IEC60870-5: 504 Pages

1.8.5. Modbus: 484 Pages

1.8.6. DNP3: 452 Pages

1.8.7. Misc.: 144 Pages (RS485, Comparison and …)

2. What will be Covered in This Course

2.1. Pre-requirements of the course and for who this course is

2.2. ABC's of Protocols

2.3. Comparing Protocols and Their Features

2.4. Modbus as the most popular protocol in industry (with all details)

2.5. TCP/IP (Since SCADA over IP and Metering over IP are popular, T104)

2.6. TCP/IP Application Layer is not Covered (like HTTP, FTP, SMTP) (these items + network issues are covered in a university course)

2.7. HDLC (as part of DLMS and similar to Hitachi, used in E1 - with full details)

2.8. IEC60870-5-101 & 104 as the most famous SCADA protocols in IR & its comparison with DNP3 with some details

2.9. DLMS/COSEM (& we have a 2 days domestic and 3 days Int. courses for it)

2.10. IEC61850 is not covered (We have a 3 days Int. course for it)

2.11. Course time is limited, so not every detail will be covered but enough resources are provided for further readings

2.12. Task to students: implementing a Modbus terminal to work with IEDs

3. What is a 'Protocol' and Why is it Important?

3.1. Interconnecting of DIGITAL Devices & Communicating Language

3.2. Languages Getting Standard like other stuff (like English Lang.)

3.2.1. IEC61850 accepted both in Europe and US (integration UCA 2.0)

3.2.2. In IGMC grid meters tender and FAHAM, protocol (& Interoperability) was mandatory

3.3. Protocol Implementation is important as a feature of IEDs

3.3.1. More Complete Implementation of Protocols Provide More Functionality

3.3.2. Age of Interoperability: Problem in DCS substations in IGMC

4. Moving Along the Time Line

4.1. Sensor to Panel Systems (Electrical and Analogue Electronic Systems)

4.2. PLC/RTU, HMI and SCADA systems (Simple Protocols or any on relays and other devices, All complexity in RTUs)

4.2.1. What SCADA Means

4.2.1.1. RTU usually doesn't have local processing and used for SCADA

4.2.1.2. PLC is used for automation because of local processing

4.2.1.3. HMI or MMI

4.3. PCs to IEDs (MCU based Intelligent devices, usually multifunctional), Protocols became Object Oriented (High complexity in Firmware)

4.3.1. IED: Relay, Modern Meter, EMS (Energy Management System)

4.3.2. Rise of Industrial Ethernet like: Ethernet/IP, EtherCAT

4.3.3. DLMS/COSEM and IEC61850

4.4. Future: IEC61850 and Intelligent CTs & PTs and … (Within Substation only we will have a data network)

4.4.1. IEC61850 Use Self-Describing XML like Configuration Language Named SCL (Substation Configuration Language)

4.4.1.1. 61850 Causes Minimum Configuration Time in Substations

4.4.2. IEC61850 Let Devices Act as Real PnP

5. Protocols Similarities from Different Perspectives

5.1. Industrial vs. General Protocols (Mission Critical Sys. & Harsh Env.)

5.1.1. CAN-bus vs. FTP

5.2. SCADA vs. Metering Protocols

5.2.1. Differences Between SCADA and Metering Industry Requirements

5.3. Ad-hoc vs. Standard Protocols

5.3.1. MultiDrop Register32 vs. Modbus

5.4. Proprietary vs. Open Protocols

5.4.1. Modbus+ vs. Modbus

5.5. Widely Used vs. Limited Used Protocols

5.5.1. Modbus vs. Indactec 33 (by BBS in Late 80) then ABB

5.6. Partial & Full Implementations Issue

5.6.1. Function Code 3 in Modbus Implementation in MK6E

6. Aspects of Modern Protocols

6.1. Comparing Protocols

6.1.1. Network Compatibility

6.1.1.1. Physical Media Limitation

6.1.1.1.1. DLMS Implementation Over ZigBee

6.1.1.2. Supported Topologies

6.1.2. Efficiency

6.1.2.1. Latency and Throughput

6.1.2.1.1. Jitter (non Linear Latency)

6.1.2.2. More Features Means Less Performance

6.1.3. Reliability

6.1.3.1. Example: Packet Loss in UDP

6.1.4. Expandability

6.1.4.1. DNP3 Can Handle Networks with 65000 Objects

6.1.5. Security

6.1.5.1. Modbus Doesn’t Support Any Security

6.1.5.1.1. Brute-Force & Dictionary attacks for breaking simple passwords

6.1.5.2. DLMS Supports AES128 which is acceptable by US Government for encryption up to confidential level

6.1.6. Acceptability (by Vendors)

6.1.7. Simplicity

6.1.7.1. Why Modus is Still Alive

6.1.8. Consistency

6.1.8.1. Versioning and Different Implementations

6.1.9. Functionality

6.1.9.1. 1ms Time Synchronization Functionality in DNP3

6.1.10. Modernity

6.1.10.1. New Protocols are Object Oriented like 61850 and DLMS

6.2. Example 1: SCADA Over IP, Modbus TCP and T104

7. Protocol from Conceptual Point of View

7.1. Abstract Model of OSI (Open System Interconnection)

7.1.1. Physical Layer (Bit Stream)

7.1.2. Data Link Layer (frames between 2 ends, ensuring of error-free frame transmission/reception)

7.1.2.1. MAC (Medium Access Sub-Layer)

7.1.2.1.1. How Communication Channel should be shared by Multiple Users?

7.1.2.1.1.1. FDM

7.1.2.1.1.2. TDM

7.1.2.1.1.3. ALOHA

7.1.2.1.1.4. Slotted ALOHA

7.1.2.1.1.5. CSMA

7.1.2.1.1.6. CSMA/CD

7.1.3. Network Layer (Packets From This Layer on and Routing)

7.1.4. Transport Layer (Communication Between 2 Ends including Data Splitting, packer re-ordering and broadcasting)

7.1.5. Session Layer (token management, resuming broken transmit)

7.1.6. Presentation Layer (Data Representation Including Encryption)

7.1.7. Application Layer (HTTP, FTP, …)

7.2. Addition of PCI (Protocol Control Information) or Header in Each Layer

7.3. OSI is Abstract; Actual Realizations have 3 or 5 layers

7.4. Connection-Oriented and Connection-less Models

7.4.1. Examples: TCP and UDP

7.5. *What is Not a Protocol*

7.5.1. RS232 & RS485: Standards for Mechanical and Electrical Details

7.5.2. DB9 and DB25 Sockets

7.5.3. RJ45 and RJ11 Sockets

7.5.4. Terminals

7.5.4.1. Spring Loaded

7.5.4.2. Screw type (Phoenix)

7.5.5. Briefing RS232 (Point to Point), CCITT V.24 Standard

7.5.6. Briefing RS485 (Point to Multipoint)

7.5.6.1. Distances up to 1200m, Baud Rates Up to 10 Mbps

7.5.6.2. 4 Wire and 2 Wire Systems: Full and Half Duplex

7.5.6.3. External Powered Ports

7.5.6.4. 31 Devices on a Single Bus

7.5.6.5. UART/USART Port of MCUs and RSxxx Drivers

7.6. Protocol Modem/Converter

7.6.1.1. Cannot cover all features of a protocol

7.6.1.2. Have some compatibility problems

7.6.1.3. Cause performance problems

7.6.1.4. Case Study: RTU560s Gets Signals from DCS Through HDLC, then Change Time Stamp and Send to SCC by DNP3, So Processing Time is Added; Solution. Packet Encapsulation

8. Modbus Protocol

8.1. By Schneider in 1979

8.2. 40% of communications use Modbus (i.e. Widely Used)

8.2.1. Specially in **outside of Power Industry** like Iran Khodro

8.3. Independent of Communication Media

8.4. It is a De-facto Industry Standard (not only for Power Industry)

8.5. Master/Slave configuration: Only Master Initiates Communication (also called **Polled** or Request/Response Protocol)

8.6. Modbus is Application Layer Protocol

8.6.1. We have Modbus over serial line implementation specification which acts as data link layer protocol for Modbus

8.6.2. Ethernet can be used as Data Link layer of Modbus over TCP

8.7. Broadcast Packets

8.8. Modbus is Big-Endian

8.9. RTU (Modbus-B) and

8.9.1. The Entire Devices on a Bus Should Communicate with the Same Transmission Mode

8.9.2. ASCII Mode is Used Only for Special/Training Purposes

8.9.3. Modbus-B default Configuration: 1 Start, 8 Data, Ev. Parity, 1 Stop

8.9.4. Modbus-ASCII default Configuration: 7 Data Bits Instead of 8

8.10. Data Model of Modbus

8.10.1. Input Register (16 bit Read Only)
8.10.2. Holding Register (16 bit Read/Write)
8.10.3. Coil (Single Bit Read/Write)
8.10.4. Discrete Input (Single Bit Read Only)
8.10.5. Disadvantage: Data Type is not Precisely Known

8.11. Modbus Functions
8.11.1. Register Read (4)
8.11.2. Status Read (2)
8.11.3. Preset Single Register (6)
8.11.4. Force Multiple Register (16)
8.11.5. Diagnostic Check and Report or LOOP-Back(8) (Serial Line Only)
8.11.5.1. Sub functions (e.g. Change ASCII Delimiter)
8.11.6. Loop Back Mechanism (I am Alive, You are Alive)
8.11.7. Not every Function is used in Metering
8.11.8. User Defined Function Codes: 65 to 72 and 100 to 110
8.11.9. Reserved Function Code

8.12. Message Format of Modbus-RTU (ADU or Application Data Unit)

8.13. Data Address (Register Address)
8.13.1. 2 Bytes from 1 to 65535

8.14. Response Types
8.14.1. Normal Type With the Same Function Code in Request
8.14.2. Exception Type With (128+ Function Code in Request)

8.15. Only 247 Slaves Can Exist (1 to 247)
8.15.1. Address 0 for broadcast and 247 to 255 is Reserved
8.15.2. There is no Response for Broadcast Messages
8.15.3. Broadcast Messages is Only for Writing

8.16. Time Synchronization: 3 msec Silence Means End of Frame

8.17. Packets with Bad CRCs are Ignored

8.18. Baud Rates 9600 and 19200 Must be Implemented

8.19. 1% Timing Accuracy is Required in Transmission, %2 Should be Accepted in Receiving

8.20. Modbus State Diagrams in master and slave sides

8.21. Modbus TCP Variation Exists (Port #502 TCP)

8.22. Modbus TCP Message Format

9. TCP/IP

9.1. Brief About the Internet

9.1.1. Paul Baran from DOD proposed mesh network in 60^{th}, but AT&T refused this silly Idea since they have based all of their work on Radial networks

9.1.2. Cold war and fear from Soviet Union Caused President Eisenhower to establish ARPA, and they Created ARPANET (Focus on Fault Tolerance) based on Baran's theory in 70^{th}.

9.2. Layers

9.2.1. Physical and Data Link layer due to Media

9.2.1.1. E.g. Ethernet (IEEE 802.3x) by Xerox

9.2.1.2. There are lots of wired and wireless data link protocols which TCP/IP is implemented on them

9.2.2. Internet Layer (or IP Layer) as Network Layer

9.2.3. Transport Layer (TCP, UDP or RTP)

9.2.4. Application Layer (SMTP, FTP, HTTP, …)

9.3. Networks Type Terminology

9.3.1. LAN (Local Area Network)

9.3.2. WAN (Wide Area Network)

9.3.3. Absolute term: MAN (Middle Area Network)

9.3.4. HAN(Home Area Network)

9.3.5. PAN (Personal Area Network)

9.3.6. WPAN (Wireless PAN)

9.4. IP Packet Format as Illustrated in Appendix 8 (RFC 791)

9.4.1. Internet is Big Endian, so Little Endian Machines Like Intel Processors Should Have Software Conversion

9.5. Meaning of Tunneling (2 networks with a protocol and an interface or intermediate network in between with another protocol)

9.5.1. E.g. Implementation: One Complete Packet as Payload of another Packet (encapsulation)

9.6. IP Addressing (Network and Host Addresses)

9.6.1. Class A: 0, 7 bits for Network Address, 24 bits for Host Address

9.6.2. Class B: 10, 14 bits for Network Address, 16 bits for Host Address

9.6.3. Class C: 110, 21 bits for Network Address, 8 bits for Host Address

9.7. Multicast, Broadcast and meaning of 0(this, network or host), 127.x.y.z(loop back) and 255(all) in Addresses

9.8. Subnets

9.8.1. 255.255.252.0 or /22 which means subnet mask is 22 bit long

9.9. Now a day we have CIDR (Classless Inter Domain Routing) Which means, we don't have IP classes and a chunk of 2048 IP addresses (or any other size) can be allocated to an organization, e.g. Oxford University starts from 194.24.16.0 and ends to 194.24.31.255 (4096 hosts- 20 bit network address, 12 bit host address)

9.10. Non IP Protocols

9.10.1. ICMP (Internet Control Message Protocol) (RFC 792)

9.10.1.1. Echo Packet, Ping

9.10.2. ARP (Address Resolution Protocol) (RFC 903)

9.10.2.1. Resolving IP Address to 48 bit Ethernet Address and ARP Spoofing

9.10.2.2. ARP Cache

9.10.3. RARP (Reverse ARP)

9.10.3.1. For booting Diskless Stations (Boot from LAN)

9.11. NAT (Network Address Translation) Technique

9.11.1. 192.168.0.0/16 range of reserved addresses

9.11.2. NAT Replaces TCP/UDP port numbers to identify packets of different hosts

9.11.3. Some protocols like H323 have problem with NAT

9.12. Ipv6 Packet Format as Illustrated in Appendix 9

9.12.1. Sample address: 8000:0000:0000:0000:0123:4567:89AB:CDEF

9.12.2. Can be written as: 8000::123:4567:89AB:CDEF

9.13. TCP/UDP Ports or TSAP (Transport Service Access Point) & Reason behind having different ports (for different processes)

9.14. Famous TCP/UDP Ports as in ports.htm/ports.txt file

9.14.1. Iana.org site

9.15. UDP Header: 16bit Source Port, 16bit Destination Port, 16bit Total Packet Length and 16 bit Checksum. If Checksum is not computed it is stored as 0, real computed 0 checksum is stored as 0xFFFF (RFC 768)

9.16. TCP Header Format as Illustrated in Appendix 10 (RFC 793)

9.17. Socket is defined as “a Port and an IP Address”

9.18. Ethernet Frame Format

10. HDLC

10.1. Stands for High Level Data Link Control

10.2. Data Link Layer Protocol

10.3. Based on IBM's SDLC

10.4. Now as ISO 13239, ADCCP by ANSI and IEC62056-46

10.5. Grand Father of Ethernet

10.6. Bit Oriented

10.7. Can be Used Both on Synchronous and Asynchronous Links

10.8. HDLC Used in E1 (Slightly Changed Version) and DLMS/COSEM

10.9. HDLC is Little-Endian

10.10. Windows Size: in DLMS something between 1 and 7. It means after this number of packets, an acknowledge packet will be sent.

10.11. Modes:

10.11.1. NRM (Normal Response Mode): Only Master can Initiate Transactions (DLMS Uses This Mode Only)

10.11.2. ABM (Asynchronous Balanced Mode): Equal Situation for the Entire Devices *[More Commonly Used]*

10.12. Frame Types:

10.12.1. Unnumbered Frames without Sequence Numbers, Used for Setting up the Connection & Its Type (NRM, ABM)

10.12.2. Informative Frames

10.12.3. Supervisory Frames Including Acknowledgement, Error & Flow Control

10.13. Description of Frame Format

11. Brief about IEC60870-5-101 & 104 (T101, T104)

11.1. IEC TC57 started working on IEC 870 (Tele-control equipment and systems) in late 80s. It is dedicated to be used in power industry

11.2. Part 5 of standard is "Transmission Protocols" which is published between 1990 to 1995

11.3. Sub-part 1 of 870-5 is Frame Formats: FT1.1, FT1.2, FT2 and FT3

11.4. DNP3 is American version of 60870-5 and developed in 1990 by Harris. DNP3 (Distributed Network Protocol) Users Group formed in 1993

11.5. DNP3 uses FT3 but 101 which is published in 1995 uses FT1.2

11.5.1. Hamming Distance: This is equal to the minimum number of single bit errors that are required to allow an incorrect message to be mistakenly accepted as a good message

11.5.2. DNP3 has a CRC for each 16 bytes, T101 has checksum for each 255 bytes

11.6. DNP3 is also used in oil industry, water industry and … (despite 870-5)

11.7. DNP3 & T101: open standards & make Interoperability easier

11.8. Both based on 3 Layer Version of OSI: Enhanced Performance Architecture (EPA) Model: Physical, Data Link and Application Layer

11.9. 60870-5 is open and reliable protocol widely accepted by SCADA device manufacturers. In Iran it is widely used.

11.10. Short hand of IEC60870-5-x is Tx; T stands for tele-control

11.11. T101 Title: Companion standard for basic tele-control tasks

11.12. Detail Look at Layers of T101 and its relation with 60870-5-X Standards

11.12.1. Physical Layer is ITU-T; i.e. RS232, RS485 (Low Speed Serial)

11.12.2. In data link layer, T101 uses FT1.2 frame format

11.12.2.1. Fixed length version only used for acknowledge & data link control command

11.12.2.2. Variable length version is used for carrying user data

11.12.2.3. 0xE5 frame is used when secondary wants to say "no data is available" (in response to a request)

11.12.2.4. Length field is 1 byte and mentioned 2 times (should be equal)

11.12.2.5. Address can be 1 or 2 bytes (in each system, it is fixed)

11.12.2.5.1. If frame is sent by primary, it contains destination address

11.12.2.5.2. If frame is sent by secondary, it contains its own address

11.12.2.6. T101 frames only contain destination address, DNP3 frames contain both source and destination addresses

11.12.2.7. Description of Control Field

11.12.2.7.1. Class 1 data has higher priority

11.12.2.7.2. Class 2 data has lower priority

11.12.2.7.3. Services of Data Link Layer due to Function Code in Control Field

11.12.2.7.3.1. Send/No Reply: a frame is transmitted and an idle time of transmission of 33 bits should be elapsed

11.12.2.7.3.2. Send/Confirm: usually for commands

11.12.2.7.3.3. Request/Response: for reading user data

11.12.2.8. T101 supports point-to-point and multi-drop topologies

11.12.2.9. T101 supports unbalanced communication (only master can initiate). Master is called primary as well in 870-5-2

11.12.2.10. T101 supports balanced communication (unsolicited response) only in point-to-point communication

11.12.2.11. DNP3 only supports balanced communication

11.12.2.12. Different ports of an IED may act as primary and secondary

11.12.2.13. In balanced communication, data link layer address byte can be 0 byte length

11.12.3. Application Layer

11.12.3.1. ASDU

11.12.3.1.1. Type Identification Field, range 1..127 is defined

11.12.3.1.2. Variable structure qualifier

11.12.3.1.3. Cause of transmission

11.12.3.1.3.1. Test bit means, command should not be executed, it is only for test purpose

11.12.3.1.3.2. Positive Confirmation means command was executed successfully (monitor direction)

11.12.3.1.3.2.1. Meaning of command and monitor directions

11.12.3.1.4. Address

11.12.3.1.4.1. Data link layer address is different from application layer address (like computer networks)

11.12.3.1.4.2. DNP3 only has data link layer addressing

11.12.3.1.4.3. Having application layer addressing (in addition to data link layer addressing) make the system capable of supporting virtual devices (e.g. meters inside DCU)

11.12.3.1.4.4. In Control direction, address is address of slave device, In monitor direction address is address of slave device too (address of sender)

11.12.3.1.4.5. We have broadcast packets (address 0xFF or 0xFFFF should be included in both data link and application layers); reset and clock synchronization

11.12.3.1.5. Information object address is 1, 2 or 3 bytes length and contain object (data) address (similar to register number)

11.12.3.1.6. Information elements: each type has its own format

11.12.3.1.7. Time Tag has three different formats

11.12.4. User Process Layer (60870-5-5)

11.12.4.1. E.g. Station Initialization procedure (protocol Initialization after power up, what packets will be sent first)

11.12.4.2. Clock Synchronization

11.13. T104 Title: Network Access using Standard Transport Profiles

11.14. DNP3 is used both for local and network communications

11.15. T102 and T103 provides data types and functions for electrical protection systems

12. History of IEC62056 & Briefing DLMS/COSEM

12.1. DLMS User Association (DLMS UA) Formed in 1997 in Geneva

12.2. Standardized as IEC62056 in 2002 by Adding 1107 & 61334 and … *(So DLMS is only a part of 62056)*

12.3. Now, DLMS User Association has 243+ Members in more than 40 Countries and more than 120 Products are Certified

12.4. First Stand for *Distribution Line Message Specification*

12.5. Then for *Device Language Message Specification*

12.6. COSEM Stand for *COmpanion Specification for Energy Metering*

12.7. Around Year 2000, DLMS upgraded to xDLMS

12.8. COSEM is a Data Model, COSEM Objects

12.9. Concept of Class, Object, Attribute and Method

12.10. DLMS/COSEM Can Be Run Over:

12.10.1. HDLC

12.10.2. TCP

12.10.3. PLC (IEC 61334), DLMS is tied to PLC rather than other Infrastructures

12.11. DLMS/COSEM is Mainly Developed for Metering

12.12. DLMS/COSEM in North America & EU

12.12.1. American Equivalent: ANSI C12.19

12.13. Advantages of DLMS/COSEM

12.13.1. Connection Oriented (Disadvantage when Infrastructure is Radio)

12.13.2. Not Only in Electricity Industry but in Gas & Water Industries

12.13.3. COSEM Objects Prevents Unambiguous Interpretation of Data Elements in Metering.

12.13.4. Secure (Encryption + Authentication)

12.13.5. Covers Simplest Devices to the Most Complex Ones.

12.13.6. Open Standard Makes Interpretability Better

12.13.7. Low Overhead and Efficient

12.13.8. Can be Run Over Internet

12.13.9. Selective Access to All Objects (e.g. Partial Load Profile Reading)

12.14. DLMS UA Publishes 4 Books

12.14.1. White Book

12.14.1.1. Glossary of Terms (FREE)

12.14.2. Yellow Book

12.14.2.1. Conformance Test Plans

12.14.2.2. DLMS Conformance Tool Description and How to get Certificate (CTT)

12.14.2.2.1. Can Be Done by Meter Manufacturer

12.14.2.3. DLMS Explorer by Kalkitech

12.14.3. Blue Book

12.14.3.1. IEC62056-61:Interface Classes

12.14.3.2. IEC62056-62:OBIS

12.14.3.2.1. Described in 3. ObjectNaming.pdf in Kalkitech's Training Course Material

12.14.4. Green Book

12.14.4.1. IEC62056-53:COSEM Application Layer

12.14.4.2. IEC62056-47: COSEM Transport Layer for IPv4

12.14.4.3. IEC62056-46: HDLC

12.14.4.4. IEC62056-42: Physical Layer (PHY)

12.14.4.5. IEC62056-21: Direct Data exchange

12.15. Implementing 3 Classes is Enough to get DLMS Certificate

12.15.1. Current Association

12.15.2. SAP Assignments

12.15.3. Logical Device Names

13. IEC1107 Now a Part of DLMS/COSEM

13.1. IEC 1107 Now is a Part of DLMS/COSEM as IEC62056-21

13.2. **Flag**: Stands for **F**erranti and **L**andis **A**nd **G**yre

13.3. Schlumberger Has Optical Port Identical to Flag but With Different Software Protocol

13.4. ANSI Type 2 or ANSI C12.18 is Equivalent to IEC1107

13.5. IEC 1107 is Usually Half Duplex and Usually over Infra-Red Interface

13.6. IEC1107 Baud: Always Starts at 300 then negotiates to reach 9600 bps

13.7. Server (Meter)/Client (PC) Model

13.7.1. Only Client Can Initiate Communication

13.8. Mode E

13.8.1. Mode E is new and added by DLMS/COSEM to 1107

13.8.2. Peripheral can Talk to Meter with DLMS only if Communication Starts in Mode E (not A, B, C or D) However it can Continue in Mode E

13.8.3. Peripheral can Start Communication with Meter by Direct HDLC

14. Parts of IEC 62056 Standard

14.1. IEC 62056-21: Direct Local Data Exchange

14.1.1. 3rd edition of IEC 61107

14.1.2. Communicating of HHUs to Tariff Devices

14.1.3. Description of Modes: A, B, C, D and E

14.2. IEC 62056-31: Using LAN on Twisted Pair

14.2.1. Extension to IEC61142

14.3. IEC 62056-41: Using PSTN to Connect to WAN

14.4. IEC 62056-53: COSEM Application Layer

14.4.1. COSEM Hierarchy: Physical Device, Logical Device and COSEM Object

14.4.1.1. It is Common to Have 3 Logical devices for Each Meter

14.4.1.1.1. General Logical Device which comprises Clock and Serial No.

14.4.1.1.2. Management Logical Device

14.4.1.1.3. Electrical Logical Device

14.4.1.2. To Reach to Each Logical Device, One new Association should be established

14.4.2. LLS (Low Level Security) is Used on Secure Channel

14.4.2.1. In LLS passwords are passed in Plain Text

14.4.2.2. In LLS only Client is Authenticated

14.4.3. HLS (High Level Security) is Used on Non Secure Channel

14.4.3.1. Describe Algorithm

14.4.3.2. HLS Uses AES Encryption Algorithm with 128 bit Key

14.4.3.2.1. AES is Successor of DES

14.4.3.2.2. AES is Published in 2001

14.4.3.2.3. AES keys are 128 or 192 or 256 bit

14.4.3.2.4. AES Encrypts data in 128 bit Chunks

14.4.3.2.5. AES is a Symmetric Key Cryptography

14.4.3.2.6. AES is Approved by NSA

14.4.3.2.7. AES is Adopted by US Government

14.4.3.2.8. Some Companies Implement AES-GCM (beside, data and key we have a random string input)

14.4.3.3. In HLS both Client and Server are Authenticated

14.4.3.4. We Have Master Key, Global Key and Session Key (also known as dedicated key)

14.5. IEC 62056-61: Object Identification System (OBIS)

14.5.1. Have a General Review on the Entire Groups & Codes

14.6. IEC 62056-62: Interface Classes (ICs)

14.6.1. Meaning of Inheritance

14.6.1.1. Base is the Top Level Class

14.6.2. Meaning of Method and Attribute

14.6.2.1. The First Attribute is LN of the Class

14.6.3. Abstract Classes (Shape, Circle, Rectangle, Oval, …)

14.6.4. Meaning of Class ID

14.6.5. Meaning of Cardinality

14.6.6. Logical Names (LN) and Short Names (SN)

14.6.6.1. LN is "OBIS Code" : "Class ID" : "Attribute ID"

14.6.6.2. SN is base_number + 8*(attibute_number -1)

14.6.6.2.1. Base Number is Due to Manufacturer

14.6.6.3. Short Names are Getting Absolute

14.6.7. Dynamic Data Types (Meter May Alternate Them) & Static

14.6.8. Complex Data Types: Arrays and Structures

14.6.9. Different Date Formats are Supported

14.7. IEC 62056-42: Physical Layer Services and Procedures for Connection-Oriented Asynchronous Data Exchange

14.8. IEC 62056-46: Data link Layer

14.8.1. Comprises 2 Sub-layers

14.8.1.1. LLC (Logical Link Control)

14.8.1.1.1. Thin Sub-layer

14.8.1.1.2. IEC 8802

14.8.1.1.3. Offers Connection-less Services on Connection-Oriented MAC

14.8.1.2. MAC (Medium Access Control)

14.8.1.2.1. Enhanced Version of HDLC

14.8.1.2.2. IEC 13239

14.9. IEC 62056-47: COSEM Transport Layers for IPv4 Networks

14.10. IEC 62056-51: Application Layer Protocols

14.10.1. Entire APDUs are Discussed

14.11. IEC 62056-52: Communication Management Protocol, DLMS Server

15. Some of COSEM Classes

15.1. Sample and Most Important Classes

15.1.1. Data (ID=1) [0..n]

15.1.1.1. Attrib: LN, Value

15.1.2. Register (ID=3) [0..n] Derived from Data

15.1.2.1. Attrib: Multiplier (Power of 10)

15.1.2.2. Method: Reset (Optional)

15.1.3. Extended Register (ID=4) [0..n] Derived from Register

15.1.3.1. Attrib: Status & Capture Time

15.1.4. Demand Register (ID=5) [0..n] Derived from Extended Register

15.1.4.1. Attrib: Start Time & Period

15.1.5. Register Monitor (ID=21) [0..n] Derived from Base

15.1.5.1. Attrib: LN, Threshold, Monitored_Value, Actions (Script to Run)

15.1.6. Clock (ID=8) [0..1] Derived from Base

15.1.6.1. Attrib: LN, Time, Time_Zone, Status, Daylight_Saving_Begin, Daylight_Saving_End, Daylight_Saving_Deviation, Daylight_Saving_Enabled

15.1.6.2. Methods: Shift_Time, Preset_Time

15.1.7. Script Table (ID=9) [0..n] Derived from Base

15.1.7.1. Attrib: LN, Scripts (an array)

15.1.7.2. Method: Execute (Mandatory Method)

15.1.8. Profile Generic (ID=7) [0..n] Derived from Base

15.1.8.1. Attrib: LN, Buffer (array), Captured_Objects, Captured_Period, Sorted_Method, Sort_Object

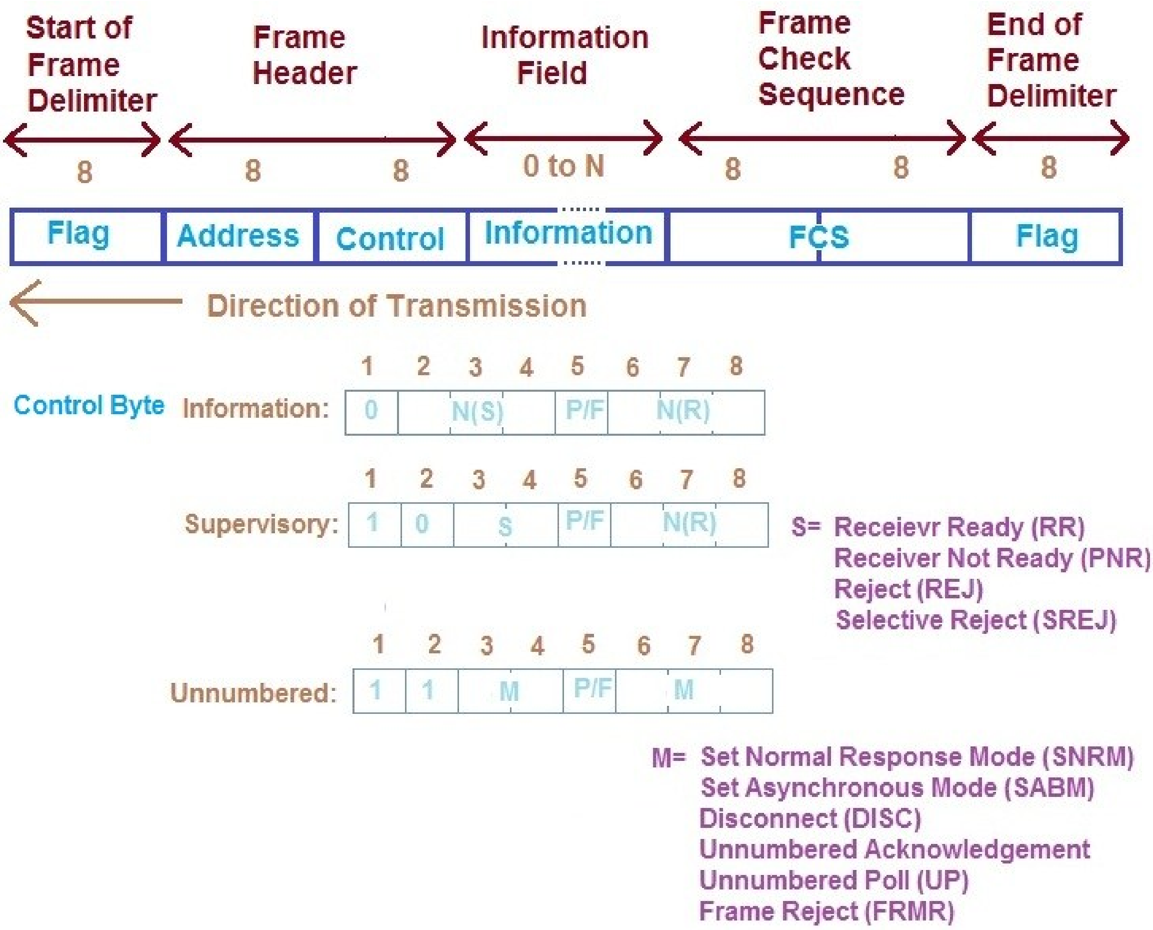
15.1.8.1.1. Capture_Object Structure: {Class_ID, LN}

15.1.8.1.2. Sort Enum: {FIFO, LIFO, Smallest, Largest, Nearest _To_Zero, Farest_From_Zero}

Appendix 0: Course Schedule

Day	Session	Topics
Tuesday	1	Protocol Definition & History
	2	Aspects of Protocols
	3	Modbus
	4	
Wednesday	1	TCP/IP (part of IEC60870-5-104)
	2	
	3	
	4	HDLC
Thursday	1	IEC60870-5-101 & T104 And comparison with DNP3
	2	
	3	DLMS/COSEM (+ IEC1107)
	4	

Appendix 1: HDLC Frame Format



- Flag Byte (or Delimiter) is Always 01111110 (0x7E)
- Broadcast Address is 11111111
- N(S) is Sender Sequence Number and N(R) is Receiver Sequence Number
- When P/F is set to 1 it means acknowledgement is required

Appendix 2: IPv4 Packet Format

32 Bit

<table>
<tr><td colspan="4">Version</td><td colspan="4">IHL</td><td colspan="6">Service Type</td><td colspan="2"></td><td colspan="16">Total Length</td></tr>
<tr><td colspan="16">ID</td><td colspan="1"></td><td colspan="1">DF</td><td colspan="1">MF</td><td colspan="13">Fragment Offset</td></tr>
<tr><td colspan="8">Time to Live</td><td colspan="8">Protocole</td><td colspan="16">Header Checksum</td></tr>
<tr><td colspan="32">Sourse Address</td></tr>
<tr><td colspan="32">Destination Address</td></tr>
<tr><td colspan="32">Options (Variable Length)</td></tr>
</table>

IHL: Header Size in multiple of 32-bits, Min is 5

Type of Service: first 3 bits are priority of packet (0: normal, 7: Network Control Packet) and next 3 bits are D (Delay is Important), T(Throughput is Important) and R(Reliability is Important)

ID: is unique for all fragments of one datagram

DF: Datagram won't be fragmented if this bit is set

MF: More Fragments, this bit is set for all fragments except the last one.

Fragment Offset: Sequential number for fragments of a datagram

Time To Live: Number of Hops

Protocol: Either TCP or UDP

Header Checksum: Will be calculated in each router node

Options: Describes Security Level of Datagram or Strict Routing Path or ...

Appendix 3: IPv6 Packet Format

32 Bit

<table>
<tr><td colspan="4">Version</td><td colspan="8">Traffic Class</td><td colspan="20">Flow Label</td></tr>
<tr><td colspan="16">Payload Length</td><td colspan="8">Next Header</td><td colspan="8">Hop Limit</td></tr>
<tr><td colspan="32">Sourse Address (16 Bytes)</td></tr>
<tr><td colspan="32">Destination Address (16 Bytes)</td></tr>
</table>

Version: for Ipv6 is 6

Traffic Class: Not Used Yet, Indicates Real-time Delivery Requirements

Flow Lable: Not Used Yet, Indicates that Receiver has Limitation for Accepting Data

Next Header: If There is an Extension for Header (Optional Header), Points to That

Hop Limit: Same as TTL (Time to Live)

Appendix 4: TCP Header Format

32 Bit

<table>
<tr><td colspan="9">Source Port</td><td>Destination Port</td></tr>
<tr><td colspan="10">Sequence Number</td></tr>
<tr><td colspan="10">Acknowledgement Number</td></tr>
<tr><td>Header Length</td><td></td><td>URG</td><td>ACK</td><td>PSH</td><td>RST</td><td>SYN</td><td>FIN</td><td colspan="2">Window Size</td></tr>
<tr><td colspan="9">Checksum</td><td>Urgent Pointer</td></tr>
<tr><td colspan="10">Option (0 or more DWORDS)</td></tr>
<tr><td colspan="10">Data (Optional)</td></tr>
</table>

Acknowledgemnet Number: Receiver adds 1 to Sequence Number of last got Packet and sends ack. Packet to sender. (It is byte number not packet number)

Header Length: Length of Header in DWORDS

URG: (Urgent) 1 Means “Urgent Pointer“ Field is Valid

ACK: (Acknowlegement) 1 Means “ Acknowlegement Number“ Field is Valid

PSH: (Pushed Data) 1 Means receievr shouls pass packet to Application layer and not buffer it (to get full sequence)

RST: (Reset) Reset a connection for a reason in the other side

SYN: (Synchronize) 1 Means a connection establishment is requested. 1st side sends a segment with SYN=1 and ACK=0 and the other side sends a packet with SYN=1 and ACK=1 (Connection Accepted)

FIN: (Finish) 1 Means Sender has no more data to send, hence connection termination requested. (NOTE: Even SYN and FIN Segments have Sequence Numbers)

Window Size: Receiever sends a number in this field which means how many further bytes it has capacity to recieve. 0 Means no more data can be accepted, after some time it can send another packet with the same ACK number and nonzero window size.

Urgent Vector: If not zero, this number should be added to Sequence number to point out the last byte of Urgent data in the stream.
Options: Including different items like maximum payload that this network can accept