



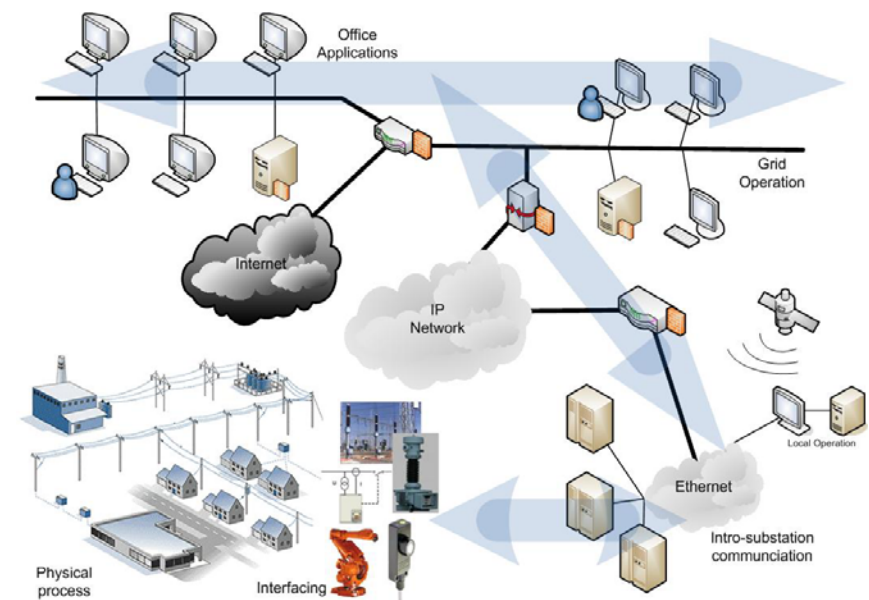
ROYAL INSTITUTE
OF TECHNOLOGY

Interfacing with OPC, IEC61850 and IEC 60870-5-10x

Nicholas Honeth (nicholash@ics.kth.se)

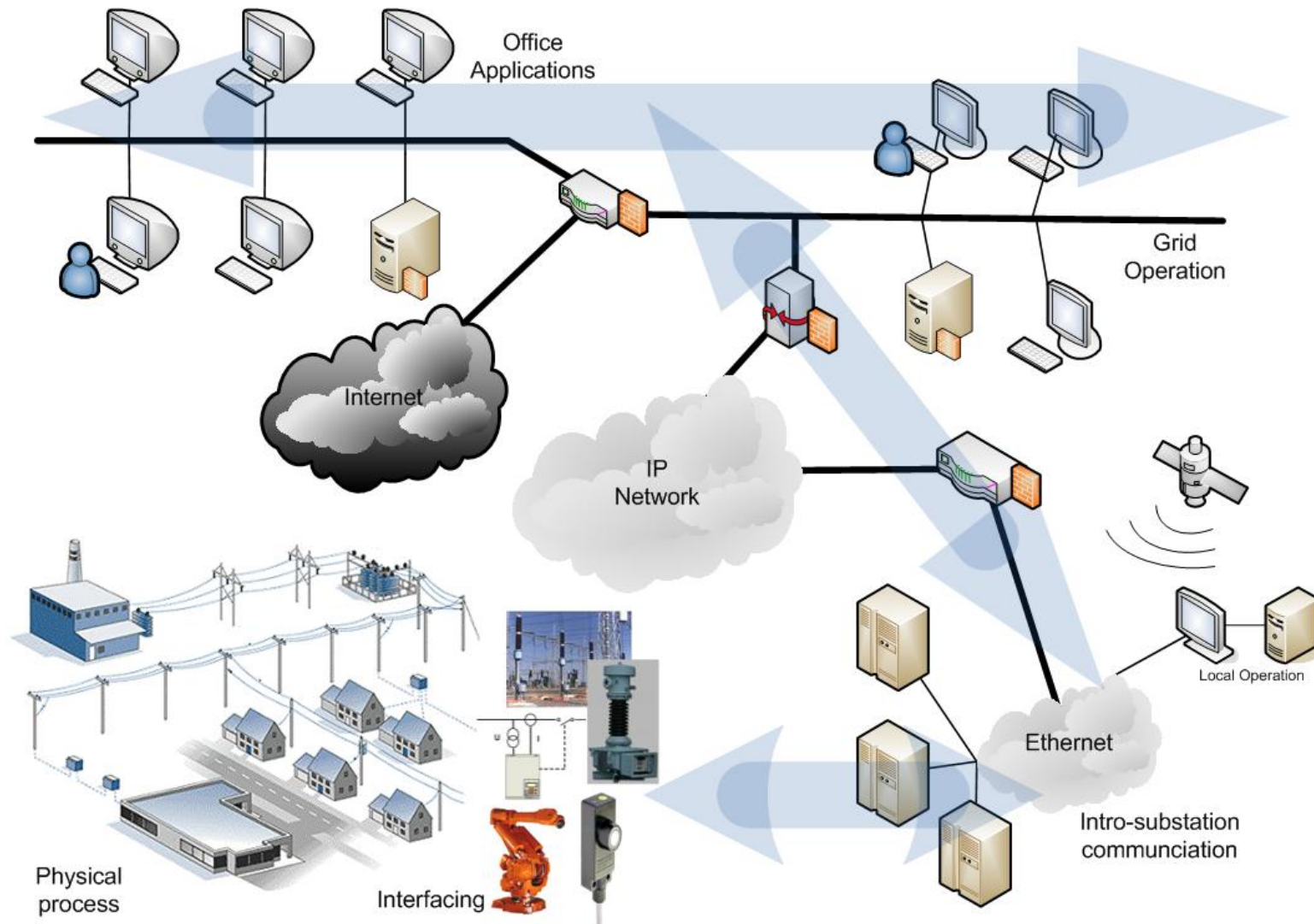
Contents of this tutorial

- Recap of protocols in power systems applications
- Quick introduction to OPC
- IED configuration overview
- JACK interfacing with OPC – the OPCagent



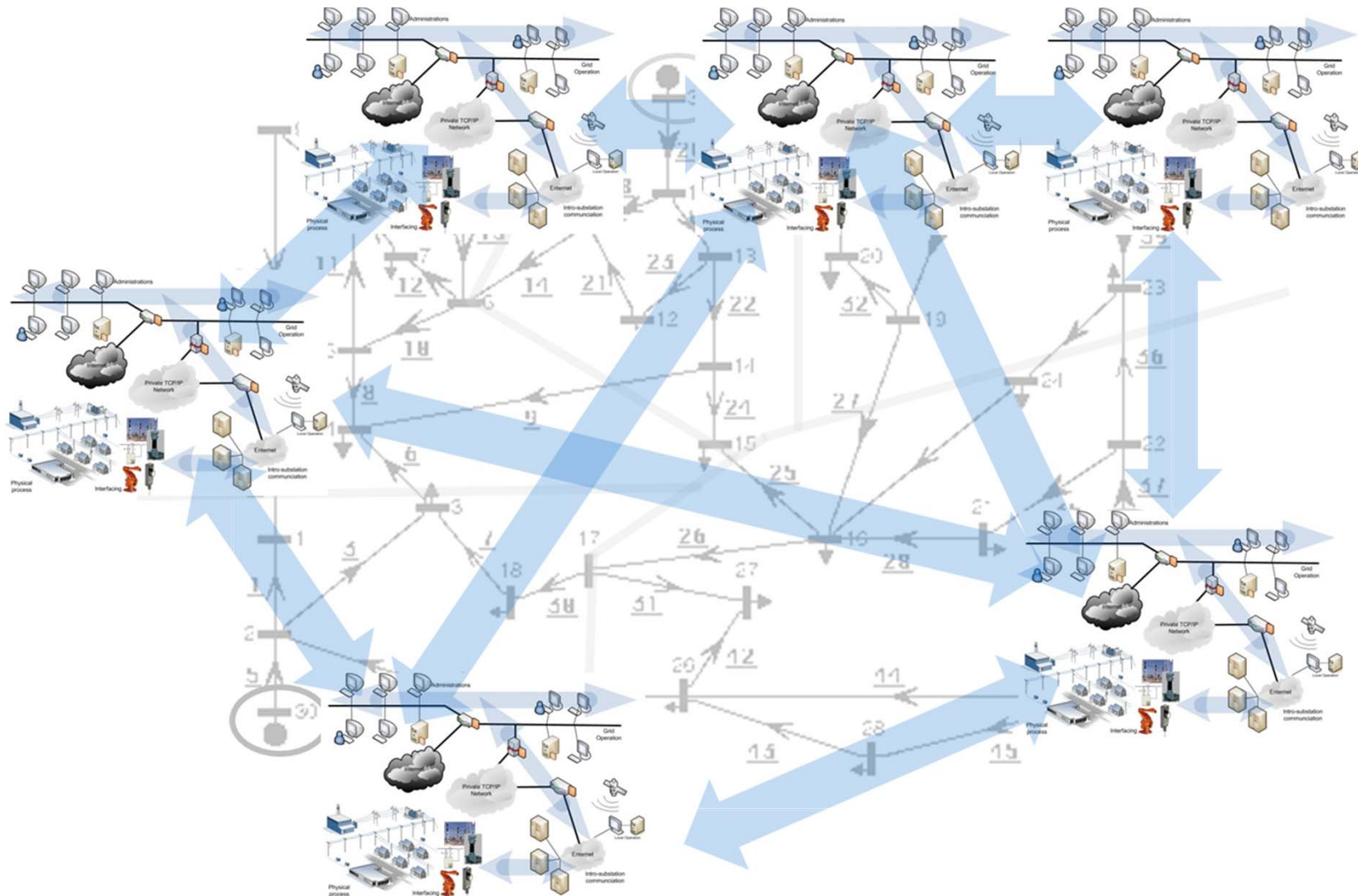
Recap

Computers and Networks in Power Systems



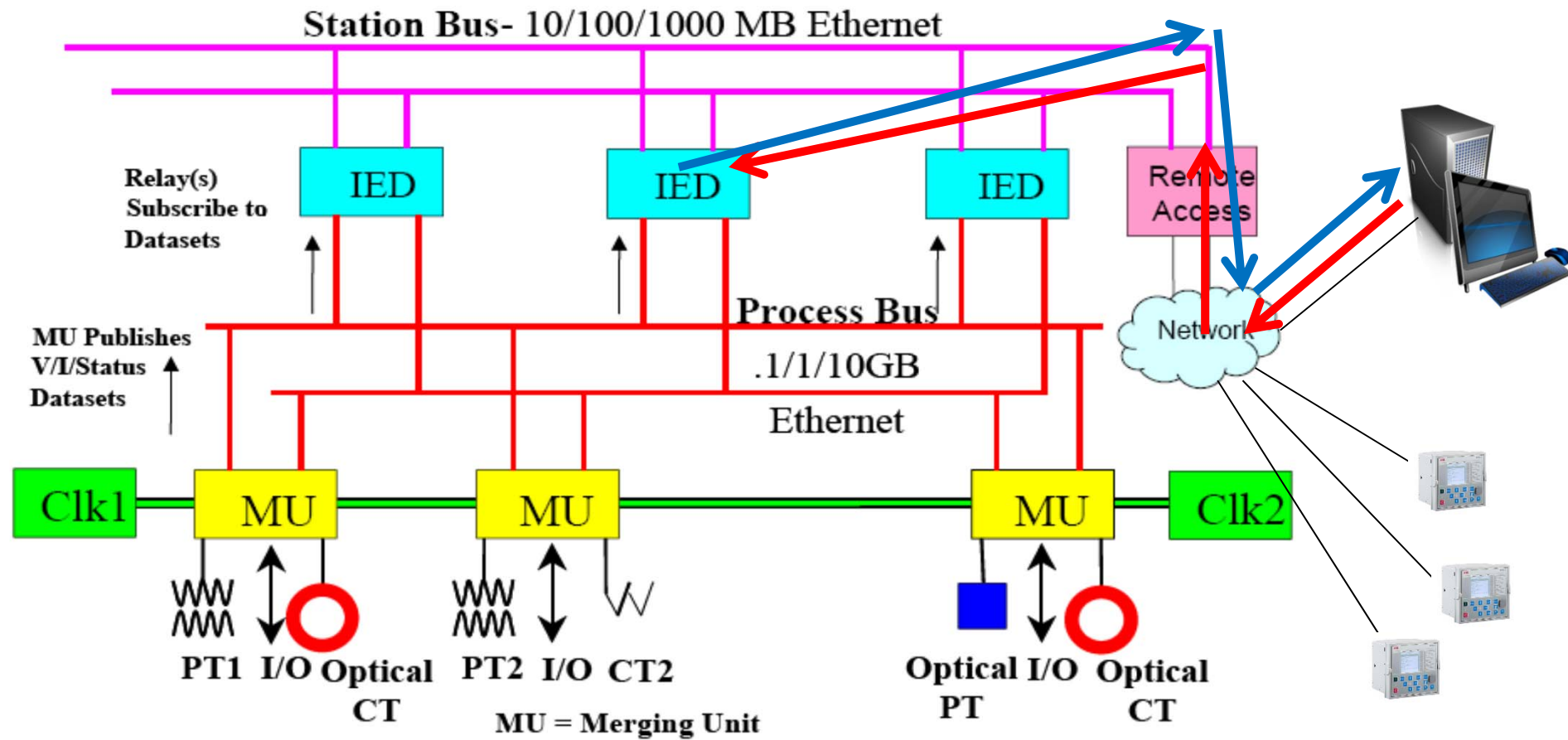
Recap

SCADA Networks



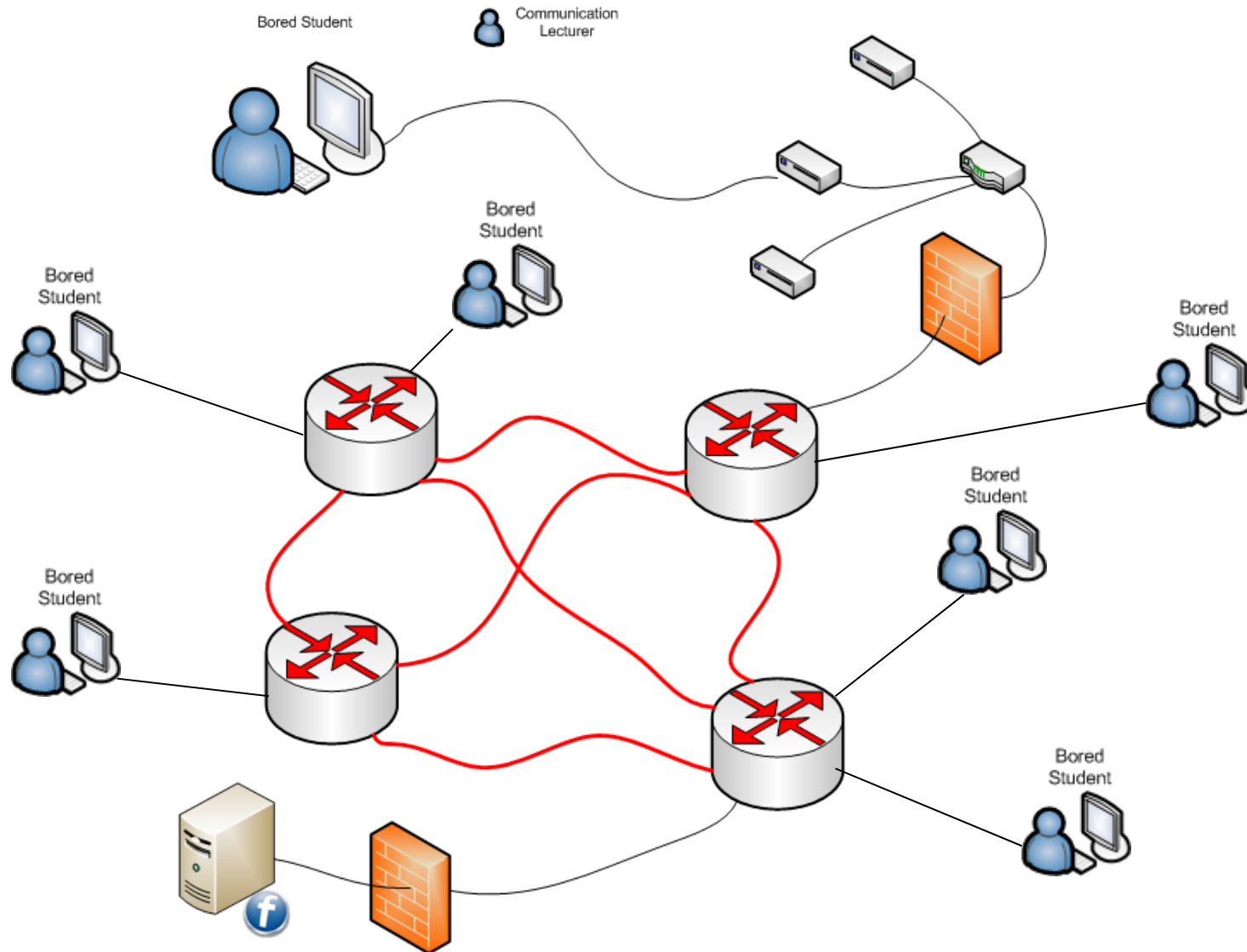
Recap

Modern substation



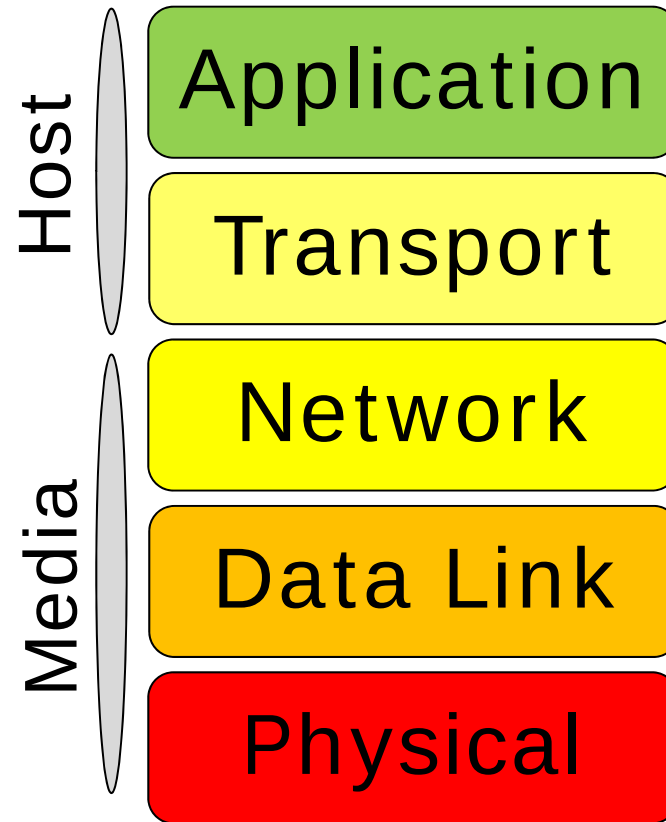
Recap

Protocol basics



Recap

The OSI model



Recap

Transition between layers

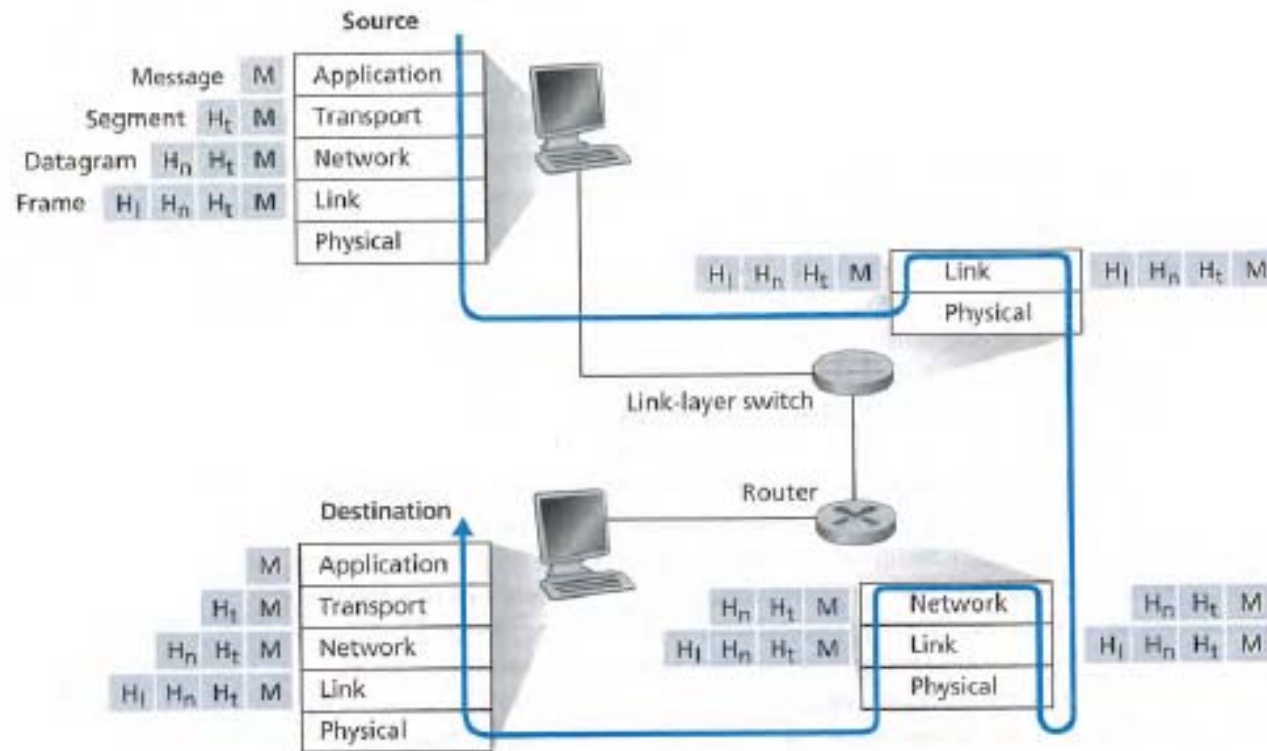
Application

Transport

Network

Data Link

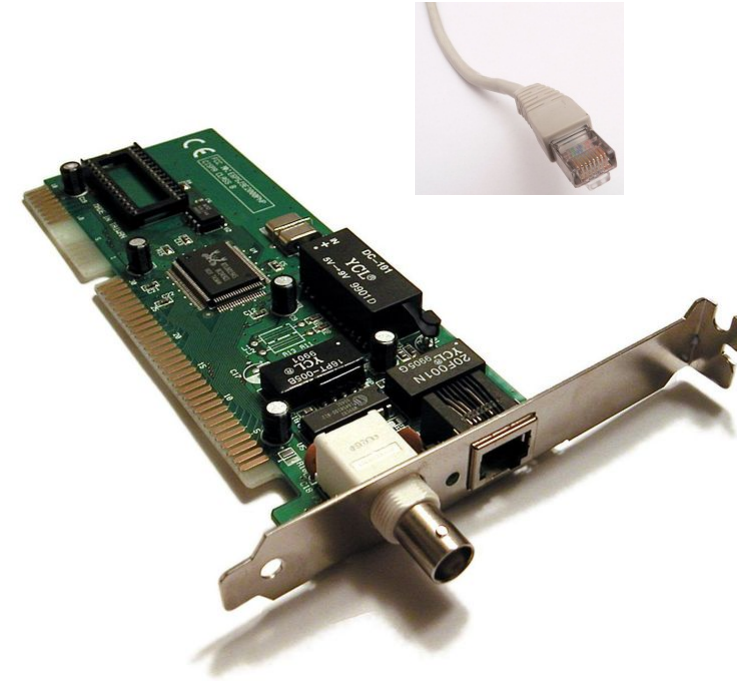
Physical



Recap - Physical media

Communication devices

- Network Interface Controller (NIC)
 - Physical and data link layer
 - Sometimes even network layer
 - Ethernet cards have unique MAC address
 - Interface to host computer
 - Polling
 - Interrupt-driven
 - Direct Memory Access



Network

Data Link

Physical

Recap - Physical media

Communication devices



- Switch

- Physical and data link layers (bridge)
- Managed switches exist
 - Security
 - Performance
- Learns the MAC address of each connected device
- “Switch” methods
 - Store-and-forward
 - Cut-through
 - Fragment-free – first 64 bytes
 - Adaptive – choose between the 3 above

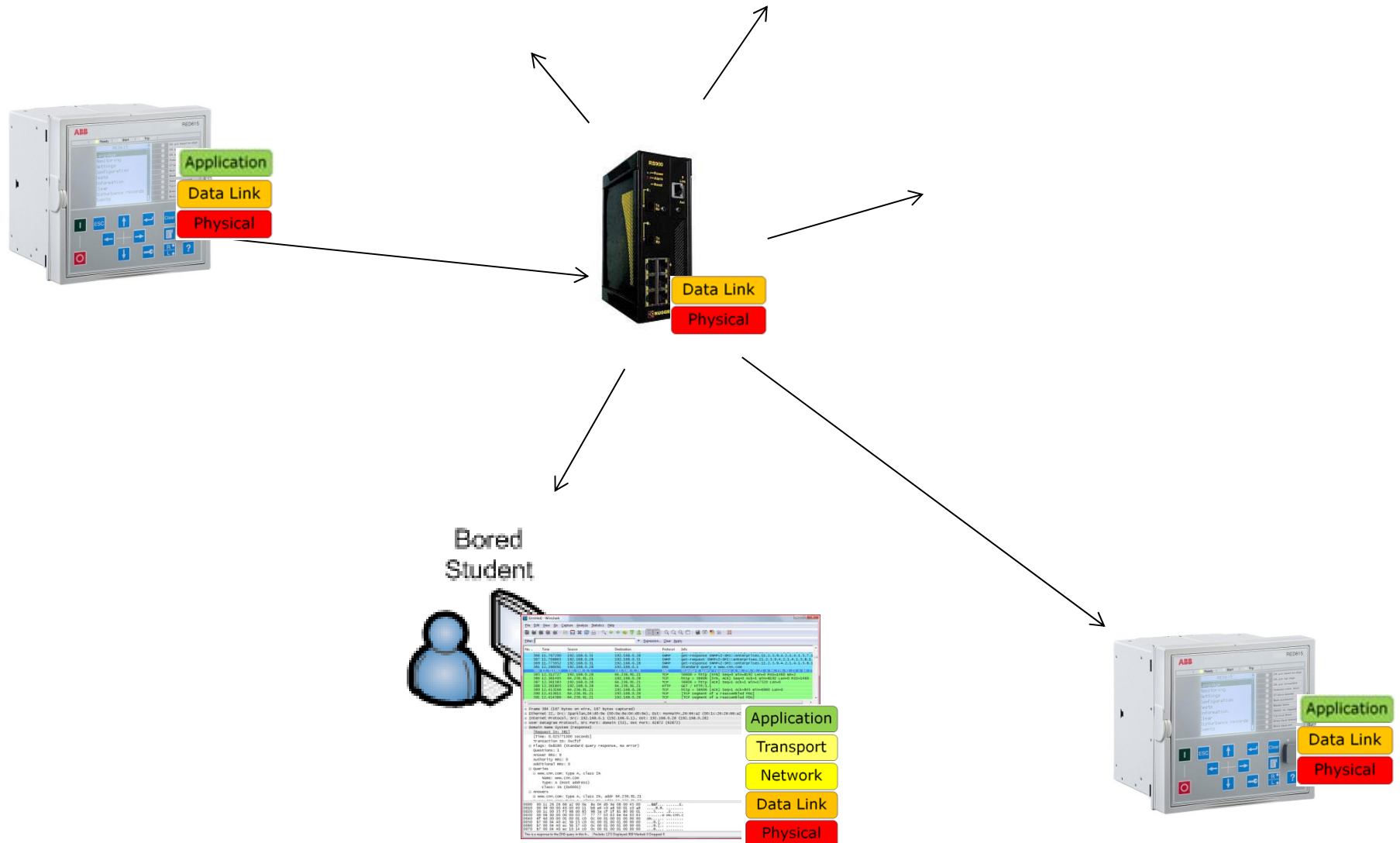


Data Link

Physical

Recap - GOOSE

OSI model explanation

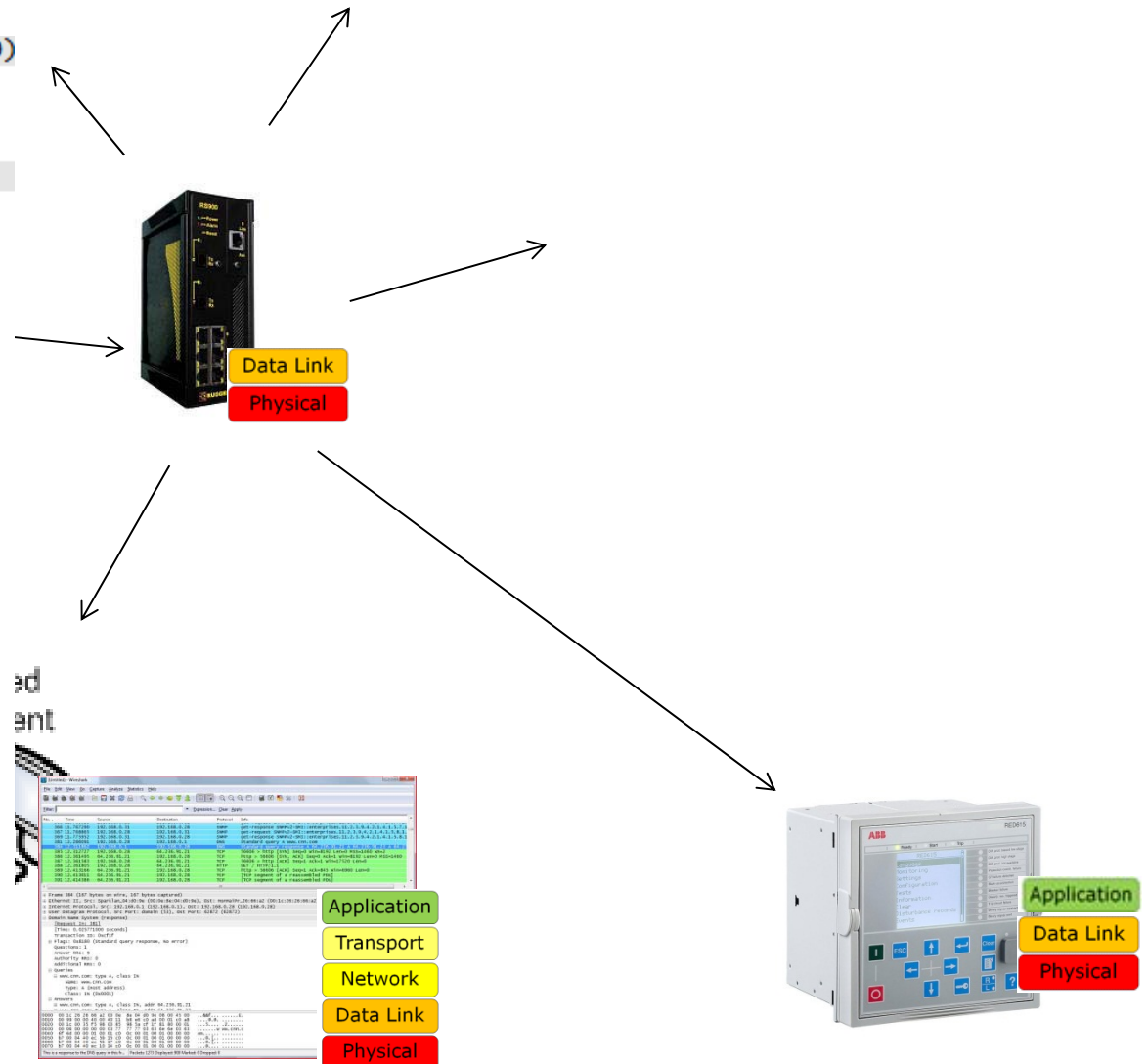


Recap - GOOSE

OSI model explanation



- [-] Ethernet II, Src: PepModul_79:05:49 (00:80:82:79:05:49)
 - [+] Destination: Iec-Tc57_01:00:01 (01:0c:cd:01:00:01)
 - [+] Source: PepModul_79:05:49 (00:80:82:79:05:49)
 - Type: IEC 61850/GOOSE (0x88b8)
- [-] GOOSE
 - APPID: 0x0001 (1)
 - Length: 129
 - Reserved 1: 0x0000 (0)
 - Reserved 2: 0x0000 (0)
 - [-] goosePdu
 - gocbRef: RET670LD0/LLN0\$GO\$ABB_GOOSE
 - timeAllowedtoLive: 1100
 - datSet: RET670LD0/LLN0\$ABB_G_TRIP
 - goID: ABB_G_TRIP
 - t: Feb 19, 2011 01:34:26.794000029 UTC
 - stNum: 48
 - sqNum: 0
 - test: False
 - confRev: 1
 - ndsCom: False
 - numDataSetEntries: 5
 - [-] allData: 5 items
 - [-] Data: boolean (3)
 - boolean: True
 - [-] Data: boolean (3)
 - boolean: True
 - [-] Data: boolean (3)
 - boolean: True
 - [-] Data: boolean (3)
 - boolean: False
 - [-] Data: bit-string (4)



GOOSE exercise

OSI model explanation

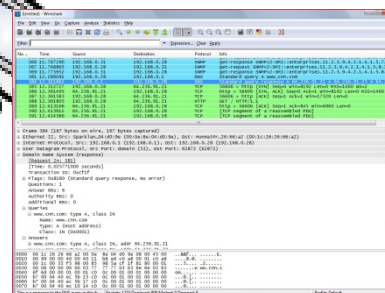
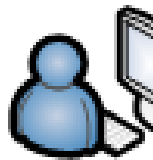


Application



- + Frame 18: 143 bytes on wire (Physical bits), 143 bytes captured (1144 bits)
- Ethernet II, Data Link pModul_79:05:49 (00:80:82:79:05:49), Dst: Iec-Tc57_
- + Destination: Iec-Tc57_01:00:01 (01:0c:cd:01:00:01)
- + Source: PepModul_79:05:49 (00:80:82:79:05:49)
- Type: IEC 61850/GOOSE (0x88b8)
- + GOOSE Application

Bored
Student

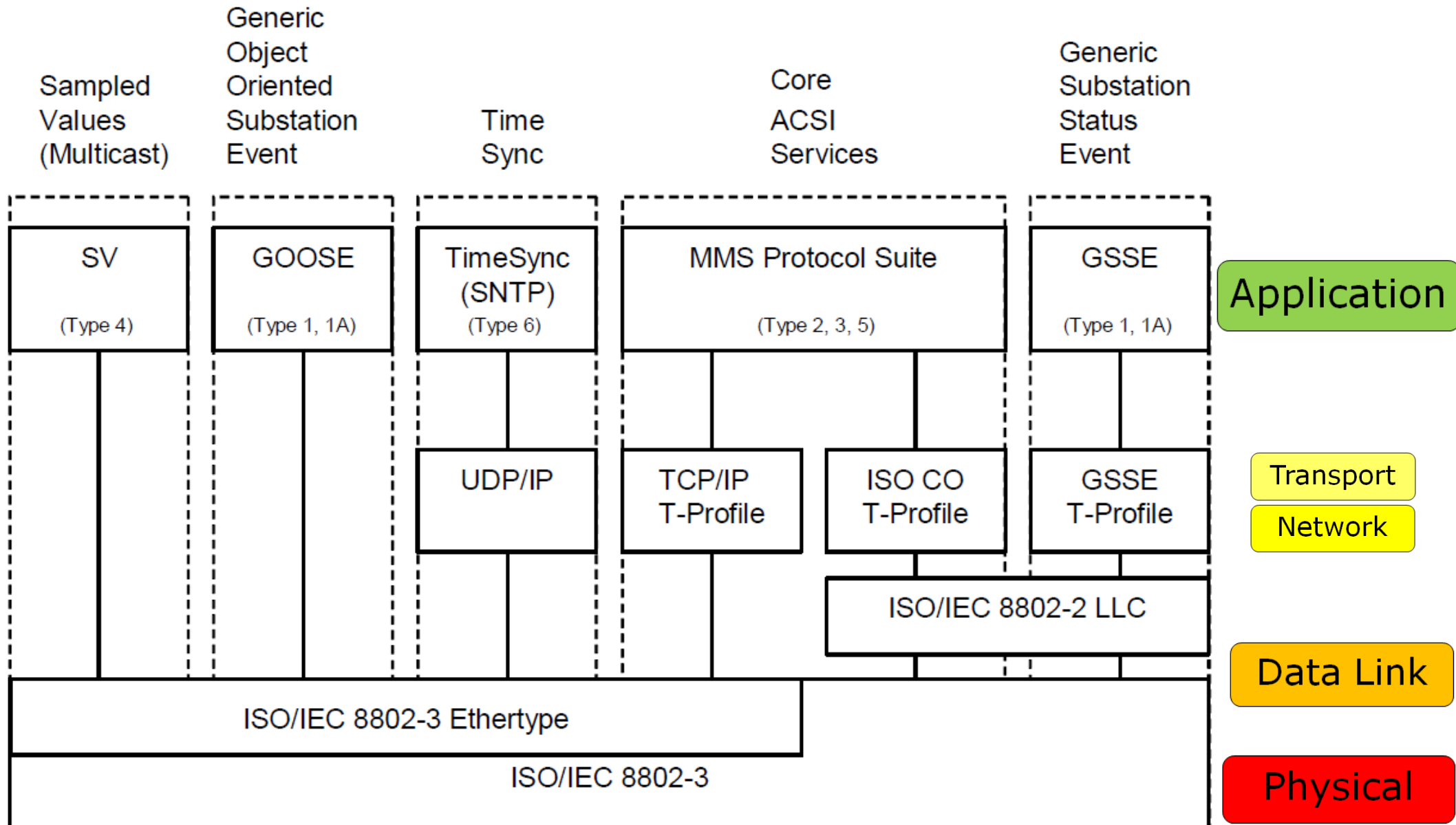


Protocols used in power systems

- IEC 61850
 - GOOSE
 - SV
 - MMS
 - IEC 60870-5-10x
 - Modbus
 - DNP3
 - ICCP
-

Protocols used in power systems

IEC 61850-8-1



Protocols used in power systems

GOOSE

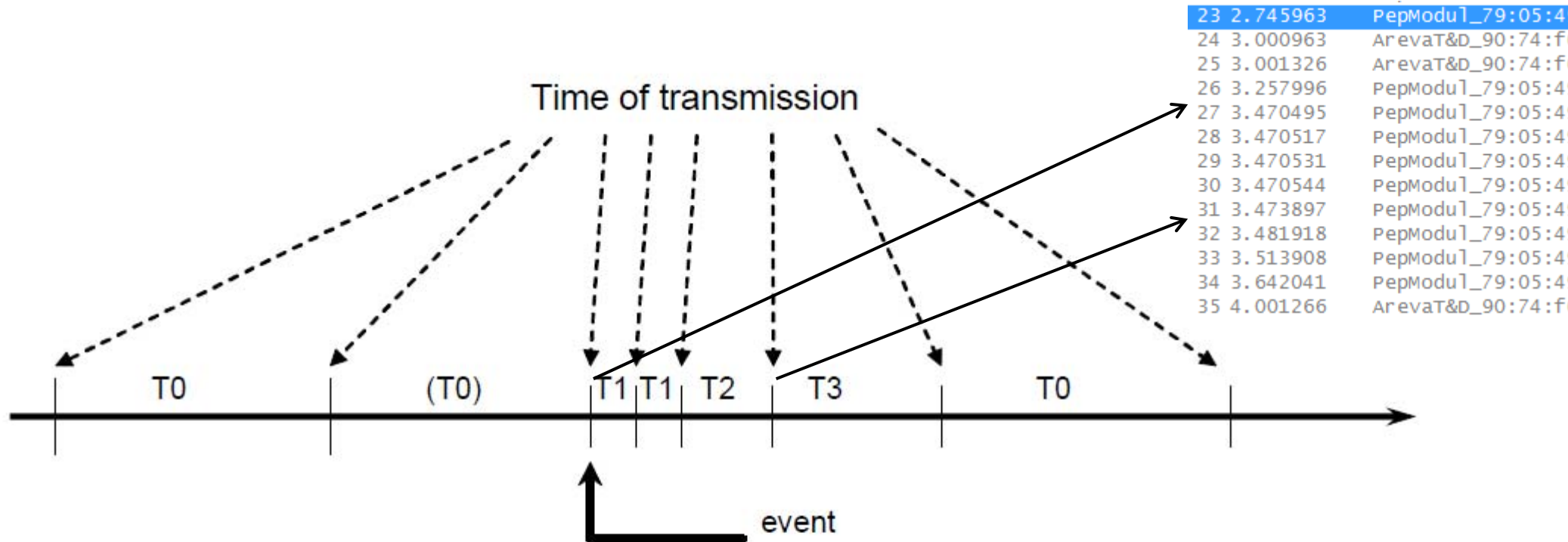
- Generic Object Oriented Substation Event

- 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
dataset: 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
numDataSetEntries: 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

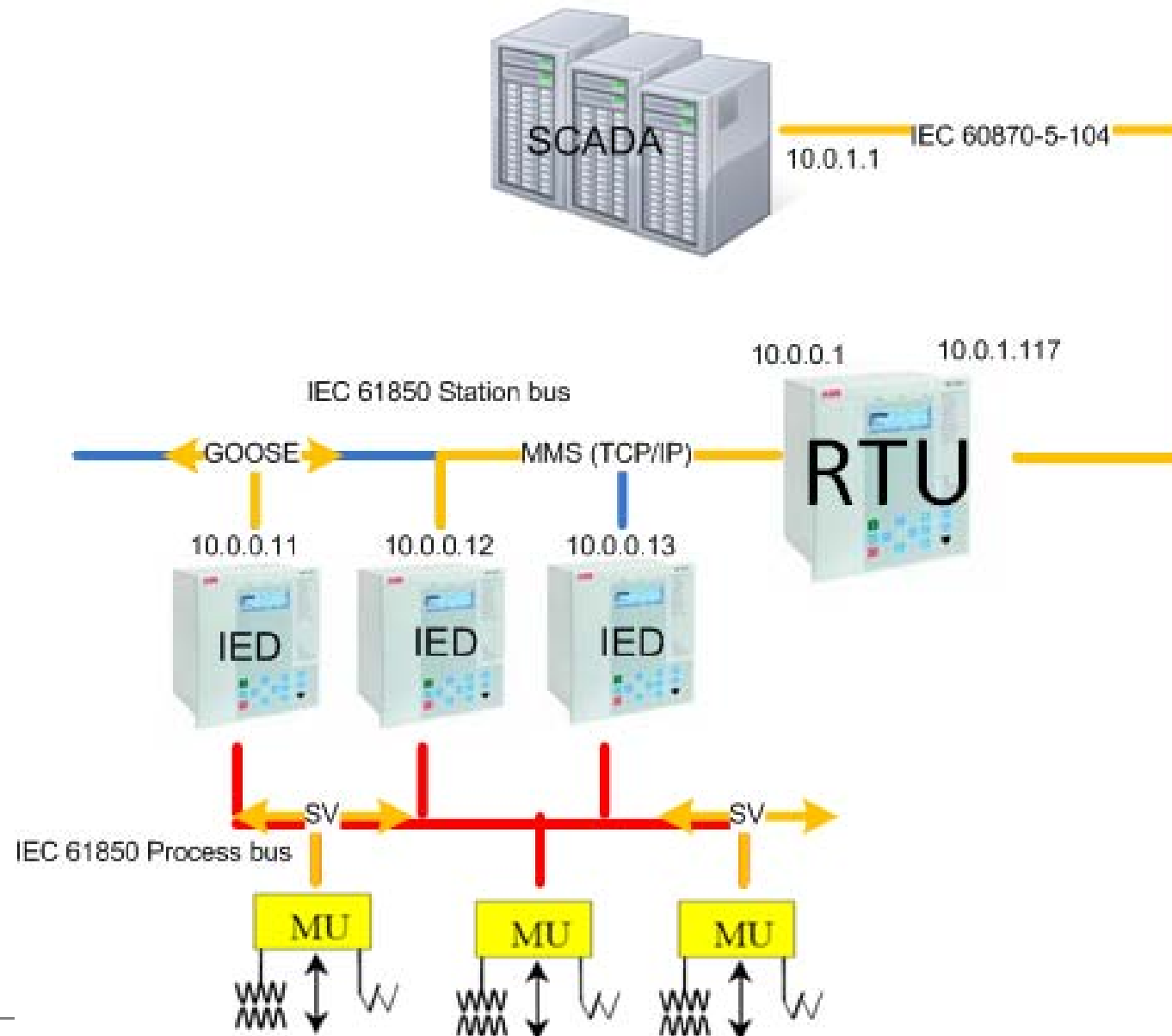
MMS

- 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 systems

IEC 61850-8-1



Protocols used in power systems

IEC 61850-8-1

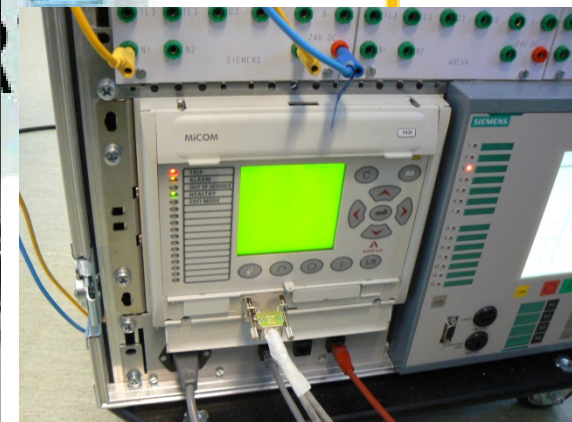
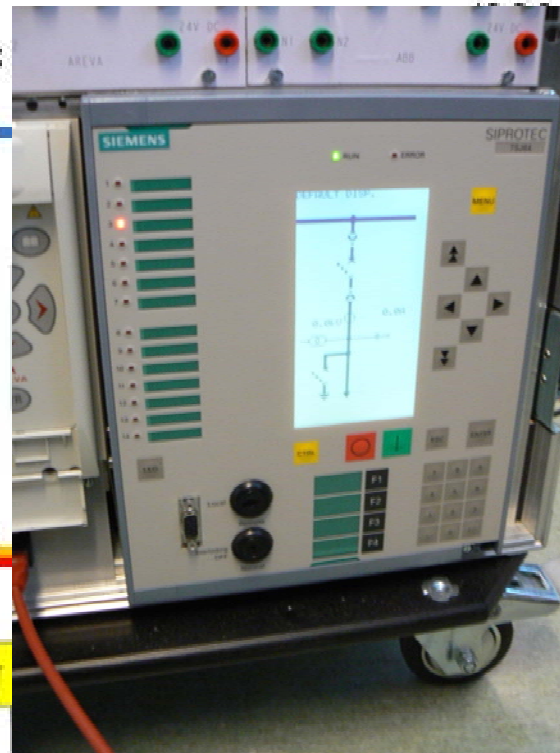


10.0.1.117



IEC 61850 F1000-5-104

IEC

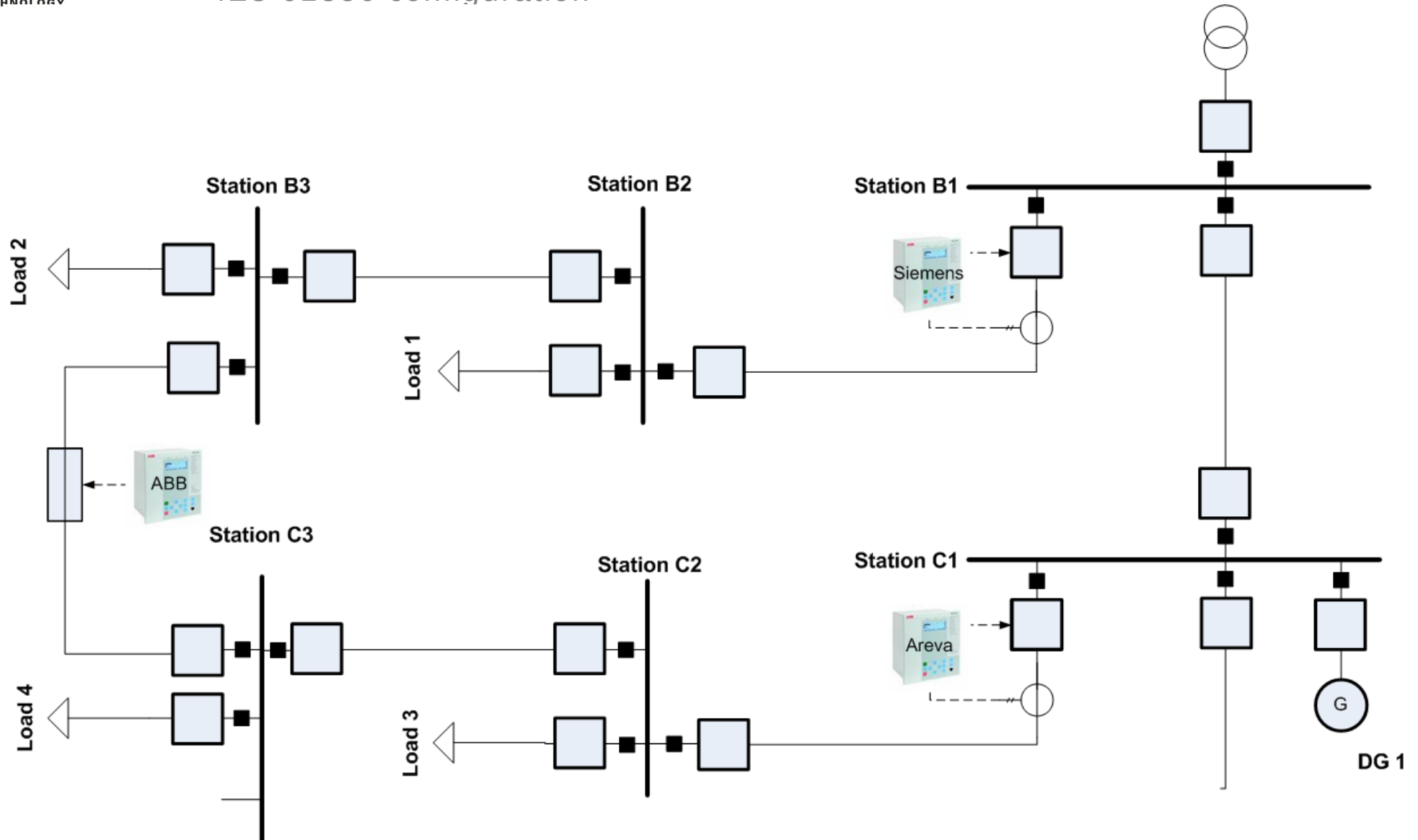


MU



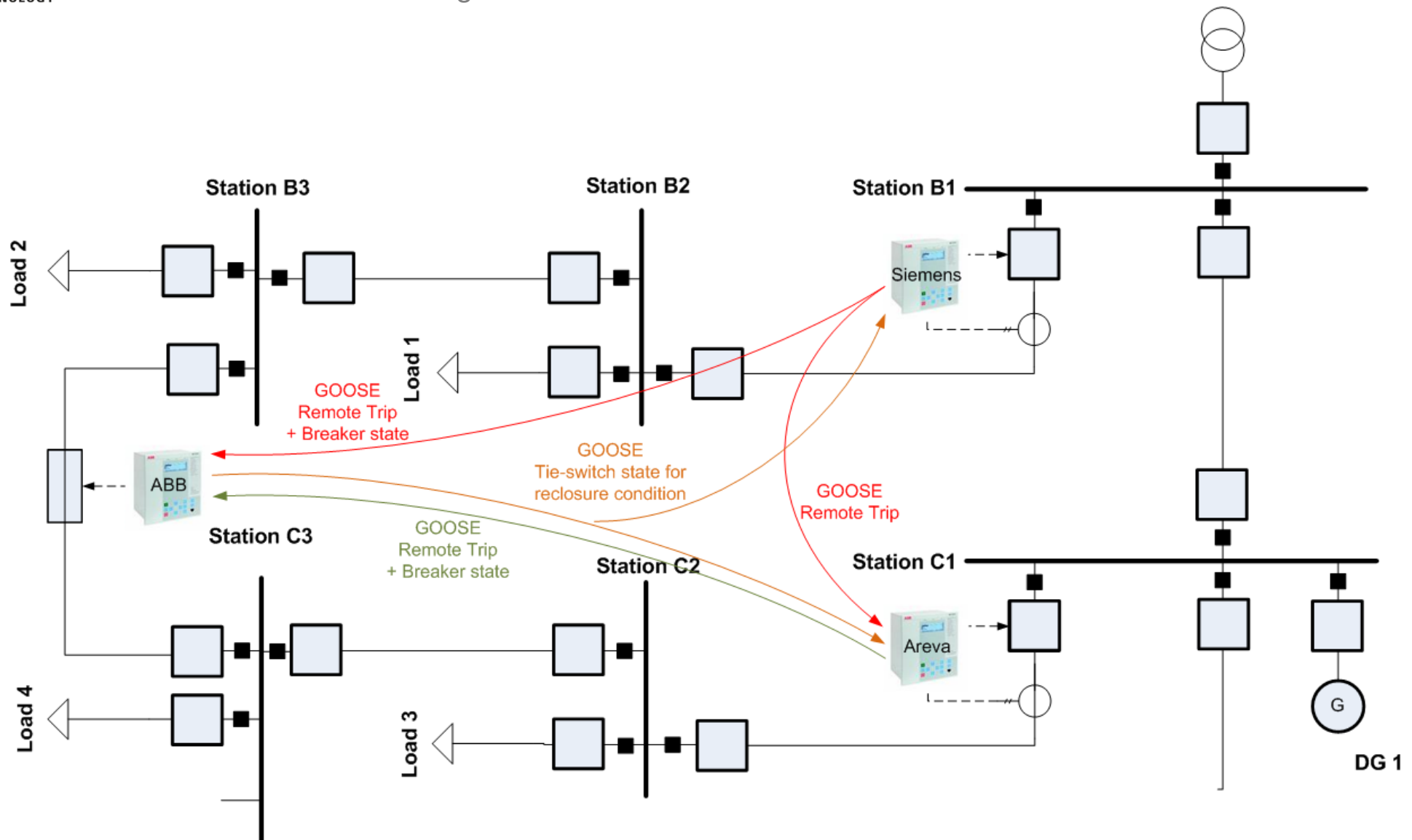
Protocols used in power systems

IEC 61850 configuration



Protocols used in power systems

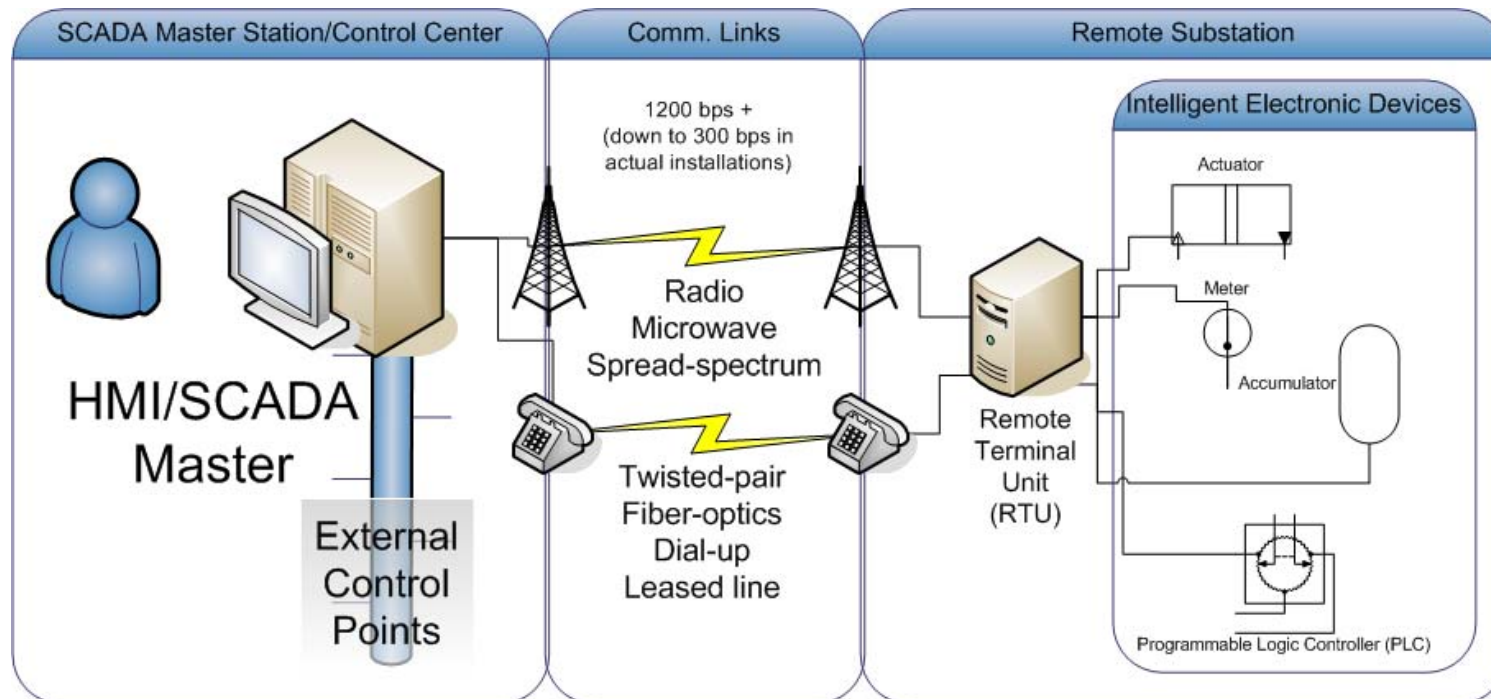
IEC 61850 configuration



Protocols used in power systems

IEC 60870-5-10x

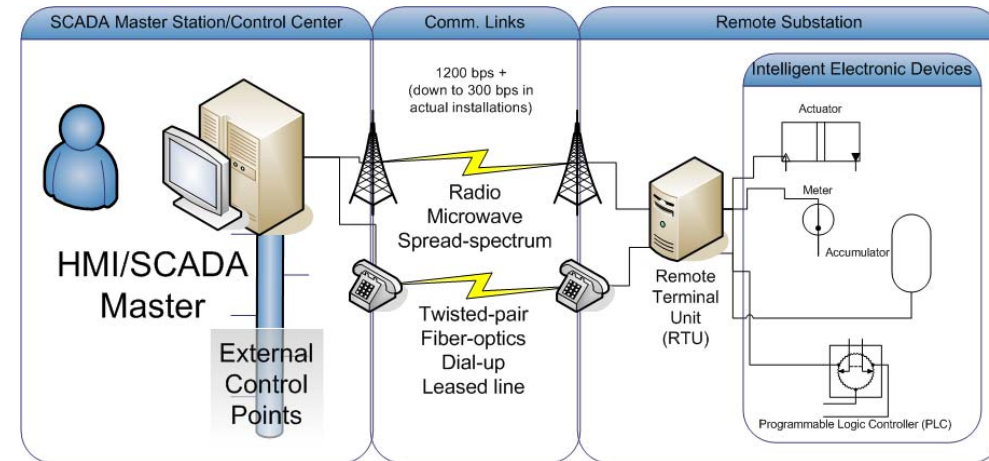
- A suite of “RTU protocols”...



Protocols used in power systems

IEC 60870-5-10x

- 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/substation devices
 - 104 – Variant of 101 carried over TCP/IP
 - Still very commonly used.
 - **Used in our lab with ICS village!**



OLE for Process Control (OPC)

- Object Linking and Embedding (OLE)
- Originally developed to provide an interface between:
 - Windows software applications and
 - Process control hardware.
- A few specifications (versions):
 - OPC Data Access (DA)
 - OPC Alarms & Events
 - OPC Data eXchange (DX)
 - OPC Commands
 - OPC XML-DA
 - OPC Unified Architecture (UA)



OPC Servers

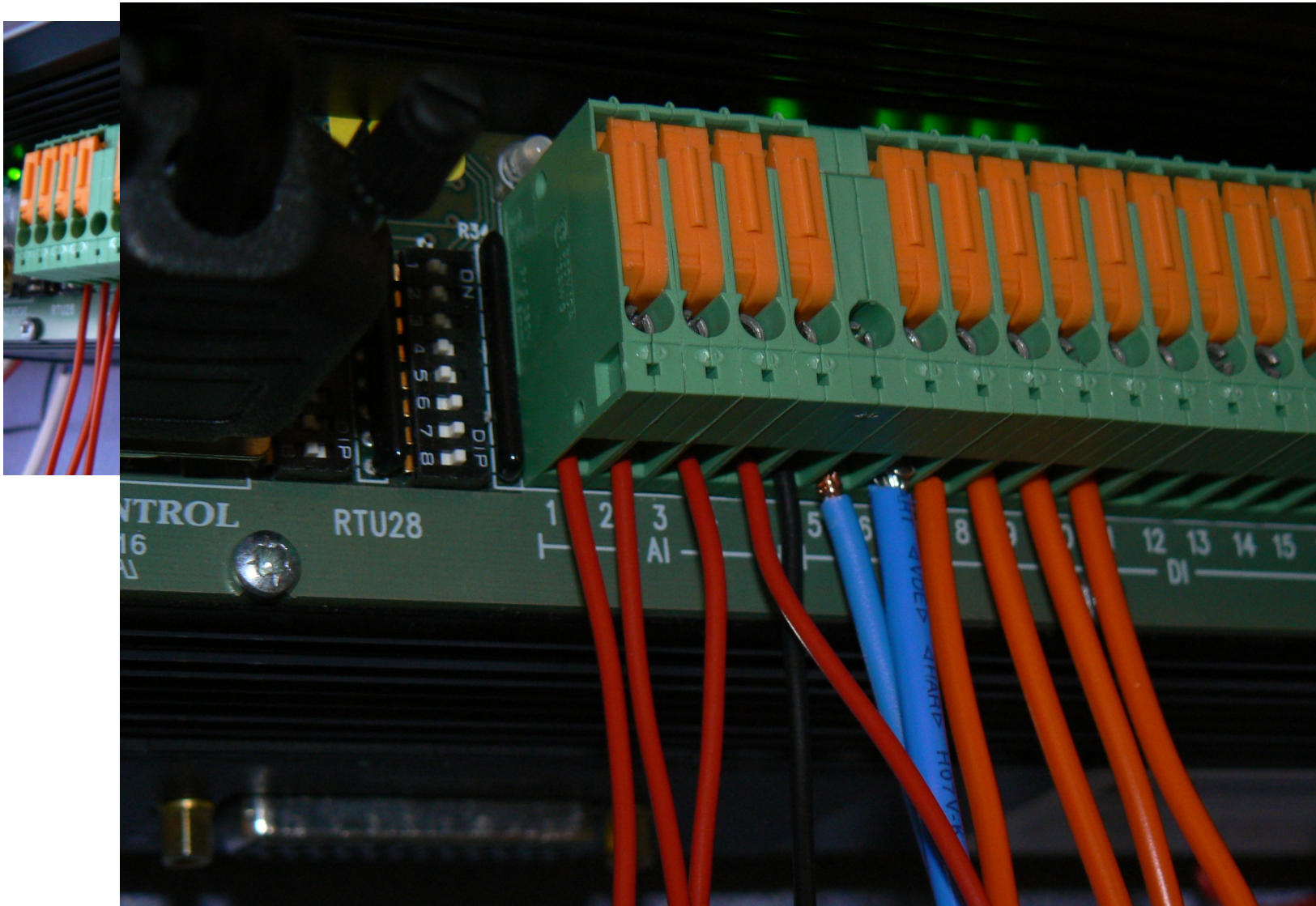
CybServer870M-10x OPC Servers

- Client to communicate with:
 - IEC 60870-5-101 (Serial)
 - IEC 60870-5-104 (IP)
- Server for OPC DA
- Makes RTU data accessible:
 - Status
 - Measurements
 - Commands
 - Map tag names to “870 addresses”

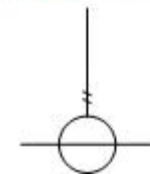
IEC 870-5-104 OPC server

Tag	870 Address	Type	Category
CommStatus	-	System	CommStatus
CommLink	-	System	CommLink
DI5	65541	Acquisition	Boolean
DI6	65542	Acquisition	Boolean
DI7	65543	Acquisition	Boolean
DI8	65544	Acquisition	Boolean
DI9	65545	Acquisition	Boolean
DI10	65546	Acquisition	Boolean
DI11	65547	Acquisition	Boolean
DI12	65548	Acquisition	Boolean
DI13	65549	Acquisition	Boolean
DI14	65550	Acquisition	Boolean
DI15	65551	Acquisition	Boolean
DI16	65552	Acquisition	Boolean
DI17	65553	Acquisition	Boolean
DI18	65554	Acquisition	Boolean
DI19	65555	Acquisition	Boolean
DI20	65556	Acquisition	Boolean
DO21	65557	Command	Double command
DO22	65558	Command	Double command
DO23	65559	Command	Double command
DO24	65560	Command	Double command
DO25	65561	Command	Double command
DO26	65562	Command	Double command
DO27	65563	Command	Double command
DO28	65564	Command	Double command

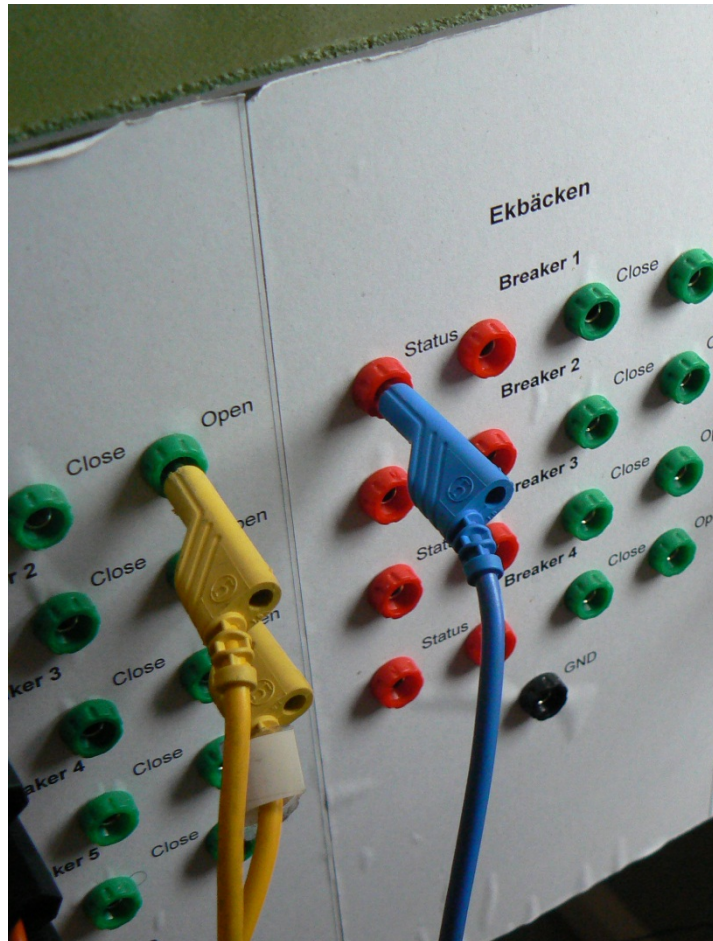
OLE for Process Control (OPC)



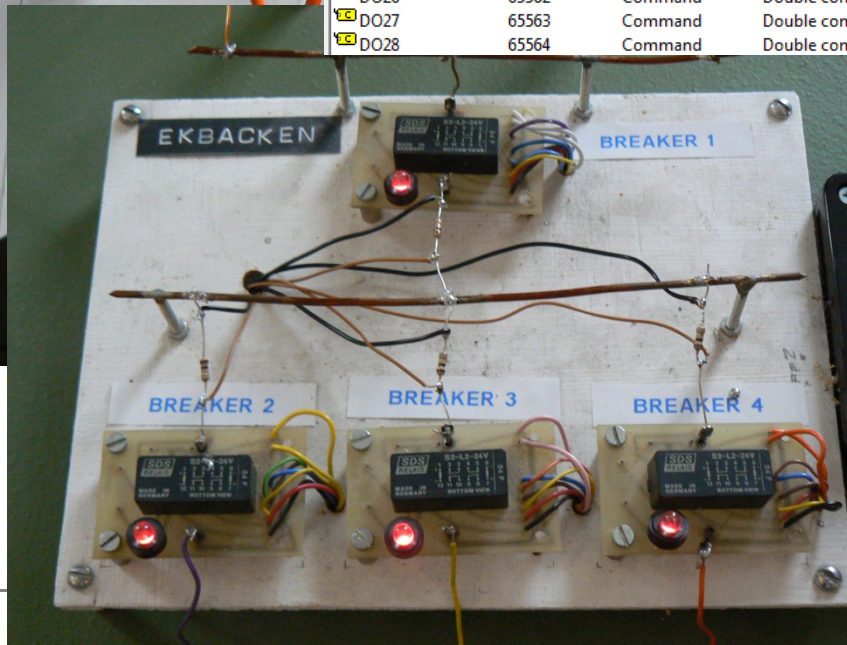
IEC 870-5-104 OPC server



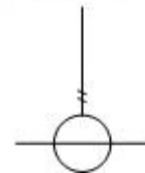
OLE for Process Control (OPC)



Tag	870 Address	Type	Category
CommStatus	-	System	CommStatus
CommLink	-	System	CommLink
DI5	65541	Acquisition	Boolean
DI6	65542	Acquisition	Boolean
DI7	65543	Acquisition	Boolean
DI8	65544	Acquisition	Boolean
DI9	65545	Acquisition	Boolean
DI10	65546	Acquisition	Boolean
DI11	65547	Acquisition	Boolean
DI12	65548	Acquisition	Boolean
DI13	65549	Acquisition	Boolean
DI14	65550	Acquisition	Boolean
DI15	65551	Acquisition	Boolean
DI16	65552	Acquisition	Boolean
DI17	65553	Acquisition	Boolean
DI18	65554	Acquisition	Boolean
DI19	65555	Acquisition	Boolean
DI20	65556	Acquisition	Boolean
DO21	65557	Command	Double command
DO22	65558	Command	Double command
DO23	65559	Command	Double command
DO24	65560	Command	Double command
DO25	65561	Command	Double command
DO26	65562	Command	Double command
DO27	65563	Command	Double command
DO28	65564	Command	Double command



IEC 870-5-104 OPC server



OPC interfacing from Java

JEasyOPC Java class library

- Open-source java class library
- Interface with OPC servers

```
import javafish.clients.opc.JCustomOpc;  
import javafish.clients.opc.JEasyOpc;  
import javafish.clients.opc.JOpc;  
import javafish.clients.opc.async.AsynchEvent;  
import javafish.clients.opc.async.OpcAsynchGroupListener;  
import javafish.clients.opc.browser.JOpcBrowser;  
import javafish.clients.opc.component.OpcGroup;  
import javafish.clients.opc.component.OpcItem;
```

Initialization:

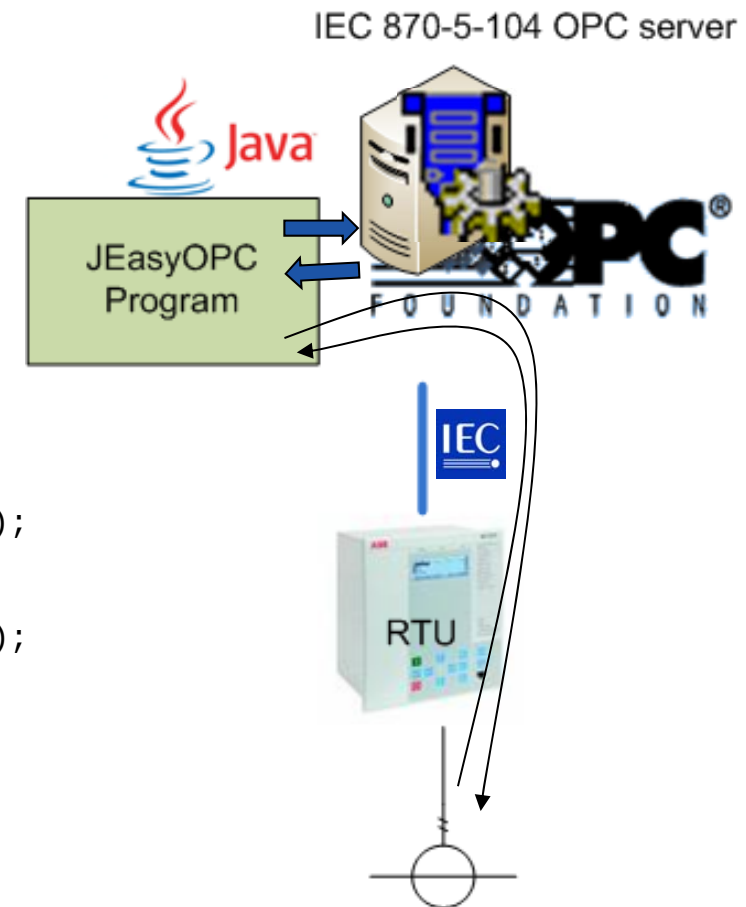
```
jopc_meas = new JEasyOpc(hostName, serverName, groupName + "_meas");
```

Reading:

```
gotItem = jopc_meas.synchReadItem(statusGroup, (OpcItem)ItemToRead);
```

Writing:

```
jopc_command.synchWriteItem(commandGroup, item);
```



OPC interfacing from JACK

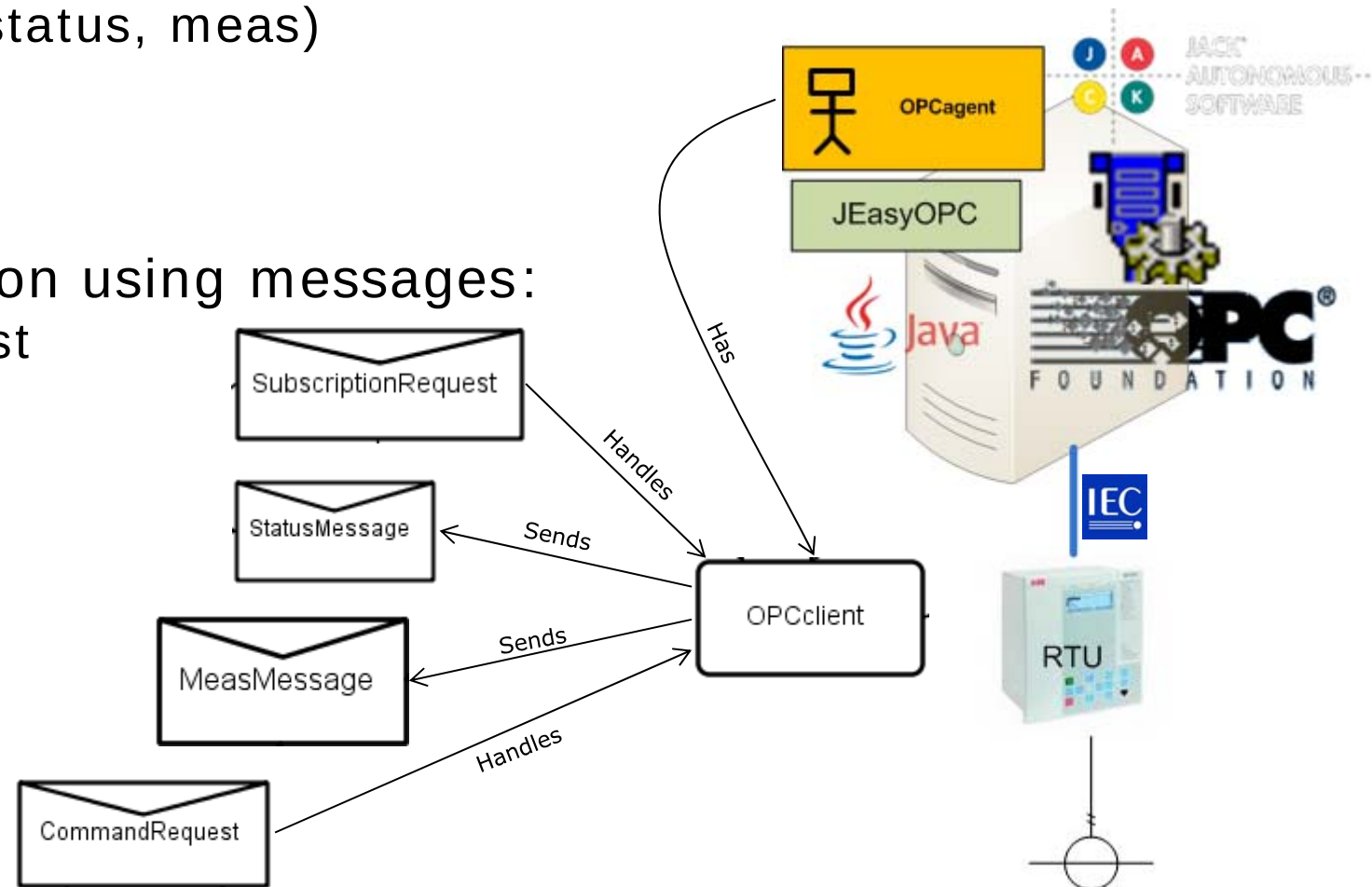
OPCagent

- JACK agent with **OPC client** capability:

- Browser OPC server
- Listen for events (status, meas)
- Issue commands

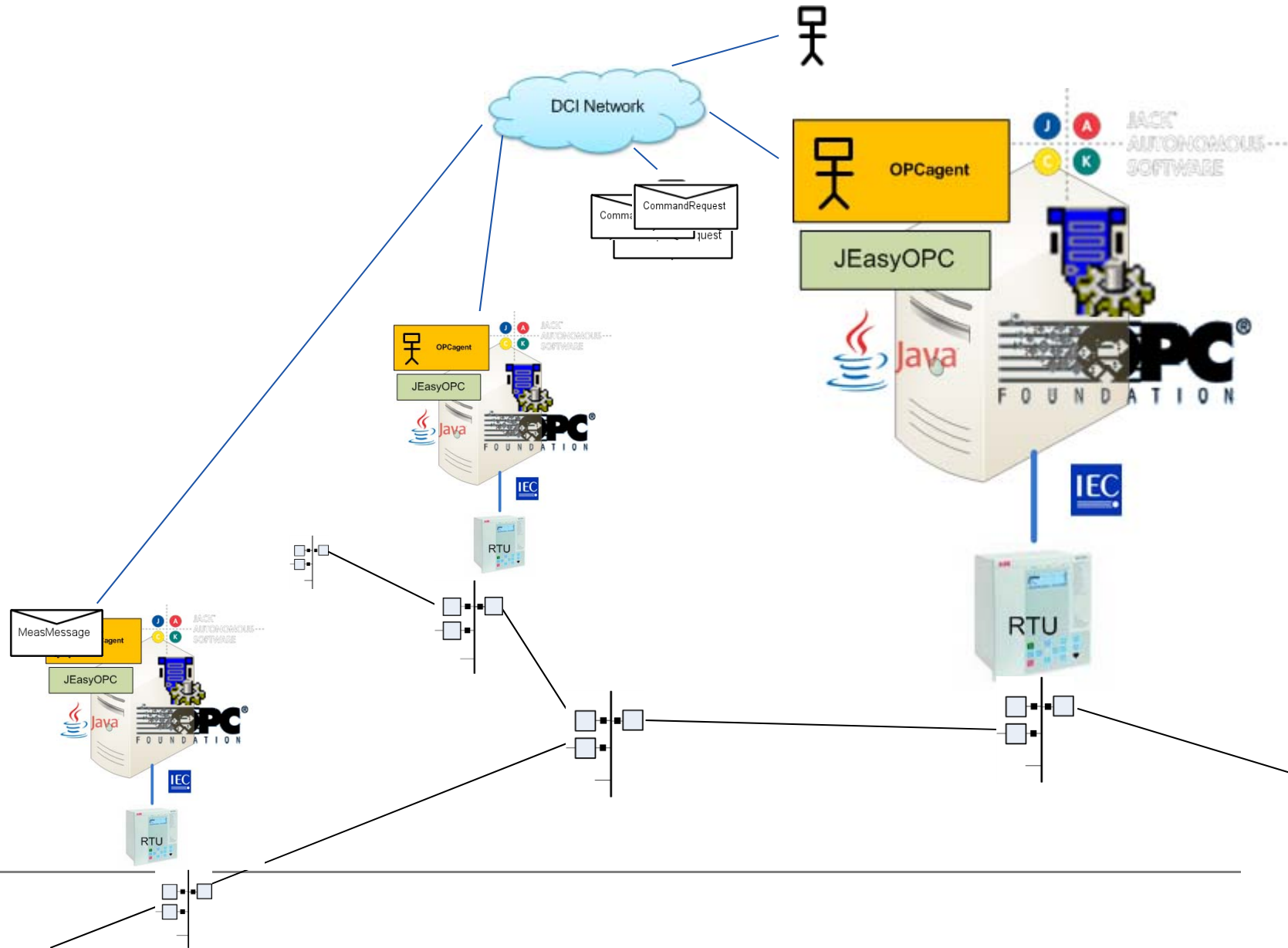
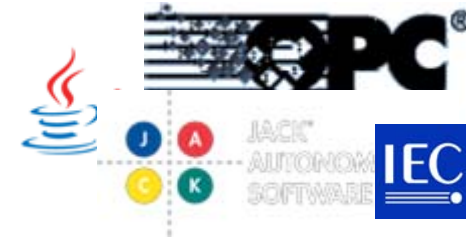
- Agent communication using messages:

- SubscriptionRequest
- StatusMessage
- MeasMessage
- CommandRequest



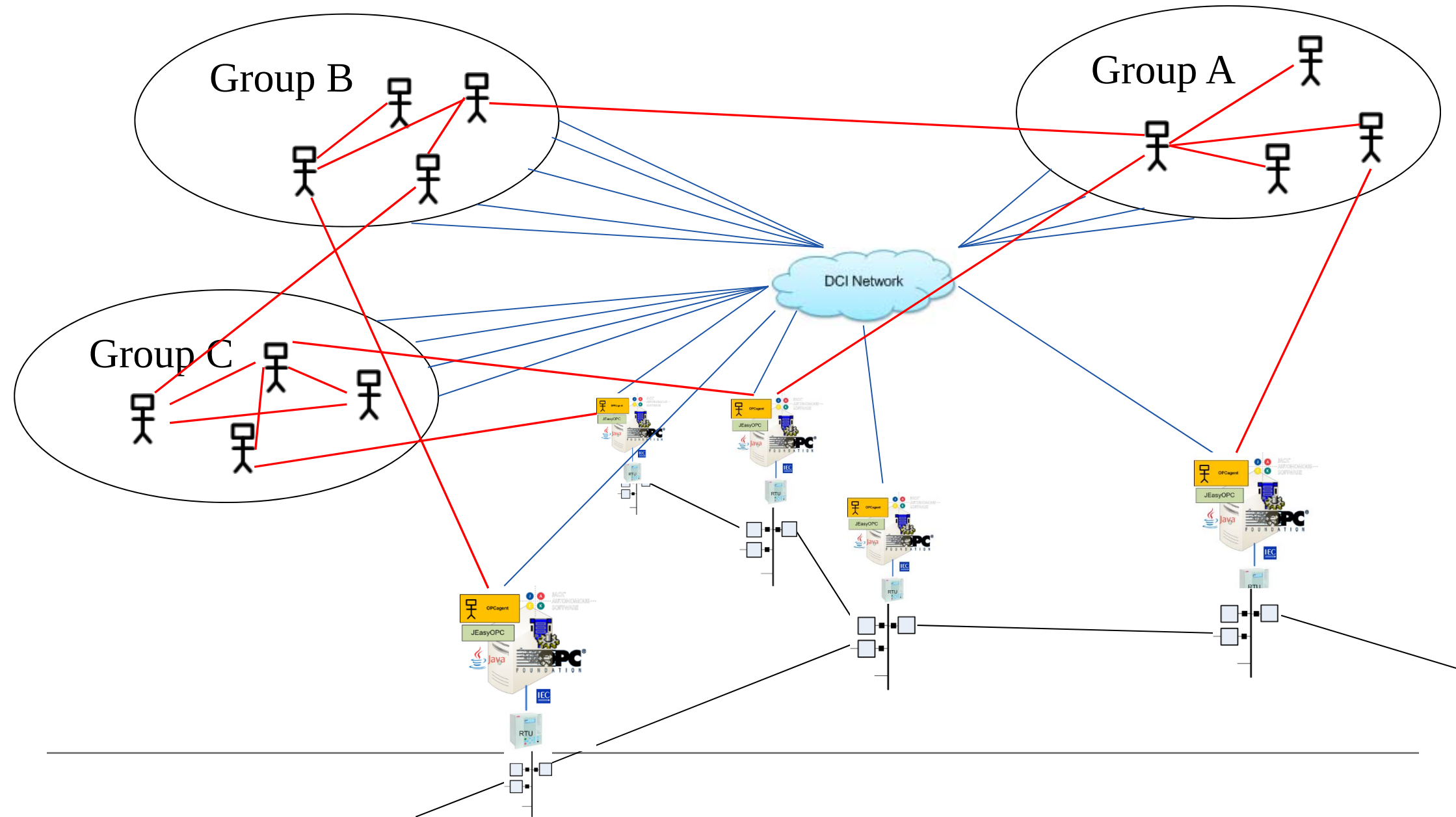
OPC interfacing from JACK

OPCagents communicating over DCI network



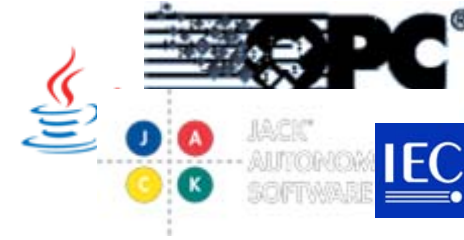
OPC interfacing from JACK

Using OPCagents for building functionality



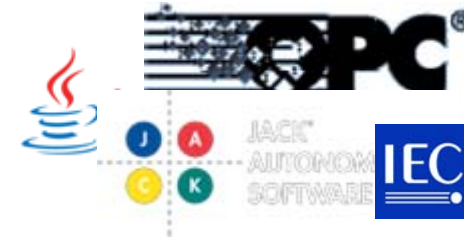
Conclusion

What's next?



- IEC 61850 configuration lab (10th Oct)
 - Divided into groups
 - 3 sessions over the day
 - Configure protection/interlocking between IEDs
 - Monitoring & Control interface via IEC 61850 OPC server
- OPCagent configuration (10th Oct in parallel)
 - Structure of OPCagent
 - Mapping RTU I/O to agent ontology
- Prerequisite – must have finished **tutorial 5**
 - Otherwise this will all feel very random.

Conclusion



- Recap of protocols in power systems applications
- Quick introduction to OPC
- IEC 61850 recap and IED configuration overview
- JACK interfacing with OPC – the OPCagent