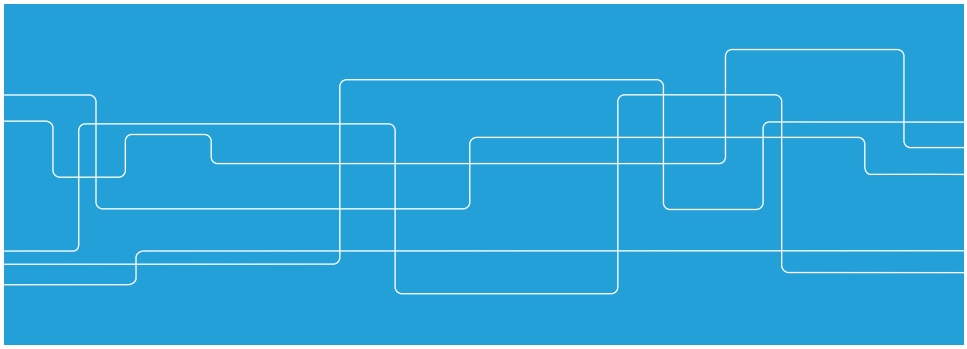
KTH ROYAL INSTITUTE
OF TECHNOLOGY

Lecture #11
Power system communication

Nicholas Honeth <honeth@kth.se>



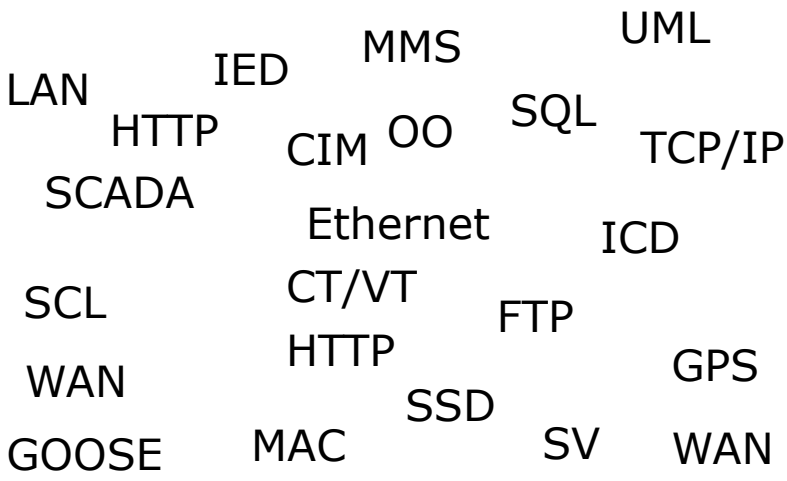
In this series…

- Lecture #9
  - Communication protocol basics
  - The OSI model
  - Relationship between OSI and SGAM
  - **Hands-on exercise**: Wireshark and HTTP
- Lecture #10
  - OSI model – physical layer
  - Topologies
  - Media Access Control
  - Routing
  - TCP/IP
  - Exercise: Traceroute, ping and Wireshark

In this series…

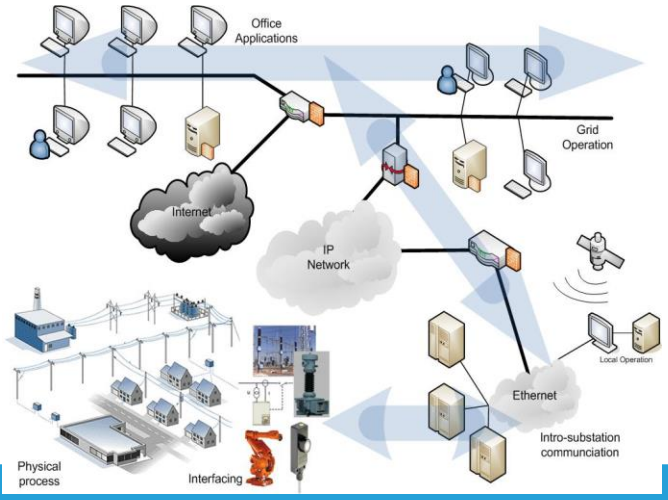
- Lecture #11
  - Power systems communication
  - Wireshark exercises
- Lecture #12
  - Delay & Jitter
  - Quality-of-Service
  - Loss and Throughput
  - Time synchronization
  - Project assignment Q&A

Some terms and acronyms…



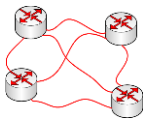
Recap

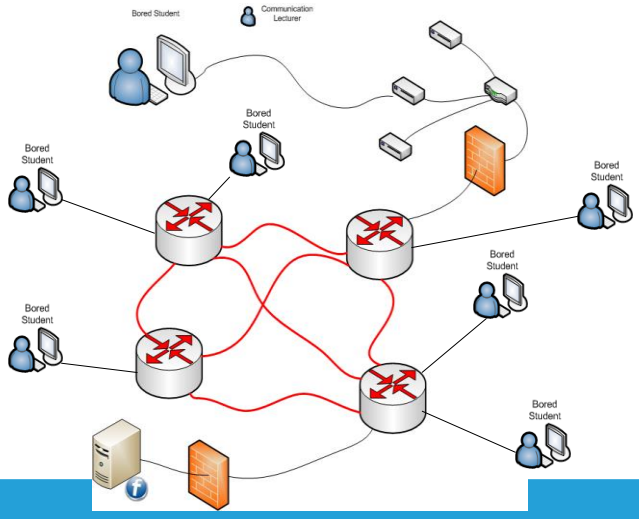
Computers and Networks in Power Systems



Recap

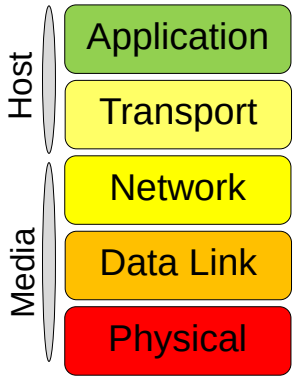
Protocol basics





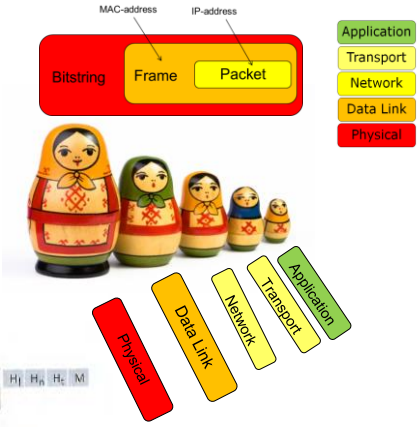
Recap

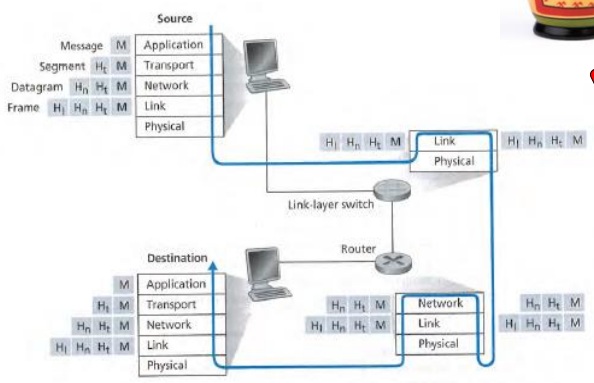
The OSI model



Recap

Transition between layers

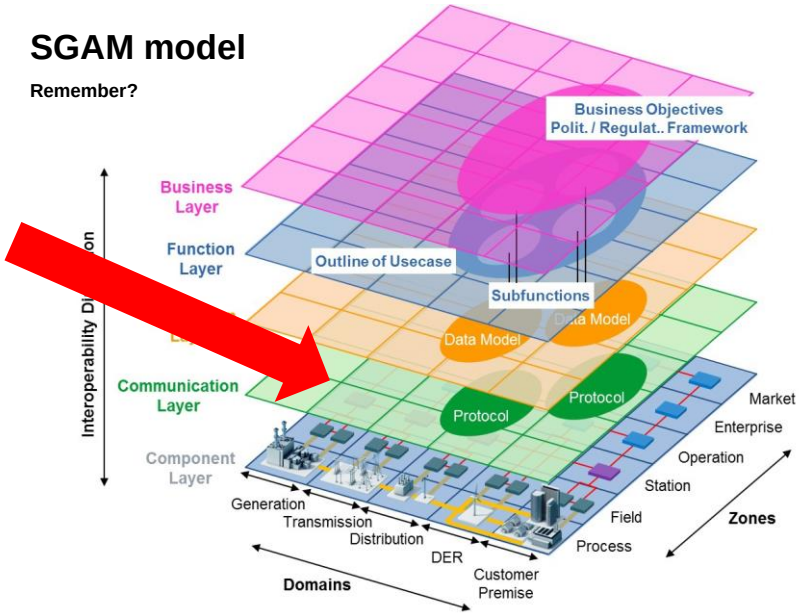




Computer Networking: A Top-Down Approach: International Edition (Kurose & Ross.) 1.5

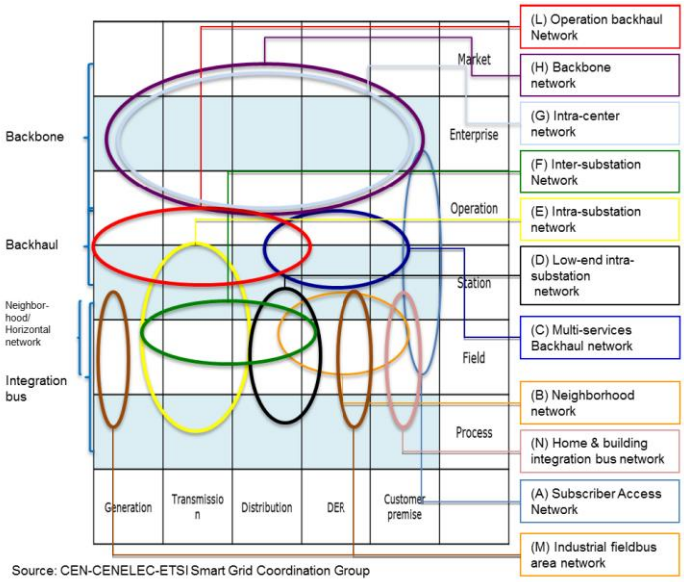
SGAM model

Remember?



SGAM model

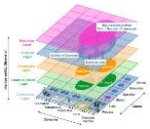
Communication Layer



Source: CEN-CENELEC-ETSI Smart Grid Coordination Group

SGAM model

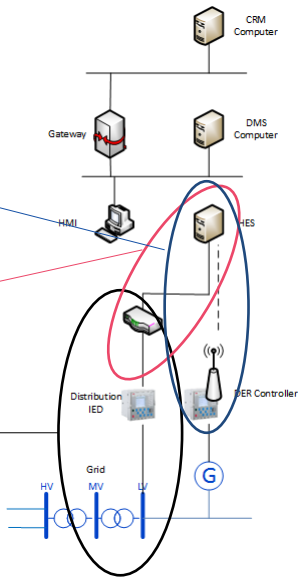
Communication Layer



Multi-services backhaul network

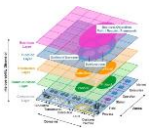
Operation backhaul network

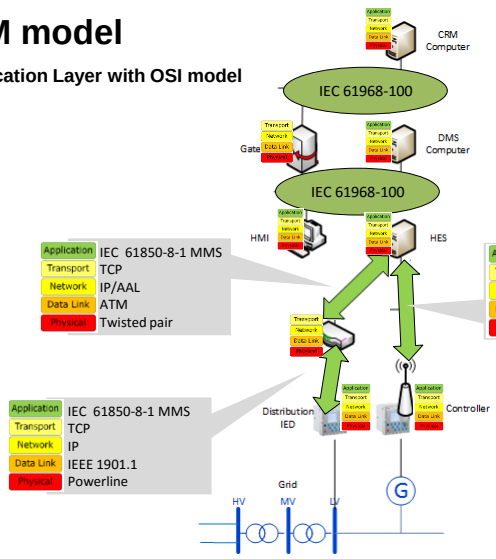
Low-end intra-substation network



SGAM model

Communication Layer with OSI model





Protocols used in power systems

Application

IEC 61850
- GOOSE
- SV
- MMS

IEC 60870-5-101 and 104

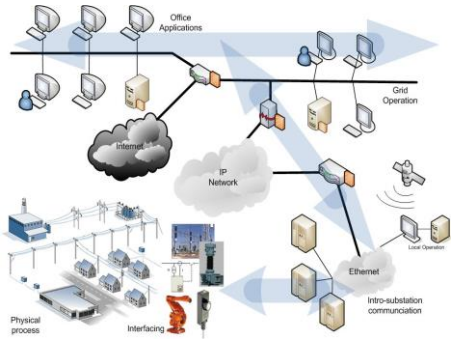
Modbus

DNP3

IEEE C37.118

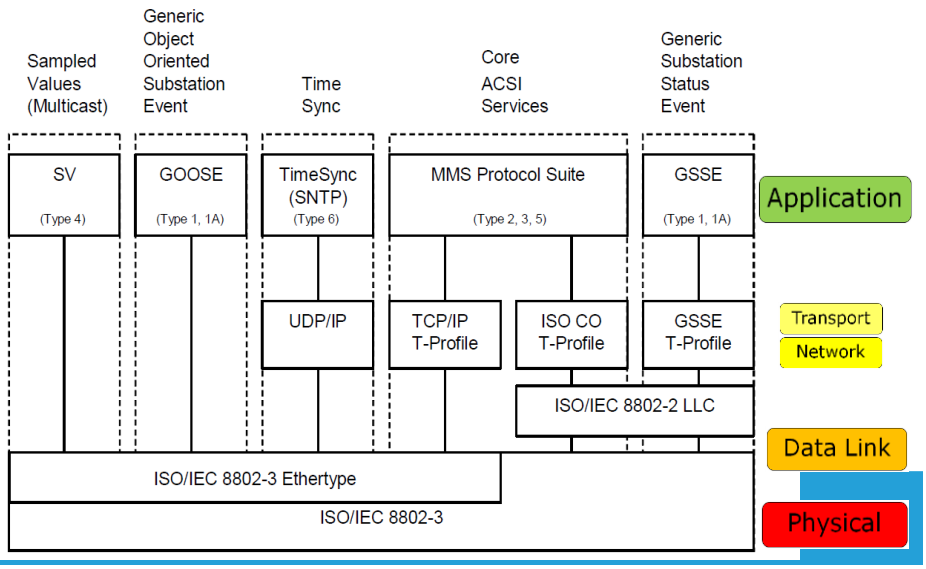
IEC 61968-100

ICCP



Protocols used in power systems

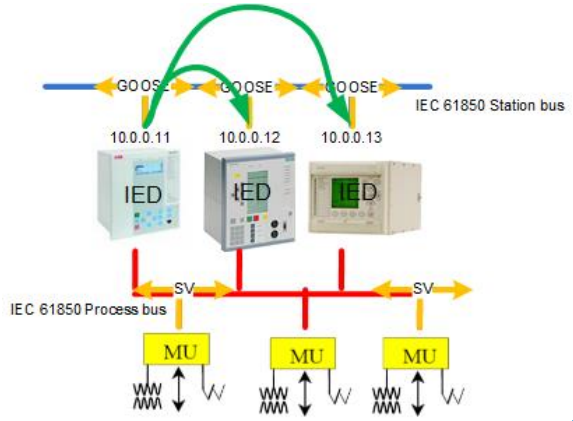
IEC 61850-8-1



Protocols used in power systems

IEC 61850-8-1

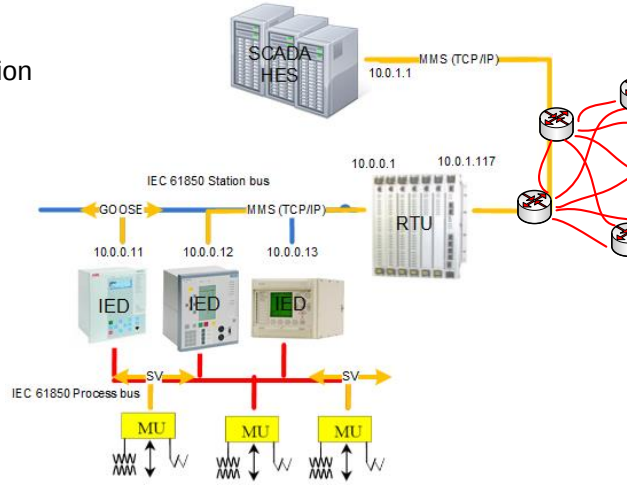
- Horizontal communication



Protocols used in power systems

IEC 61850-8-1

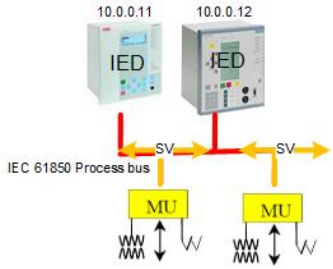
- Vertical communication



Protocols used in power systems

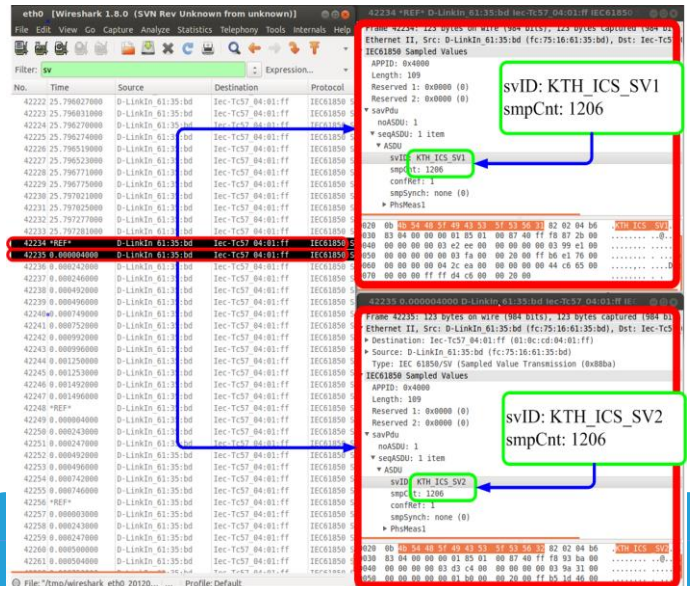
IEC 61850-9-2 Sampled Values (SV)

- Used on the process bus
- Transmits 3-phase CT/VT measurements
- Sampling rate of 4kHz
- Need time synchronization



Protocols used in power systems

IEC 61850-9-2 Sampled Values (SV)

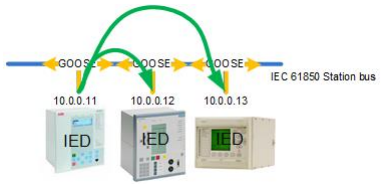


Protocols used in power systems

GOOSE

Generic Object Oriented Substation/System Event

- Specified in IEC 61850-8-1
- Status and values
- Grouped into dataset
- Transmitted within a time of 4ms




```
gocbRef: RET670LD0/LLN0$GO$ABB_GOOSE
timeAllowedtoLive: 1100
datSet: RET670LD0/LLN0$ABB_G_TRIP
goID: ABB_G_TRIP
t: Feb 19, 2011 01:34:27.690000057 UTC
stNum: 53
sqNum: 4
test: False
confRev: 1
ndsCom: False
numDatSetEntries: 5
⊞ allData: 5 items
```

Protocols used in power systems

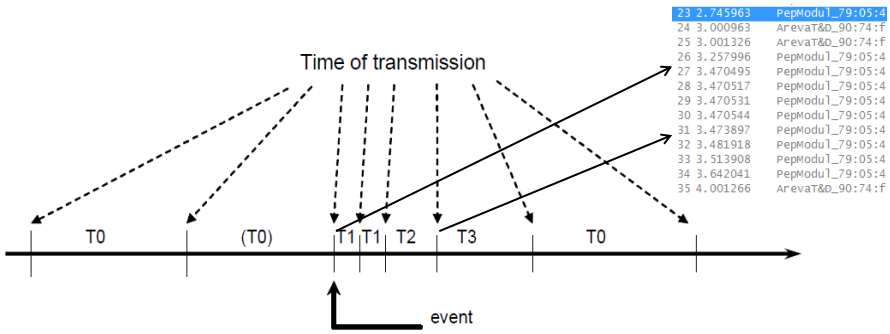
GOOSE

IEC 61850-7-2 parameter	Parameter name
Argument	Argument
	Destination address
DatSet	datSet
GoID[a)]	goID
GoCBRef	gocbRef
T	t
StNum	stNum
SqNum	sqNum
timeAllowedtoLive	timeAllowedtoLive
Test	test
ConfRev	confRev
NdsCom	ndsCom
GOOSEData	numDatSetEnries
	allData
	timeAllowedToLive

```
gocbRef: RET670LD0/LLN0$GO$ABB_GOOSE
timeAllowedtoLive: 1100
datSet: RET670LD0/LLN0$ABB_G_TRIP
goID: ABB_G_TRIP
t: Feb 19, 2011 01:34:27.690000057 UTC
stNum: 53
sqNum: 4
test: False
confRev: 1
ndsCom: False
numDatSetEntries: 5
⊞ allData: 5 items
```

Protocols used in power systems

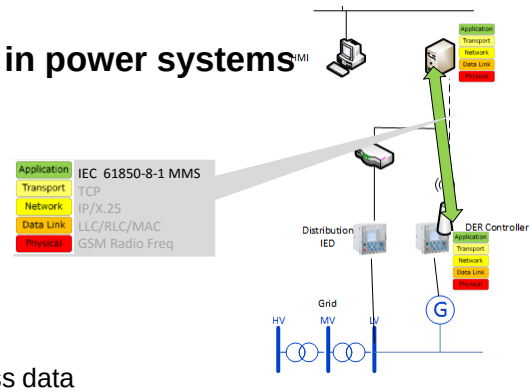
GOOSE – retransmission strategy



T0	retransmission in stable conditions (no event for a long time).
(T0)	retransmission in stable conditions may be shortened by an event.
T1	shortest retransmission time after the event.
T2, T3	retransmission times until achieving the stable conditions time.

Protocols used in power systems

MMS



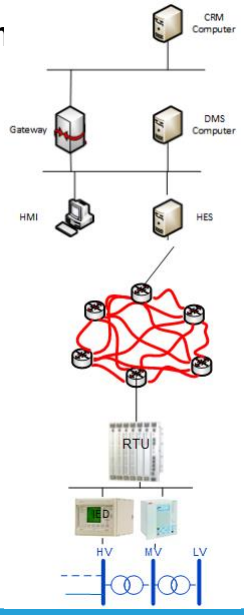
- Open standard
- Transferring real-time process data
- Provides standard messages
- Encoding rules

Application	Association Control Service Element (ACSE)- ISO 8649/8650
Presentation	Connection Oriented Presentation - ISO 8822/8823 Abstract Syntax Notation (ASN)- ISO 8824/8825
Session	Connection Oriented Session - ISO 8326/8327
Transport	ISO transport over TCP - RFC 1006 Transmission Control Protocol (TCP) - RFC 793
Network	Internet Control Message Protocol (ICMP) - RFC 792 Internet Protocol (IP)- RFC 791 Address Resolution Protocol (ARP)- RFC 826
Link	IP datagrams over Ethernet - RFC 894 MAC - ISO 8802-3 [Ethernet]
Physical	Ethernet

Protocols used in power system

IEC 60870-5-10x

- A suite of “RTU protocols”…

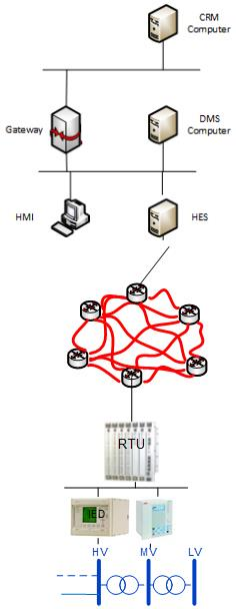


Protocols used in power systems

IEC 60870-5-101 and IEC 60870-5-104

Standard by TC57 (same as IEC 61850)

- Specifically for power systems
  - Monitoring
  - Control
  - Teleprotection
- A few difference flavors exist:
  - 101 – Serial RTU protocol
  - 103 – interoperability between protection/substatio devices
  - 104 – Variant of 101 carried over TCP/IP
- Still very commonly used.



Protocols used in power systems

IEC 60870-5-101 and IEC 60870-5-104

IEC 101 Frame Format, Variable length		
Data unit	**Name**	**Function**
Start Frame	Start Character	*Indicates start of Frame*
	Length Field (*2)	*Total length of Frame*
	Start Character (repeat)	*Repeat provided for reliability*
	Control Field	*Indicates control functions like message direction*
	Link Address (*0,1 or 2*)	*Normally used as the device / station address*
Data Unit Identifier	Type Identifier	*Defines the data type which contains specific format of information objects*
	Variable Structure Qualifier	*Indicates whether type contains multiple information objects or not*
	COT (*1 or 2*)	*Indicates causes of data transmissions like spontaneous or cyclic*
	ASDU Address (*1 or 2*)	*Denotes separate segments and its address inside a device*
Information Object	Information Object Address (*1 or 2 or 3*)	*Provides address of the information object element*
	Information Elements (n)	*Contains details of the information element depending on the type*
Information Object-2	-----	
-----	-----	
Information Object-m		
Stop Frame	Checksum	*Used for Error checks*
	Stop Char	*Indicates end of a frame*

Protocols used in power systems

Modbus

Master/slave RTU protocol mainly for PLC interfacing

- Address up to 240 devices
- *Coils* and *contacts* – old names for status and command points

- Many versions (“flavours”)
  - Serial RTU, ACSII
  - TCP/IP
  - UDP

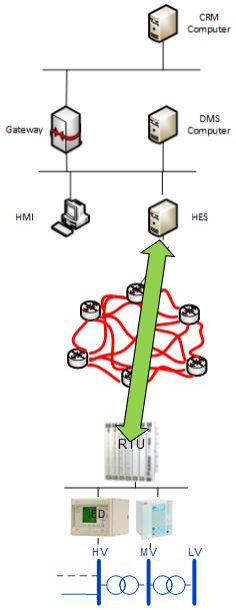
Modbus TCP Frame Format		
Name	**Length**	**Function**
Transaction Identifier	2 bytes	*For synchronization between messages of server & client*
Protocol Identifier	2 bytes	*Zero for MODBUS/TCP*
Length Field	2 bytes	*Number of remaining bytes in this frame*
Unit Identifier	1 byte	*Slave Address (255 if not used)*
Function code	1 byte	*Function codes as in other variants*
Data bytes	n bytes	*Data as response or commands*

Modbus RTU Frame Format		
Name	**Length**	**Function**
Start	3.5c idle	*at least 3-1/2 character times of silence (MARK condition)*
Address	8 bits	*Station Address*
Function	8 bits	*Indicates the function codes like read coils / inputs*
Data	n * 8 bits	*Data + length will be filled depending on the message type*
CRC Check	16 bits	*Error checks*
End	3.5c idle	*at least 3-1/2 character times of silence between frames*

Protocols used in power systems

DNP3

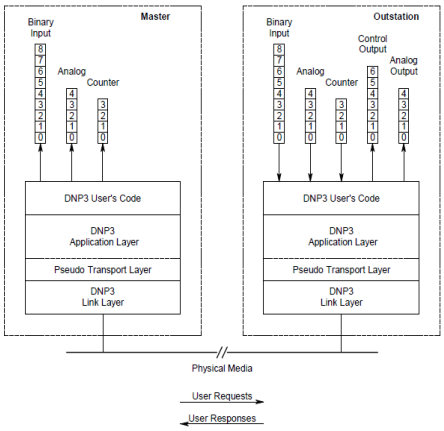
Also an ”RTU protocol”…

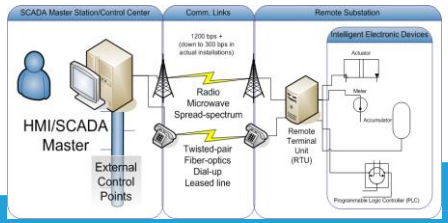


Protocols used in power systems

DNP3

- Distributed Network Protocol
  - SCADA master
  - Remote Terminal Units (RTU)
  - Intelligent Electronic Devices (IED)
  - Mainly for SCADA->RTU/IED
  - Polling and spontaneous access

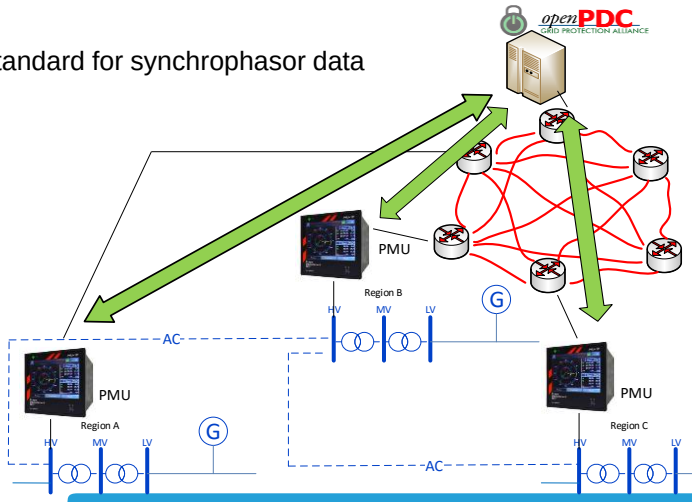




Protocols used in power systems

IEEE C37.118

Standard for synchrophasor data



Protocols used in power systems

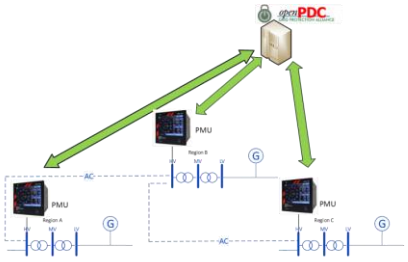
IEEE C37.118

Protocol for real-time exchange of synchronized phasor measurements

Transmission from Phasor Measurement Unit (PMU) to Phasor Data Concentrator (PDC)

Defines:

- Frequency
- Rate of change of frequency



Protocols used in power systems

IEEE C37.118 vs. IEC 61850

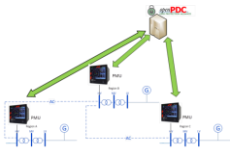


table 1 Comparison of IEEE C37.118 and IEC 61850

Function	C37.118	IEC 61850 GOOSE and SV
Streaming Protocol	Yes	Sampled Values
Rate of Measurement/Reporting	10 -30 samples/sec.	80-256 samples/cycle (4800–15360 samples/sec.)
Natively Routable using IP	Yes	No. Must use bridged-routing (brouting)
Application Focus	Situational Awareness	Control
Standard Addresses Security	No	Yes
Communication profile fully specified	No	Yes
Measurement Specification for synchrophasors	Yes	No
Event Driven Capability	No	GOOSE
Protocol is semantically driven (e.g. object oriented)	No	Yes
Standardized configuration language	No	Yes

https://www.pacw.org/issue/december_2012_issue/iec_61850905_an_overview/iec_61850905_an_overview.html

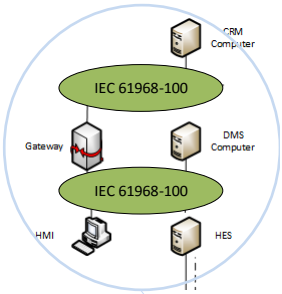
Protocols used in power systems

IEC 61968-100

- Exchanging Common Information Model data at enterprise level
- IEC 61968-100 – Defines profile for application of the other parts of 61968 using common integration technologies, including JMS and web services.
- Provides guidelines and recommendations for usage of Enterprise Service Bus technologies and specific message exchange patterns.

Goal: Make IEC 61968 standards more useful in the marketplace.

- Vendor-specific implementation

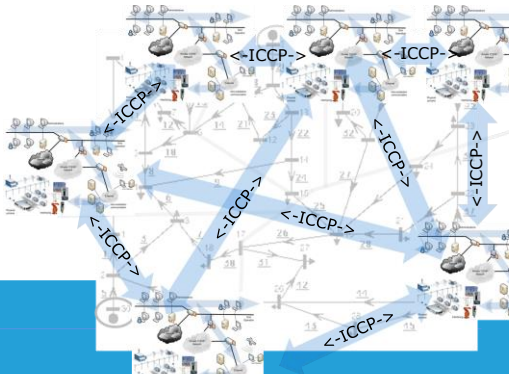


Intra-center network

Protocols used in power systems

ICCP

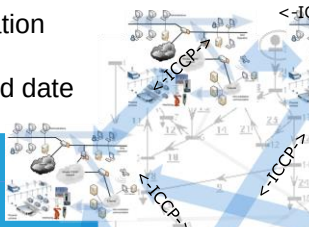
- Inter-Control Center Communications Protocol (IEC 60870-6/TASE.2)
  - Communication between SCADA systems
  - Client/server model
  - Carried over TCP/IP
  - No authentication or encryption



Protocols used in power systems

ICCP - Functionality

- Functions such as:
  - Periodic System Data
    - Status points, analogue points, quality flags, time stamp, counters, protection events
  - Device Control
    - on/off, trip/close, raise/lower etc and digital setpoints.
  - Program Control
    - Allows an ICCP client to remote control programs executing on an ICCP server.
  - Scheduling, accounting, outage and plant information
  - Historical time series data between a start and end date



Protocols used in power systems

Conclusions

We've looked at some **application-layer protocols** which are specific to power systems applications.

There are **many more of these** and there is a lot of overlap between them.

Some protocols (like GOOSE and SV) are link-local and leave-out transport and network-layer functionality.

Many power systems application-layer protocols are carried over TCP/IP (or UDP/IP in some cases).